

Message

From: Edwin Portugal [REDACTED]
Sent: 3/8/2019 3:57:36 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: AFSA Comments on CCPA
Attachments: AFSA comment letter - CCPA.pdf

Good afternoon,

I work at the American Financial Services Association (AFSA), the national trade association that has represented the consumer credit industry since 1916. On behalf of our industry, we are submitting written comments on the California Consumer Privacy Act. We appreciate the Attorney General's efforts to engage stakeholders through public forums and provide guidance to businesses for how to comply and clarify the law's requirements through the implementing regulations.

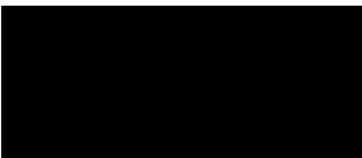
Thank you in advance for taking the time to consider our comments during the rulemaking process. Please let me know if you have any questions.

Best,
Edwin Portugal

Edwin Portugal

State Government Affairs Analyst

American Financial Services Association



March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

Re: CCPA preliminary rulemaking process

On behalf of the American Financial Services Association (“AFSA”),¹ I thank you for the opportunity to provide comments and participate in public forums as part of the Attorney General’s Office’s (“AGO”) preliminary rulemaking process for the California Consumer Privacy Act (“CCPA”). We appreciate AGO’s efforts to provide guidance to businesses for how to comply and clarify the law’s requirements through the implementing regulations.

Though AFSA members share the state’s goal of protecting the privacy of consumers, we have significant concerns about the CCPA, as passed by the legislature, due to vague terms and definitions and the substantial burden it places on covered entities.

Vague Terms and Definitions

Throughout the Act, multiple sections fail to provide a definition for a “verifiable customer request” for information. Notably, the term is referenced in sections 1798.100, 1798.105, 1798.115, and 1798.130. The law offers no framework or guidelines under which a covered business may attempt to verify an individual’s identity, particularly in the cases of individuals with no formal customer relationships. Will a covered business be punished if its identity verification requirements for requesters are too lax or too stringent? The law also offers no guidance whether a consumer’s request for information on behalf of another individual is a “verifiable customer request,” or whether a covered business must comply with a request for a minor’s information from a parent or guardian. We request that rulemaking clearly defines a “verifiable customer request” for information and outlines the process to verify a customer’s identity.

The Act is also vague on how specific the disclosures provided to an individual must be regarding personal information collected and the purposes for which it will be used. The Act does not make clear whether business must disclose only the “categories” or the “specific pieces” of Personal Information about an individual. We request that the rulemaking require only that businesses disclose the categories of Personal Information collected. Such a requirement would be the most helpful way for consumers to understand what information is being collected and would not require the business to aggregate otherwise-segregated or anonymized data and associate it with a specific individual.

1798.105 – Requests for Deletion of Personal Information

This section is vague with respect to the extent of the following deletion exceptions: “reasonably anticipated” within the context of the ongoing business relationship; the “reasonably aligned with the expectations of the

¹ Founded in 1916, the American Financial Services Association (AFSA), based in Washington, D.C., is the primary trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including direct and indirect vehicle financing, traditional installment loans, mortgages, payment cards, and retail sales finance. AFSA members do not provide payday or vehicle title loans.

(individual) based on the consumer's relationship with the business" exception; the "compatible with the context in which the (individual) provided the information" exception; and instances when a requested deletion of Personal Information by a business triggers the no violation of the freedom of speech provisions of the law. Each of these exceptions should be interpreted broadly to ensure minimal disruption of existing customer relationships. Further, the section does not adequately address concerns with the deletion of data used to detect and prevent fraud, which would have troubling consequences for consumers and the economy.

The deletion requirement raises serious concerns regarding information that a business has previously legally acquired in accordance with existing law. Can a state require that a business destroy informational property it has legally acquired that may be of ongoing value to the business? Is this a permissible "taking" of that business asset? If it is permissible, is the business entitled to just compensation from the state for that taken business asset?

1798.115 – Disclosure of Sold Personal Information and Third Party Notice

We request that the rulemaking allow for disclosure using a public website to meet the notice requirements as the categories disclosed are not specific to an individual consumer. Additionally, the section prohibits a third party from selling personal information unless the consumer has received "explicit" notice and is provided an opportunity to exercise the CCPA right to opt-out. Third parties may not have a direct relationship with consumer and may not be able to provide direct notice. As a result, the law may unnecessarily affect the flow of data. As the law is silent to how a third party should receive notice in order to comply with the requirement, we request that the rulemaking allow a third party to rely on its own privacy policy statements or written assurances from first party data providers.

1798.125 Discrimination Based on Exercise of CCPA Rights

The law sets no standard for determining if an extra charge to an individual who exercised CCPA rights is "reasonably related to the value provided by the individual's data." The law fails to define an "unjust, unreasonable, coercive or usurious" financial incentive practice. What happens if an individual who provides the required opt-in to a financial incentive later revokes that consent after he/she has received the financial incentive benefits?

Businesses are required to provide individuals with a clear website opt-out link, but the law fails to specify whether this is the only means by which an individual may opt-out. Would a business be required to honor an opt-out request if an individual contacts any part of a business, anywhere in the world, and makes a request? Could a California resident stop a seasonal sales associate in a Portland, Maine retail store and give her/his opt-out request for Personal Information held by that company? Like other privacy law opt-outs, the individual should be required to use the designated communication process described in the notice given to the customer.

1798.135 – Internet Home Page

The law requires that a business "respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information." If a business changes its financial incentive offerings pursuant to 1798.125, would the business be allowed to provide notice of the new incentives to an individual within 12 months of the decision to opt-out?

1798.140 Definitions

(c) Business

Nonprofit organizations, including political parties and campaign organizations, are excluded from the definition and the law's requirements. The definitions used for commonly controlled businesses typically use a 25 percent threshold (e.g., the federal Bank Holding Company Act), but this law defines control using 50

percent. The controlled entities provision only brings in other entities that have at least 50 percent common ownership AND also share a common brand.

(d) Business Purposes

Are the seven listed examples a comprehensive list of the activities within the definition and its triggered exemptions?

(g) Consumer

This is a misleading term, as the definition is any individual, and is not limited to the type of interaction with a business—ex. personal, family or household use (consumer) or business (commercial)—and the individual need not be a customer of the business. The definition of “Consumer” should not include employees, who already have extensive personal data protection under state and federal employment laws.

The definition incorporates the California income tax definition of a California income taxpayer, which creates numerous problems and fails to consider several situations. What if the individual is a California taxpayer but all the interactions between the individual and the business take place in another state? (ex. a Massachusetts business has an account with a student at a Massachusetts college who provided a Massachusetts address, but is a California taxpayer) What if the individual was not a California taxpayer in the last completed tax year and the tax analysis for the current year, which is based on actions in the entire current year, cannot yet be completed? What if the individual was a California taxpayer in the last completed tax year and moved out of state right after that tax year ended? What if the individual was not a California taxpayer in the last completed tax year and moved to California immediately after that tax year ended? What if the individual believes they are not a California taxpayer and the California income tax authority later establishes they were a California taxpayer? In this same situation, what if the California taxpayer appeals that decision in court? A better test would be an individual who has provided a California mailing address to the business, similar to the federal Gramm-Leach-Bliley law.

(h) Deidentified

What does “cannot reasonably identify” mean?

(j) Device

This definition should not include an object that is capable of being connected to another object, but not connected to the internet (ex. a keyboard attached to a computer with no internet connection).

(o) Personal Information

This definition includes any information connected to a “household,” but that term is not defined. Do household members have to be related? Does it include a college dormitory or multiple tenants cohabitating in an apartment?

The definition broadly includes information that is “capable of being associated” to a person or household, even if the business has never contemplated making that connection. Would this make information that a business never associated with a specific individual, and never intends to try and associate with an individual, but which could possibly, with some effort, be associated with a specific individual, within the definition of that individual’s Personal Information? Personal Information should be limited to information associated with an identified individual and not a device, a household or a family.

The exclusion from the protected Personal Information definition for “publicly available information” is limited to government record information. Vast amounts of public information that can readily be obtained—from the

internet or a phone book, for instance—is covered by this law. This exemption should include information readily available to the general public, like other California privacy laws and federal privacy law. Personal Information should be limited to information collected from an individual and should not include any information related to that person collected from any other source.

(i) Sell, Selling, Sale or Sold

The definition fails to further define “other valuable consideration.” Other valuable consideration is vague and could be interpreted to include every mutually beneficial exchange of Personal Information by covered businesses (ex. a community bank gives another small bank a credit reference for no charge, anticipating that they may someday ask that other bank for a credit reference). The definition should be limited to information being provided for monetary consideration.

1798.145 CCPA Limits

(a)(6) Conduct Outside of California

Without access to geolocation data a business cannot determine if information collected via mobile phone or a portable personal computer was collected while the individual was in California. If an individual in California attempts to shield their location from the business (ex. through use of a virtual private network (VPN)), and the business has no other indication the individual is in California, will the business be in violation of the law if it collects or sells that information? This also raises questions over whether it is constitutionally permissible for California to regulate business that occurs in other states or as part of interstate commerce.

(d) Federal FCRA Exception

The exemption for the Fair Credit Reporting Act exemption only applies to the “sale” of personal information. The term “sale” is defined under the law and requires “monetary or other valuable consideration.” “Valuable consideration” is not defined under the law and, as a result, the exemption may not be complete to cover the transfer of personal information from a lender. The furnishing of credit data is not sold to a consumer credit reporting agency. If the CCPA were to be interpreted to not apply to the furnishing of data to a consumer credit reporting agency, it would have significant economic impacts to the credit reporting system. The Attorney General should provide clarification that the “sale of” requirement in the FCRA exemption would apply to the furnishing of information that is not made for monetary consideration.

(f) Federal Driver’s License Law Exception

It is not clear exactly what information is covered by this exception. Is it just information that is protected by that law, or does it include any information related to a driver’s license that is subject to the law?

(g) Allowed Response Exceptions

The law allows a business up to 90 additional days to respond “where necessary,” but the scope of this exception is vague. It is also vague as to what qualifies as a “manifestly unfounded or excessive” request by an individual that allows a business to charge a fee or refuse to comply with the request.

(h) Service Provider Violations

The law does not create a clear standard for when a business hiring a service provider has “reason to believe,” but no actual knowledge, that a service provider intends to violate this law, thus making the business liable for that violation.

1798.150 Civil Damages

The civil damages authorized by the law are unreasonably burdensome and guarantee at least \$100 to individuals whose personal information was part of an unauthorized access, exfiltration, theft or disclosure, who suffered no harm. These damages would add up very quickly in the event of a large breach or a class action suit

that could involve millions of customers. There are concerns about the constitutionality of imposing automatic punitive damages when there was no harm to the plaintiff(s). For instance, should the unauthorized disclosure of any Personal Information, like a phone number that is publicly available in a phone book, create these rights to an automatic windfall? This allows a court to award an individual up to \$750, as well as undefined “other relief the court deems appropriate,” despite the individual suffering no harm.

The law fails to define what “cure” is required from the business within 30 days of notice from the individual to avoid liability. Further changes to the law and future regulations should describe what is required to be a sufficient notice to cure and how it should be provided to the business. A cure typically cannot involve undoing the data breach, so the only reasonable interpretation of “cure” would be a fix of the conditions that allowed the unauthorized access, exfiltration, theft or disclosure. We request that the rulemaking verify this interpretation.

There is no express standard or duty regarding what a business has to do to reasonably protect Personal Information, just a penalty for any unauthorized access, exfiltration, theft or disclosure of any Personal Information, regardless of the effect or lack of effect of that event. The California Attorney General has created standards for personal data protection, and compliance with those standards should protect a business from liability, particularly when individuals were not harmed by the unauthorized access, exfiltration, theft or disclosure. This law should use compliance with commonly accepted data security “best practices” standards to protect a business from liability for unauthorized access, exfiltration, theft or disclosure of Personal Information, like Ohio recently enacted with House Bill 220.

1798.155 Attorney General Provisions

As with the previous, this section fails to define what “cure” is required from the business within 30 days of notice from the Attorney General to avoid liability. Since that cure often cannot involve undoing all the effects of a violation, is the required “cure” a fix of the conditions of that violation? We also request that regulations verify that the \$7500 amount is a cap on actual damages not an automatic punitive damage award.

1798.185 Attorney General Regulations

The law requires the attorney general adopt regulations to explain how to comply with this new law by July 1, 2020. It allows the attorney general to start enforcement actions beginning six months following adoption of regulations or July 1, 2020, whichever is sooner. This does not allow enough time for businesses to implement the complicated disclosure processes AFTER they are defined by the Attorney General, which could be as late as July 1, 2020, the date businesses are required to be in compliance. The compliance date should be the *later of* six months following adoption or July 1, 2020.

1798.192 No Waiver

It is unclear whether a binding arbitration provision specifically allowed by the Federal Arbitration Act (FAA) violates this prohibition by being an effective waiver of the express right in the law to have court awarded statutory punitive damages. The federal preemption under the FAA requires that the CCPA not limit such binding arbitration provisions.

1798.198 January 1, 2020, Effective Date

Private rights of action for any unauthorized access, exfiltration, theft or disclosure of any Personal Information are allowed on and after January 1, 2020, even if the Attorney General has not yet issued interpretive regulations. Such actions should not be allowed any sooner than the later of six months following adoption or July 1, 2020.

The law does not specify whether businesses will be expected to provide Personal Information pursuant to Section 1798.130(a) for the 12 months preceding January 1, 2020, or if the requirement to track and provide the various categories of Personal Information begins as of January 1, 2020.

Thank you in advance for your consideration of our comments. If you have any questions or would like to discuss this further, please do not hesitate to contact me at [REDACTED]

Sincerely,

A handwritten signature in blue ink, appearing to read "Matthew Kownacki".

Matthew Kownacki
Director, State Research and Policy
American Financial Services Association
919 Eighteenth Street, NW, Suite 300
Washington, DC 20006-5517

Message

From: Kris Rosa [REDACTED]
Sent: 3/8/2019 12:42:14 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: AG Comments on CCPA
Attachments: AG Comments 030719.docx; ATT00001.txt

Please see the attachment containing comments on the CCPA by The Nonprofit Alliance.

Thank you.
Kris

Kris Rosa
Noteware and Rosa
1201 K Street, Suite 1030
Sacramento, CA 95814
[REDACTED]



March 8, 2019

Stacey D. Schesser
Supervising Deputy Attorney General
Consumer Law Section, Privacy Unit
Department of Justice
Office of Attorney General
1300 I Street, Suite 1740
Sacramento, CA 95814

RE: Public Comment on California Consumer Privacy Act

Dear Ms. Schesser:

On behalf of The Nonprofit Alliance, I'd like to thank you for the opportunity to provide written comments regarding the need for clarifying and the narrowing of scope of the California Consumer Privacy Act (CCPA).

When the CCPA was being negotiated and drafted last year, legislators exempted nonprofits from the bill. We are grateful to the Legislature for recognizing the clear intent to exclude nonprofits from the direct hit of the costly impact of this legislation. Nonprofits, however, are still nevertheless impacted because we do not operate in a vacuum.

We use consumer data and third-party data providers to ensure our programmatic and fundraising marketing messages are delivered to those most likely to benefit—and, likewise, not to those who will not.

It is more efficient, more cost effective, and better for potential donors for nonprofits to use data to connect with people. For example, if a consumer purchases a pair of hiking boots at REI, the consumer may be interested in helping support nature conservancy efforts.

The AARP Foundation is an example of how nonprofits use data to fulfill programmatic missions. When seniors are in crisis and are removing themselves further from society, they tend to not raise their hands and ask for help. Instead, seniors in crisis need to be found—and we use data to find them. Certain changes in consumer behavior can be indications that a senior is becoming socially isolated. It's not hard to think of what some of those purchasing changes may be: suddenly no longer buying gas for a car, for example, or only purchasing food products twice a month. AARP can use third party data algorithms to catch these possible red flags and in an appropriate, non-intrusive way ensure that individuals have access to services like transportation

www.TNPA.org

1133 19th St. NW, Suite 402 | Washington, DC 20036

CCPA00000009

to preventative doctor appointments, social activities at community centers, and opportunities to volunteer and regain their sense of worth and connectedness.

We also rely on commercial data companies to maintain our data in secure environments at a level that many nonprofits could not afford to maintain on our own, certainly not without significantly reducing the funds we spend on direct mission work.

The legislative exemptions, therefore, while wonderfully well-intentioned, inadequately protect us from the indirect financial impact of the CCPA.

In fact, nonprofits may be the first to suffer the full impact of the changes when our commercial partners are forced to give us an ultimatum due to the increased costs associated with the CCPA: pay us more due to compliance costs or cease entirely your outreach to 12% of the U.S. population residing in California.

Interestingly, and perhaps not surprisingly to those of us that live in this state—Californians are especially charitable and represent as much as 20% of the fundraising support to national organizations. Their proportional value to smaller state and regional organizations is naturally even greater.

It is not an exaggeration to say that restricting the ability to reach California donors, due to cost impacts of the CCPA, will be devastating to the U.S. nonprofit sector.

There are some specific concerns with the CCPA, and the ways in which they will negatively impact nonprofits, our beneficiaries, and the work done on their behalf.

First, without significant clarity on the scope of obligations relating to the disclosure of information to consumers, we are unnecessarily driving up the cost of data. The CCPA will almost certainly require significant staff augmentation by most data providers unless the scope is narrowed and/or clarified.

A large part of the burden will be in handling requests to provide consumers with copies of the “particular pieces” of personal data.

Data providers have many different types of information, but much of it is meaningless to consumers, and much of it is not easily accessible. The law applies to a very broad category of information, including not only specific information collected from a consumer or observed about a consumer, but also inferences made about a consumer.

For example, a data provider may have internal inferences in an analytical modeling system that ordinarily cannot even be seen by the data provider’s personnel.

Will data providers be required to scour their live and back up records to disclose every score that was produced over a year-long period, or to disclose individual analytical variables from a modeling system?

For most organizations, this will require manual searches to gather data from systems that are not even intended to be read by humans. We do not think consumers need or want that type of disclosure. Without narrowing the scope of disclosure, costs will go up and nonprofits are hit hard.

We believe the CCPA can be clarified and improved so that consumers are given meaningful disclosures and choices without extreme levels of expense.

The Nonprofit Alliance is seeking clarification and narrowing of scope to meaningful information that will benefit the consumers and thereby reduce the heavy cost impact of data related to compliance.

By way of information, The Nonprofit Alliance formed in 2018 in response to a growing urgency from the nonprofit sector for an authoritative voice to promote, protect, and strengthen the philanthropic sector.

The Nonprofit Alliance represents a diverse landscape of causes. We feed the hungry, shelter the homeless, rescue the lost, stand up for our veterans, advocate for the neglected, search for cures, protect the threatened, and help piece together communities after disasters. Public support from individual donors represents almost 80% of philanthropic funding in the United States, and with every contribution, our donors affirm their faith that we will adhere to the highest standards of trust and effectiveness.

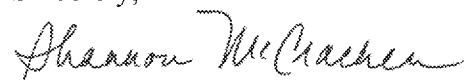
We take their trust and their generosity very seriously, for it is through this partnership of donors and nonprofits that we make a meaningful difference in our world.

We are organizations like American Heart Association, The Nature Conservancy, AARP Foundation, Alzheimer's Association, Food & Water Watch, DAV, Share Our Strength, Food for the Poor, YWCA, Special Olympics, National Audubon Society, Feed the Children, National Aquarium, Defenders of Wildlife, and Doctors Without Borders; and we are the expert partners that help nonprofits in their public outreach, fundraising, and resource development.

We care about accountability to a society that understands and values the vital role of nonprofits in our world today. We care about responsible use of technology and data that enable nonprofits to provide relevant, timely outreach to people who care about our missions. We care about donors and supporters who are as invested in our work as we are. And we care the future of our sector. The Nonprofit Alliance is committed to doing what is necessary today to ensure that nonprofits continue to have the resources and influence needed to thrive.

Thank you for your consideration.

Sincerely,



Shannon McCracken
CEO

www.TNPA.org

1133 19th St. NW, Suite 402 | Washington, DC 20036

CCPA00000011

Sent from my iPhone

Message

From: Christopher Oswald [REDACTED]
Sent: 2/5/2019 3:20:45 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: ANA statement - Sacramento
Attachments: ANA Statement at CA Hearing (Sacramento) (002).pdf
Flag: Follow up

Attached is the Association of National Advertisers statement delivered today, February 5, 2019 at the Sacramento public hearing. We look forward to submitting formal written comments at a later date.

Please feel free to contact me if you have any questions.

Christopher Oswald | SVP, Government Relations

ANA – Association of National Advertisers



www.ana.net | @ANAGovRel





**MAKES A
DIFFERENCE**
For you, your brands,
our marketing industry

**Statement of the Association of National Advertisers to the
California Attorney General on the California Consumer Privacy Act
February 5, 2019**

Good morning, and thank you for the opportunity to provide comments regarding CCPA impacts on consumers and the advertising industry, in particular, and the digital economy in general. My name is Christopher Oswald, and I am the Senior Vice President of Government Relations at the Association of National Advertisers.

The ANA is the advertising industry's oldest trade association. ANA's membership includes nearly 2,000 companies and marketing solutions providers, with 25,000 brands that engage almost 150,000 industry professionals and collectively spend or support more than \$400 billion in marketing and advertising annually. Nearly every advertisement consumers see in print, online, or on TV is connected in some way to ANA members' activities. In California, advertising helps generate \$767.7 billion or 16.4% of the state's economic activity and helps produce 2.7 million jobs or 16.8% of all jobs in the state. Our members include leading marketing data science and technology suppliers, ad agencies, law firms, consultants, and vendors. The ANA also counts among its membership a large number of nonprofits and charities that will be substantially affected by the CCPA, as they are highly dependent on the use of data provided by groups covered by the act to market and to reach donors effectively to fulfill their missions. Many of ANA's members are headquartered in California or carry out significant business in California.

The ANA strongly supports the underlying goals of the CCPA. Privacy is an extraordinarily important value that deserves meaningful protections in the marketplace. As an industry, we've taken a number of steps to put these values into practice—for instance, providing consumers control over data transparency with respect to the collection, use and transfer of data, and implementing strong self-regulatory bodies, such as the Digital Advertising Alliance, or "DAA", to ensure accountability in the marketplace. As I noted during the January 14th hearing in San Diego, as we look closely at the CCPA we are concerned that some aspects of the law will have unintended adverse consequences for consumers, businesses, and advertisers that will inadvertently undermine rather than enhance consumer privacy. During that hearing I urged you to:

- 1. Permit a business to offer loyalty-based discount programs that consumers value and expect without the program constituting "discrimination" under the CCPA (Section 1798.125).**
- 2. Recognize that a written assurance of CCPA compliance is sufficient and reasonable for ensuring the consumer has received "explicit notice" and is provided an opportunity to exercise the right to opt out of that sale (Section 1798.115(d)).**

3. Clarify that businesses may offer reasonable options to consumers to choose the types of “sales” they want to opt-out of, the types of data they want deleted, or to completely opt-out—and not have to just provide an all-or-nothing opt-out option (Sections 1798.105 and 1798.120).

4. Clarify that individualized privacy policies for each consumer need not be created in order to disclose the “specific pieces of personal information the business has collected about that consumer” (Section 1798.110(c)).

5. Refine the definition of the term “Personal Information.” Currently, the term creates tremendous ambiguity around what data is covered by the law (Section 1798.140(o)).

Today, I add to that list three other important issues that we urge you to clarify during the rulemaking process:

First, Section 1798.140(o)(1)’s definition of “personal information,” in combination with Section 1798.140(g)’s definition of “consumer,” suggests that the law will treat pseudonymized data in the same manner as data that could directly identify an individual. However, pseudonymized data does not include data types that individually identify a person, like name or email address. Instead, pseudonymized data is rendered in a manner that does not directly identify a specific consumer without the use of additional information. Pseudonymized data, therefore, does not raise the same privacy concerns as identifiable information. The CCPA could have the unintended effect of forcing business to associate non-identifiable, pseudonymized device data with a specific person seeking to exercise their CCPA rights. This approach would remove existing data privacy protections enjoyed by California residents pursuant to the DAA’s privacy program. We urge you to distinguish pseudonymized data from personal information while imposing DAA-like safeguards against the processing of pseudonymized data. This approach will help ensure California residents continue to benefit from existing privacy choices while helping to assure that data related to their online activities does not become identifiable.

Second, Section 1798.140(y) and other sections of the CCPA allow for a person or entity that is “authorized by the consumer to act on the consumer’s behalf” to make a deletion or access request for the consumer under the law. Our concern is that authorized third parties who make requests on behalf of consumers appear to be under no obligation to fully inform consumers of the implications of their choices, but they should be required to inform consumers of the practical results of making a CCPA request, since the business that will need to comply with the request will not be able to do so. Without such a requirement, consumers would not be able to make informed choices in the course of exercising their CCPA rights. ANA requests that you require authorized third parties that make CCPA requests on behalf of consumers to communicate information to consumers about the implications of the request.

Third, Section 1798.105(d)(1) provides an exception to the deletion right for businesses that need a consumer’s personal information “in order to... provide a good or service requested by the consumer, or reasonably anticipated within the context of a business’s ongoing

business relationship with the consumer.” This language does not clearly place marketing messages, such as subscription renewal reminders, within the purview of the exception. Consumers expect and value these messages. The ANA asks you to clarify that the deletion exception for providing a service requested by the consumer or reasonably anticipated by the consumer includes marketing messages, such as subscription renewal reminders.

Thank you for the opportunity to speak today. There are a number of other areas of concern, and the ANA looks forward to submitting detailed written comments and working with you to develop implementing regulations for this important legislation. To the extent that there are needed changes identified in this submission to protect consumer privacy and other important interests that cannot be rectified by this rulemaking, but are better suited for legislation, we hope the AG will make such recommendations to the California Legislature.

Thank you.

Message

From: Christopher Oswald [REDACTED]
Sent: 1/14/2019 12:14:33 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: ANA statement - San Marcos
Attachments: ANA Statement to CA AG on CCPA final.pdf
Flag: Follow up

Attached is the Association of National Advertisers statement delivered today, January 14, 2019 at the San Marcos public hearing. We look forward to submitting formal written comments at a later date.

Please feel free to contact me if you have any questions.

Christopher Oswald | SVP, Government Relations

ANA – Association of National Advertisers



www.ana.net | @ANAGovRel





**MAKES A
DIFFERENCE**
For you, your brands,
our marketing industry

**Statement of the Association of National Advertisers to the
California Attorney General on the California Consumer Privacy Act
January 14, 2019**

Good morning, and thank you for the opportunity to provide input on the CCPA concerning its impacts on consumers and the advertising industry, in particular, and the digital economy in general. My name is Christopher Oswald, and I am the Senior Vice President of Government Relations at the Association of National Advertisers.

The ANA is the advertising industry's oldest trade association. ANA's membership includes nearly 2,000 companies, marketing solutions providers, with 25,000 brands that engage almost 150,000 industry professionals and collectively spend or support more than \$400 billion in marketing and advertising annually. In California, advertising helps generate \$767.7 billion or 16.4% of the state's economic activity and helps produce 2.7 million jobs or 16.8% of all jobs in the state. Our members include leading marketing data science and technology suppliers, ad agencies, law firms, consultants, and vendors. The ANA also counts among its membership a large number of nonprofits and charities that are affected by the CCPA, as they use data and marketing to reach donors and carry out their missions. Nearly every advertisement you'll see in print, online, or on TV is connected in some way to ANA members' activities. Many of ANA's members are headquartered in California or carry out significant business in California.

The ANA strongly supports the underlying goals of the CCPA. Privacy is an extraordinarily important value that deserves meaningful protections in the marketplace. As an industry, we've taken a number of steps to put these values into practice—for instance, providing consumers control over data, transparency with respect to the collection, use and transfer of data, and implementing strong self-regulatory bodies to ensure accountability in the marketplace. As we look closely at the CCPA, however, we are concerned that some aspects of the law, while well-intentioned, will have unintended consequences for consumers, businesses, and advertisers that will inadvertently undermine rather than enhance consumer privacy.

The Attorney General plays a critical role in interpreting and clarifying this new law. In doing so, we urge the AG to consider clarifying a number of provisions in the law; especially the five important issues we highlight today:

First, Section 1798.125 of the CCPA prohibits businesses from “discriminating” against consumers who have exercised their rights under the law unless the activity is “reasonably related to the value provided to the consumer.” Our concern is that the “reasonably related to the value provided to the consumer” language is not defined, and there is no standard to assess its meaning. In addition, it seems quite possible that loyalty discount programs may be considered a discriminatory practice under the CCPA since these programs create different price levels between consumers – and, therefore, may be prohibited. Consumers who make a deletion request or opt-out request will restrict the very data that allows them to participate in a loyalty program.

As a result, those consumers who cannot participate will automatically be treated differently than other consumers in the loyalty program. This could run afoul of the ambiguous wording in the law, which only allows these types of programs when the activity is “reasonably related to the value provided to the consumer.” There is nothing in the law that provides guidance on how this determination of what is “reasonable” could or should be made. We contend that these loyalty programs should not be jeopardized because one, or a few, consumers exercised their rights under the law and can no longer participate because a business does not have their data. Loyalty programs allow businesses to maintain and foster positive relationships with consumers. They provide consumers significant benefits in the form of lower prices and access to special offers. Accordingly, the ANA urges the AG to permit a business to offer loyalty-based discount programs that consumers value and expect without the program constituting “discrimination” under the CCPA.

Second, Section 1798.115(d) of the CCPA prohibits a company from selling consumer personal information that it did not receive directly from the consumer unless the consumer has received “explicit notice” and is provided an opportunity to exercise the right to opt-out of that sale. Our concern is that the company may have no way to directly provide “explicit notice” to the consumer. As such, the company must be able to rely on assurances from its data provider that the consumer received proper notice. If not, the online advertising ecosystem, which involves multiple parties that may not have direct relationships with consumers in order to deliver advertisements, will fall apart. These companies may not be able to provide consumers the proper notice, which would prevent them from sharing information to deliver advertising. Accordingly, the ANA urges the AG to recognize that a written assurance of CCPA compliance is sufficient and reasonable under the circumstances.

Third, Sections 1798.105 and 1798.120 of the CCPA allow consumers entirely to opt-out of the sale of their data or delete their data; but the law does not explicitly permit a business to allow a consumer the choice to delete or opt-out regarding *some, but not all*, of their data. The law is not clear on whether consumers can be offered multiple choices related to their deletion and opt-out rights, even though consumers may value those additional choices. For that reason, the ANA requests that the AG clarify that businesses may offer reasonable options to consumers to choose the types of “sales” they want to opt-out of, the types of data they want deleted, or to completely opt-out—and not have to just provide an all or nothing option.

Fourth, Section 1798.110(c) of the CCPA arguably requires a business’ privacy policy to disclose to a consumer the “specific pieces of personal information the business has collected about that consumer.” Since data differs from one consumer to another, to comply with this provision, a business would need to create personalized privacy policies for each consumer that visits their website. We do not believe that the Legislature intended this outcome, as this would be incredibly burdensome and raises the likelihood of inadvertent disclosures of specific consumer information to the wrong recipients. Also, this requirement, confusingly, is found in the part of the law describing consumer access rights, which suggests that the provision is meant to cover specific consumer requests, not simply anytime the consumer looks at the privacy policy. Thus, the ANA asks the AG to clarify that a business does not need to create individualized privacy policies for each consumer to comply with the law.

Fifth, Section 1798.140(o)'s definition of "personal information" is extremely broad and includes information that is "capable of being associated with" a "particular consumer or household," which creates tremendous ambiguity around what data is covered by the law.

There are three issues of importance here: (A) Any data theoretically is "capable of being associated with" a particular consumer, which means that there is no reasonable limitation on the scope of the law. Without more clarity, businesses may end up deleting or sharing more information than is necessary. (B) The use of the term "consumer" in the CCPA arguably could include employees and employee data. When a person is acting in the marketplace on behalf of their business, the data that is captured is business data, not consumer data. If not corrected, this provision would allow employees to access information and potentially compromise confidential business information and inappropriately utilize deletion and opt-out rights. (C) Finally, the law states that information about a "household" is covered although the term "household" is not defined in the law and could lead to information disclosures to the wrong individuals. What is a household, and who is included within a household? Are room-mates part of the same household? Are grown children part of the same household? For these reasons, the ANA asks the AG to clarify: (1) the definition of "personal information" to ensure that the term does not cover data that is just theoretically possible of being associated with a consumer or household but that is actually or reasonably related to a particular consumer or household; (2) provide clarity on the definition of "consumer" so that it does not include employee or other business data; and (3) clarify the definition of "household" to provide meaningful and practical guidance to consumers and the marketplace.

Thank you for the opportunity to speak today. The ANA looks forward to submitting detailed written comments and working with you as the AG develops implementing regulations for this important legislation. To the extent that there are needed changes in the CCPA to protect consumer privacy and other important interests that cannot be rectified by this rulemaking, but are better suited legislation, we hope the AG will make such recommendations to the California Legislature.

Thank you.

Message

From: katiekennedy@apple.com [REDACTED]
on behalf of Katie Kennedy [REDACTED]
Sent: 3/8/2019 3:10:54 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Apple Inc Comments to the California Department of Justice re CCPA
Attachments: Apple Inc Comments to California Department of Justice re CCPA.pdf

To Whom It May Concern:

Please find attached comments filed on behalf of Apple Inc. with the California Department of Justice in connection with the Office of the Attorney General Rulemaking regarding the California Consumer Privacy Act of 2018.

Please do not hesitate to reach out with any questions.

Thank you,

Katie

Katie Kennedy | Privacy and Information Security Counsel | [REDACTED]



COMMENTS OF APPLE INC.
in connection with the Office of the Attorney General Rulemaking
regarding the California Consumer Privacy Act of 2018

At Apple, we believe privacy is a fundamental human right. We purposely design our products and services to minimize our collection of user data. When we do collect data, we are transparent about it, and we work to disassociate it from the user where possible. If we do collect information that is associated with a particular user, we take steps to provide users with choice and control over their personal information. The customer is not our product, and our business model does not depend on collecting vast amounts of personal information to enrich targeted profiles marketed to advertisers.

We are proud of our deep commitment to protecting consumer privacy. However, we also recognize that privacy needs to be protected by safeguards that go beyond the commitments of individual companies. Laws and regulations are needed to ensure that individuals can understand how their personal information is used and trust that their privacy will be respected, regardless of the values or business model of the company that is processing their data.

As a technology company on a quest to be continuously situated at the forefront of technological innovation, we also understand the immensely important role that user data plays in providing, researching, and developing valuable services for consumers. From our own experience, we know that respect for user privacy and the provision of innovative data-driven services are not mutually exclusive. Therefore, it is crucial that any privacy law be implemented in a way that appropriately balances important consumer privacy considerations with the benefits that individuals can derive from transparent and respectful use of their data and incentivizes the creation and deployment of privacy preserving architectures and technologies.

We applaud the California Attorney General's office for its extensive efforts to solicit comments from the public, civil society, and industry as part of the California Consumer Privacy Act rule-making process. We respectfully offer the following comments on certain key issues where the Attorney General has the power to adopt rules that could clarify ambiguities in the text of the CCPA, mitigate the risk of unintended negative consequences, and improve the overall effectiveness of the law in protecting consumer privacy.

As discussed in more detail below, we encourage the Attorney General to support and encourage privacy-protective technologies and design choices, including by confirming that not all information that can be linked to a rotating or resettable device-generated identifier is necessarily "personal information." As explored below, keying data to rotating or resettable device-generated identifiers that are not associated with personally identifiable information are important techniques that protects user privacy. We also encourage the Attorney General to

Apple
One Apple Park Way
Cupertino, CA 95014



consider the role of security in protecting privacy and personal information in its rulemaking, for example by recognizing the benefit of requiring sign-on to an existing account for verification provided such account has reasonable and appropriate security controls for access to personal information.

We thank you for this opportunity to provide comments on this first-in-kind U.S. privacy law.

I. The Attorney General's CCPA Rules Should Support and Encourage Privacy Protective Technologies and Design Choices

A. *Apple's comprehensive design choices protect consumer privacy while allowing for the collection of information that supports and helps improve the services that consumers request*

As part of our privacy-focused culture at Apple, we strive to minimize our collection of user data. However, it is sometimes necessary to collect data from users to provide or enhance valuable services to our users. In those instances, we employ privacy by design, including by building our services so that the data we collect cannot be associated with a specific identified user.

Both Apple's Maps and intelligent assistant services are leading examples of great features that rely on data from users and provide great privacy. We encourage the Attorney General to consider how the CCPA rules can be used to incentivize businesses to adopt these or other novel privacy protective technologies so that both consumers and companies will be better off than they were before.

1. *Apple Maps*

At Apple, we recognize that tracking a user's precise location information has the potential to provide insights about the person's habits, characteristics, and preferences. While some companies have sought to exploit this data, Apple has made a firm commitment to protect the privacy of where you've been, where you are, and where you go. We believe that just because your device needs to know your location to provide you with relevant services, such as the weather at your location, does not mean that Apple — or any company — should know exactly where you are unless you have made an informed choice to share that information with them. Because of this, Apple collects location data only after a user has made the affirmative decision to turn on Location Services. And, Apple only collects location data associated with an identifiable individual to provide features to those users like Find iPhone and Find Friends; other location data that Apple collects is associated with random rotating identifiers or no identifier at all.



It's that simple, and it's because we focused on developing privacy protective technologies of the sort that could be incentivized by the CCPA and its rulemaking.

Where location information is necessary to provide valuable services that are requested by users, one of Apple's first questions is whether and how the service could be provided without the need for any personally identifying information to reach Apple — that is, can we provide the same service without having to identify the user. An example of one such service is Apple Maps, a navigational tool that allows users to plan trips and learn about their surroundings:

You don't need to sign in to use Maps. And, information about your Maps trips, including locations searched and destination are associated with random identifiers that automatically reset themselves as you use the app. In fact, in challenging ourselves to create a privacy protective Maps technology, we realized that we did not need to know information about your whole trip to help you get from A to B or to estimate how long it takes you to get there or even when you need to leave; all we need to know is how long it takes an average person to travel a given stretch of road. This is key because one of the greatest differentiators among the trips people take is the first few minutes of driving and the last few minutes of driving — the precise locations of where you are starting and where you are going. It's this information that tells companies where you live and go to work and helps them to infer who your best friends are or where you bank and create profiles on you. By disconnecting the start and end segments from each other and then again from those in the middle of the trip, Apple can calculate how long it should take you to travel each segment without needing to know anything about *you* in particular. Apple can then send information about the average segment duration to your device, which knows your start and end point, and which can calculate the total trip time or even tell you when you need to leave. All this can occur without Apple needing to know a thing about your precise whereabouts.

As noted above, the random segment identifiers automatically reset themselves, so that you — or even segments of your trip — are not associated with the same identifier each time you travel. And, these random identifiers are not associated with any other personally identifying information such as name, email, or Apple ID. By relying on the privacy protective technology of non-personally identifiable, random, resetting device generated IDs, Apple can provide you maps that are private so that information about where you go during the day stays yours.

2. *Siri*

Siri is another Apple service designed with privacy at the forefront. Siri is an intelligent assistant that allows users to quickly take a variety of actions on their Apple devices by simply speaking their request. When a user interacts with Siri (e.g., asks a question), the recording of their request is sent to Apple servers, where it is processed and a response is generated. To facilitate context-based actions by Siri (e.g., calling the contact the user has labeled as "Dad," turning



on the set of lights the user has labeled “Living Room”), the device may also send Apple certain information from the user’s device (e.g., contact names, names of apps installed on the device).

As with Apple Maps, to protect user privacy, Apple identifies your Siri data not with an email address or phone number but rather by using resettable device-generated identifiers. Apple does not associate a Siri ID with any other identifier that is connected to a particular user, such as email or Apple ID. Additionally, users have the ability to easily reset their randomly generated Siri ID by disabling and re-enabling Siri in their device settings, effectively restarting the relationship with Siri. When a user disables Siri, Apple deletes all of the information associated with that Siri identifier, and Siri will start learning to understand the user all over again.

In addition, as explored above with Maps, where Apple can provide the service without needing to send your information from the device to Apple, we work to do just that. In the Siri context this means that using Siri for things like searching for a photo does not involve sending photos off of the device; they can stay right there — Apple doesn’t need to see them.

By using a random, resettable device identifier for Siri-related data, Apple is able to perform the complex server-based processing operations that power Siri, while also taking steps to ensure that the information collected in the context of Siri requests cannot be traced back to any identified user.

B. To support privacy-protective technologies, the Attorney General should clarify that data keyed to rotating or resettable device-generated identifiers and not associated with personally identifiable information does not fall within the definition of personal information

This rulemaking process provides the Attorney General with an opportunity to greatly enhance consumer privacy and the underlying goals of the CCPA by confirming that the term “personal information” does not include data identified by non-personally identifiable identifiers such as those that are random, resettable, or rotating.

Under the CCPA, the definition of “personal information,” includes information that “relates to, describes, [or] is capable of being associated with [...] a particular consumer or household.” If the term “personal information” were interpreted overly broad so as to include data identified solely by a random, non-static or resettable identifier, a business that maintained such data may be forced to build a way to link random, non-static or resettable identifiers to identified consumers in order to respond to consumers’ CCPA access or deletion requests. Doing so would likely undermine the privacy interests of consumers (including those who may not exercise their specific CCPA rights) and unnecessarily burden businesses that already provide privacy-protective services to consumers.



First, linking identified consumers to data that was previously keyed to rotating or resettable device-generated identifiers solely for CCPA compliance purposes increases the risk that private information about the individual could be revealed in the event the data is subject to unauthorized access (e.g., a data breach). A key benefit of the use of non-personally identifiable identifiers is that neither the business that collects the data, nor any unauthorized recipients of the data (such as a hacker) learns about particular identified consumers.

Second, businesses that have made efforts to protect user privacy through the use of non-personally identifiable identifiers could be forced to reengineer systems to make it possible to connect identified users to data connected with those non-personally identifiable identifiers and provide or delete such data in response to CCPA requests. Additionally, companies will have reduced or nonexistent incentives to take the privacy-protective step of using non-personally identifiable identifiers in future products and services if they will ultimately be forced to link those non-personally identifiable identifiers to identified consumers due to CCPA obligations.

Confirming that data identified solely by a non-personally identifiable identifier does not constitute “personal information” would also help to harmonize the CCPA with other key global privacy frameworks, such as the GDPR. The GDPR defines “personal data” to include information that relates to an “identified or identifiable natural person” and would therefore exclude data that is identified solely by a non-personally identifiable identifier.

II. The Importance of Reasonable and Appropriate Security Controls to Safeguard Privacy Rights and Protections Should Be Considered in the Rulemaking

Meaningful privacy protections cannot exist without the underlying support of reasonable and appropriate security controls designed to safeguard consumer privacy rights. Reasonable and appropriate security controls should include those designed to protect personal information on systems and networks and in transit, and also protect personal information from unauthorized or fraudulent access requests. We encourage the Attorney General to consider the role of data security controls in its rulemaking.

For example, given the potentially sensitive nature of the personal information that may be provided in response to a consumer’s CCPA request, it is important to ensure that businesses follow reasonably secure processes in verifying the identity of the person making the request. Under the text of the CCPA, the standards for verification are left to the Attorney General’s rulemaking. While there are many considerations to address in the verification process, we encourage the Attorney General to ensure that the verification requirements will not obligate businesses to collect sensitive information unnecessarily or displace existing reasonably secure verification mechanisms.



Verification standards that focus solely on traditional (generally offline) methods of identity verification, such as government IDs (e.g., driver's licenses), could place additional sensitive consumer information at risk and impose an unnecessary cybersecurity burden on some businesses. Such obligations would also be unnecessary – and could potentially reduce consumer privacy – for businesses that have implemented robust privacy-by-design procedures and designed their systems and processes in a manner that minimizes their collection of sensitive (and other) personal information in the first instance. The burdens imposed by government identifier-focused verification methods would fall particularly hard on small businesses and startups that lack the financial resources needed to implement the information security measures that are necessary to protect sensitive data.

We encourage the Attorney General to codify the use of account-based verifications for personal information requests, which not only avoids the negative impacts imposed by government identifier-based verification but also appears to have been envisioned by the drafters of the CCPA. Today, countless popular services allow consumers to use a username and password to access online accounts that contain sensitive information (e.g., banking, email, medical services). As a result, it would be reasonable to treat CCPA requests made through an account that a user has previously established with the business as being verified, provided that the business maintains reasonable account security procedures. And, the Attorney General rule-making provision discussing the verification rules refers to “treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request.” We agree with the drafters that appropriately secured account-based verification should be a verification method.

III. Conclusion

Apple supports the California Attorney General's efforts to seek broad comment on how best to implement the California Consumer Privacy Act. We applaud California's leadership in recognizing privacy as an individual right and taking legislative steps to protect privacy and provide consumers with meaningful privacy protections and control over their personal information. We encourage the Attorney General to consider the foregoing points in its efforts to help ensure that the goals of the CCPA are met in a way that protects individuals and encourages privacy protective innovations. Doing so will help harness the benefits that individuals' can derive from transparent and respectful use of their data, provide further clarity to the CCPA's requirements, mitigate the risk of unintended negative consequences, and improve the overall effectiveness of the law in protecting consumer privacy.

Message

From: Ari Levenfeld [REDACTED]
Sent: 3/8/2019 4:16:24 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: ATTN: Privacy Regulations Coordinator - Quantcast Comments on CCPA
Attachments: Quantcast Corp Comments - CCPA Rulemaking.docx.pdf

Dear Mr. Becerra,

Quantcast is pleased to share the attached letter detailing our response to your office's request for comments on the implementation of the California Consumer Privacy Act of 2018 (CCPA). We appreciate your office's work, and the time you are taking to gather feedback and different perspectives on rulemaking and implementation for this important California state law.

Best regards,

Ari Levenfeld

Chief Privacy Officer

Quantcast Corp.



795 Folsom St, Floor 5
San Francisco, CA, 94107


quantcast.com

March 8, 2019

VIA ELECTRONIC MAIL

The Honorable Xavier Becerra
Attorney General
CA Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

RE: Implementing Regulations for the California Consumer Privacy Act of 2018

Dear Mr. Becerra:

Quantcast is pleased to share this letter detailing our response to your office's request for comments on the implementation of the California Consumer Privacy Act of 2018 (CCPA).

Overview of Quantcast

Quantcast's mission is to build the audience platform to radically simplify advertising on the open internet. Today Quantcast draws live data from more than 100 million online destinations and applies machine learning to help marketers, publishers, and agencies grow their brands by better understanding and predicting consumer interactions in real-time. Founded in 2006, Quantcast is headquartered in San Francisco and has employees in more than 20 offices across 10 countries.

Quantcast is an active member of industry associations that govern the policies around online consumer privacy in the context of internet-based advertising, including: the Network Advertising Initiative (NAI), the Digital Advertising Alliance (DAA), and the European Interactive Digital Advertising Alliance (EDAA). Quantcast complies with the [NAI Codes of Conduct](#), the [DAA Self-Regulatory Principles](#), and the [EDAA Self-Regulatory Principles](#). We believe that these codes and principles help protect consumer privacy. The self regulatory codes of conduct and principles that third-party advertising companies such as Quantcast have agreed to abide by were founded on the same guiding principles that are at the core of the CCPA, including transparency, choice and accountability, as well as important concepts such as data minimization and privacy by design. Other aspects of the law that align with self-regulatory codes of conduct include requirements that members such as Quantcast provide a mechanism to opt out of interest-based advertising, that we disclose what type of information we collect for interest based advertising and how we use that information. More recently, some large technology companies with first party relationships with users have received attention for their level of commitment to consumer privacy. This does not mean that self-regulation, which is largely applied to

third parties, has failed. The fact that many aspects of the CCPA align with existing self regulatory guidelines that explicitly apply to third parties is a welcome attribute of the law, and something we hope your office will take into consideration.

Part I: Comments on Definitions

A. CCPA implementing rules and regulations should clarify the important differences between “Personal Information”, “Pseudonymous Information”, and “De-identified Information”.

The CCPA includes a definition of “Personal Information”, which further defines many of the compliance requirements of other sections of the law. But not all personal information is the same, and different types of personal information carry different potential risks. The scope of the definition of “Personal Information” which is currently very broad, includes a range of different types of information that may be collected for a variety of uses in different contexts. One category of data within in the current definition of “Personal Information” is data that can reasonably be tied back to a natural person or be so closely associated with a natural person that it should carry with it the obligations imposed by the CCPA. Another category of data that falls within the current definition “Personal Information” does not have the same privacy implications associated with it and businesses may have intentionally chosen to collect it, instead of more intrusive forms of information. Companies make this election to incorporate privacy by design concepts in their products. But they also are reacting to what the market wants, and what the risks are for collecting and using one type of data over another. A powerful way to motivate companies to choose to work with less intrusive pseudonymous information over more more invasive PII is to create stricter standards for compliance when collecting PII. If companies realize that the compliance requirements are more straightforward when only pseudonymous data is collected and used, they will be more likely to only collect that type of information. Thus, it would be beneficial to reflect these distinct categories in the law and in your office’s rulemaking guidance. Doing so will create powerful incentives to minimize the type of data collected by businesses, as the requirements for compliance will be different and less rigorous. This drafting philosophy can be found in well established, existing privacy statutes such as the Federal Health Insurance Portability and Accountability Act of 1996 (HIPPA).

More specifically, as written, the definition of “Personal Information” in its current form does not distinguish between immutable types of information, such as a person’s name or social security number (which are nearly impossible to change) on the one hand, and, on the other, less intrusive information like randomly-generated pseudonymous IDs associated with cookies that may be changed or deleted with relative ease and as often as a consumer wishes.

Because PII, pseudonymous data and de-identified data serve different purposes, are derived differently, and have different risk profiles, they should be separately defined and treated differently under the law.

In addition, the inclusion of “household” as a qualifier to help define what data may be personal information unnecessarily broadens the definition and could reasonably interpreted to include a variety

of data, with associated compliance requirements, which would not serve to improve the data protection or privacy of California residents. We do not believe this was the intention of those who drafted the bill.

Thus, we recommend making the following, underlined changes, including additions and deletions, to the definition of "Personal Information", to establish which type of data are in scope and many of the provisions of the statute should be applied to.

"Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household without the use of additional information. Personal information includes, but is not limited to, the following:

- (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.**
- (B) Any categories of personal information described in subdivision (e) of Section 1798.80.**
- (C) Characteristics of protected classifications under California or federal law.**
- (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.**
- (E) Biometric information.**
- (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.**
- (G) Geolocation data.**
- (H) Audio, electronic, visual, thermal, olfactory, or similar information.**
- (I) Professional or employment-related information.**
- (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).**
- (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.**

Furthermore, we recommend including a definition of "Pseudonymous Information" that captures the distinction between "Personal Information", which should be applied to more privacy invasive data that consumers should be provided with a means for exercising control over, and "De-identified Information" which is a very high standard that is impractical for commercial purposes. Because the CCPA does not currently define "Pseudonymous Information", it forces the CCPA to improperly classify a wide spectrum of information into definitions that do not fit either "Personal Information" or "De-Identified Information". The absence of a pseudonymous data category also means that the CCPA does not reflect the reality of today's digital landscape. Pseudonymous data, which is not derived from PII, is used to inform digital communication and transactions, but is not necessarily the subject of those

transactions. In those cases, consideration is not provided in exchange for such pseudonymous data. Importantly, the failure to distinguish between personally identifiable information ("PII") and pseudonymous information misses an opportunity to incentivize companies to use the least data they need to achieve business goals. We propose that the definitions of "Personal Information" suggested above and "De-Identified Information" suggested below, be amended as well, and that a third definition, "Pseudonymous Information" be introduced. Said another way, refining the current definitions and adding the term "Pseudonymous Information" would incentivize businesses to create an important rationale for companies to make, or continue to make, privacy friendly choices and incorporate privacy by design principles by relying on pseudonymous data rather than personally identifiable information.

Thus, we recommend including the following, new definition of "Pseudonymous Information":

"Pseudonymous Information" means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

(A) "Pseudonymization" can reduce the risk of harm to consumers by removing the likelihood that an inference or decision may be made permanent.

(B) "Pseudonymization" may facilitate the processing of personal information beyond the original collection purposes without posing potential risks or harms to the consumer.

(C) "Pseudonymization" is an important safeguard for processing personal data for scientific, historical and statistical purposes.

(D) "Pseudonymization" is a central feature of "data protection by design."

Finally, the definition of "Deidentified" should be modified to align with the amended definitions of "Personal Information" and the inclusion of a "Pseudonymous Information" definition. Companies usually obtain personally identifiable information directly from individuals. With PII, there isn't any other information one needs to identify an actual person. Similarly, companies often obtain the data underlying de-identified data directly from customers and then strip that data of PII. Truly de-identifying data is, however difficult because a company must ensure that no other data may reasonably intermingle with other information collected. So, the standard for true de-identification is nearly impossible to achieve, and is effectively impossible if more than one piece of information is cross referenced with enough of another type of information. Thus, deidentification is not an effective standard to include in the CCPA as the difficulty in achieving its standard does not create a reasonably attainable standard for commercial interests. Thus, we suggest this amended definition of "Deidentification" which narrows the scope so it is referring to "personal information".

"Deidentified" means personal information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

- (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.**
- (2) Has implemented business processes that specifically prohibit reidentification of the information.**

March 8, 2019

Error! AutoText entry not defined.

(3) Has implemented business processes to prevent inadvertent release of deidentified information.

(4) Makes no attempt to reidentify the information.

B. Regulatory language should be revised so that the definitions of “personal information” and “deidentified” as well as the newly included “pseudonymous information” may be applied.

Note that both the amended definition of “Personal Information” and “deidentified” Information, as well as the inclusion of a “Pseudonymous Information” definition, are directly related to the concept of how, and what type of information may be associated with an identifiable individual. To capture the range of possible outcomes depending on which definition information falls into, we propose the following change to other regulatory language:

For purposes of paragraph (1) of subdivision (o) of Section 1798.140 of the Act, information shall not constitute “personal information” where such information is deidentified or is aggregate consumer information.

A. Regulations should include a definition for pseudonymous data, which may be used to incentivize companies to collect less privacy intrusive data

B. Regulations implementing CCPA should clarify that the definition of “sale” applies only when the purpose of a transaction is the exchange of personal information for consideration.

Today’s digital economy relies on data flows of all kinds. The structure of the Internet requires the transmission and receipt of data about web browsers, devices, and networks that arguably are Personal Information under CCPA’s broad definition of the term. These data flows are critical for many functions of the Internet, and are often, but not always, governed by commercial contracts. Even where these exchanges are structured around contracts, they are not accurately characterized as sales of data. Instead, while the information provides context for a transaction, it is merely tangential to it.

Like almost all web-based Internet activity, selecting and serving advertisements using Interest-Based Advertising (IBA) involves the transmission of information like IP addresses, user-agent strings, and pseudonymous IDs associated with cookies. However, the economic reality of IBA is that it involves the sale of ad space, and not the sale information. In marketplaces that serve the digital ad industry, which support the free content we enjoy, data is often used to inform a transaction even when it is not the subject of the transaction and is merely tangential.

C. The definition of “Sale” under the law should be modified to reflect instances where personal information is exchanged for consideration, and not in cases where it is merely used to inform a transaction or facilitate communication.

We agree that, consistent with Article 1 of California’s State Constitution, consumers should understand how, why, and when their information is sold. Data resellers should be held to the same standard as the original data seller. Consumers also should have a right to exercise control over the sale of their

information. However, a large amount of information used merely to facilitate transactions is not sold but under the current definition would improperly be subject to restrictions.

Indeed, the current definition goes beyond what the common understanding of sale is and extends to any exchange of personal information. This definition has adverse and likely unintended consequences on the way that computers and the Internet function. For example, companies use information to communicate effectively with one another, and conduct media transactions. The marketplaces that websites rely on to sell advertising, and thus fund free content, rely on the exchange of pseudonymous information - not PII - to function. This practice should be treated differently than transactions where personal information is explicitly bought and sold by data brokers for monetary consideration. Similarly, our devices rely on a constant exchange of information in order to function. For example, rendering bits of information into readable text on screen. Making that exchange of information subject to the current definition of sale would introduce unnecessary friction in providing valuable content, products and services that consumers need. Therefore, we believe that the definition of "sale" should change to reflect the way that all technology operates.

Thus, we recommend making the following, underlined changes to the definition of sale, to capture instances where personal information is being directly exchanged for consideration, rather than being used to inform a particular transaction or in the course of electronic communication between businesses.

(1) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration directly for the receipt of personal information.

(2) For purposes of this title, a business does not sell personal information when:

[...](A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.

(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purposes if both of the following conditions are met: services that the service provider performs on the business' behalf or another service provider's behalf related to the services, provided that the service provider also does not sell the personal information.

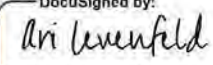
[...]

- (i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.
- (ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.
- (D) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business provided that information is used or shared consistently with Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

We appreciate your time and consideration in reviewing our feedback and suggestions as part of this rulemaking process.

Respectfully Submitted,

Quantcast Corporation

DocuSigned by:
BY: 
B501540DD92A460

Ari Levenfeld

Chief Privacy Officer

Message

From: Mary Ross [REDACTED]
Sent: 3/7/2019 11:40:38 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: ATTN: Privacy Regulations Coordinator
Attachments: AG Listening Comments v.1.docx; MSR Edits to SB 1121.docx

Hi--

I am attaching my comments to SB 1121 as well as a copy of the remarks I delivered at the open forum at Stanford on Tuesday. I was a co-author and a proponent of the original initiative, however, I am no longer affiliated with Californians for Consumer Privacy.

Please let me know if you have questions. I'm truly happy to help.

All the best,
Mary

Mary Stone Ross
Principal
MSR Strategies
[REDACTED]

CONFIDENTIALITY NOTICE: This electronic mail transmission may contain privileged and/or confidential information only for use by the intended recipients. Unless you are the addressee (or authorized to receive messages for the addressee), you may not use, copy, disclose, or distribute this message (or any information contained in or attached to it) to anyone. You may be subject to civil action and/or criminal penalties for violation of this restriction. If you received this transmission in error, please notify the sender by reply e-mail and delete the transmission. Thank you.

Hello. My name is Mary Stone Ross. I was one of the original proponents of the initiative that became the CCPA and formerly president of Californians for Consumer Privacy. I am no longer a part of that group, however, and my comments today are my own.

I am here today to remind Attorney General Becerra and his office of our original intent inspiring the initiative—to give all Californians meaningful transparency into what personal information businesses are collecting about them and their devices and—unlike current privacy laws—make sure that the law could be enforced.

As you are aware, the Right to Privacy is a fundamental right protected by the California constitution and the state has a clear interest in protecting the privacy rights of its citizens. Today, businesses can state their policies in vague terms, change them more or less at will and offer very little, if any privacy protections to consumers. The CCPA will change this and shift the balance of power more equally towards consumers, but there are ways that your office can make the protections even stronger.

Transparency--The Right to Know in the CCPA—is the cornerstone of the entire law. A consumer can only truly consent to the collection, use and the sale of their personal information—including the terms of service and privacy policies they readily click to agree to—if they understand what information is being collected. For example, if a flashlight app is in fact collecting precise geographic location that

should be clearly disclosed. Thus, the burden on consumers to make a verifiable request should be as low as possible.

I think that there should be two standards of verifiable requests—one if a consumer is only requesting the categories of information a business is collecting, and a second, higher standard, if a consumer is requesting the specific pieces of personal information. It should be as easy as possible for a consumer to request the categories of information. It should also be legally clear that a consumer can exercise their right to know the categories of personal information without finding out the specific pieces. From a consumer privacy standpoint, it does make sense to have a much higher standard of verifiable request if a consumer is requesting the specific pieces of personal information. Further, since many businesses that do not have a direct relationship with a consumer still collect that consumer's personal information, a consumer should be allowed to authorize a third party—including a non-profit or another business—to opt out of the sale of their personal information on their behalf.

Definitions are critical. I agree with some of the criticisms of the CCPA that “household” is a vague and ill defined term. However, it is necessary that a consumer be allowed to find out what personal information a business collects about their devices since, for example, my cell phone and watch travel with me everywhere and—from a data collection standpoint—are essentially me. I advise that the definition of personal information is changed to delete references

to “households” and go back to the original reference of “individual consumer or device.”

We wanted to create a living law that could be updated as technologies changed—the lack of which was a failing in past privacy regulations. There is therefore a thoughtful burden on the AG’s office to continuously add to the categories of personal information. For starters, I would advise that “psychometric information” is added back to the categories of personal information, as defined by the initiative. As evidenced by the Cambridge Analytica scandal, this is clearly a category that consumers need to know.

Enforcement is key. I agree with the concerns raised by your office that the Attorney General alone is not well positioned to be the sole enforcer of such a broad act. I encourage your office to work with Sacramento to allow, like the original initiative, enforcement by any district attorney or by any county counsel, city attorney or city prosecutor whose city or county meets certain population thresholds.

As written, the non-discrimination provision is a mess and, in effect, is a non non-discrimination provision. I encourage your office to work with Sacramento and come up with guidelines on when a consumer can sell their personal information, with the understanding that privacy is not a commodity that only the wealthy should be able to afford. Consumers are in a position of relative dependence with respect to the technologies and many of the apps that we use. Businesses have considerable expertise and knowledge about the

value and uses of our data. Therefore, in order for the consumer to give meaningful consent, the business should have the burden to clearly define the value provided to the business by the consumer's data.

Finally, I want to remind all interested parties that privacy is good for business. When we drafted the initiative, we wanted to encourage businesses to comply—one of the reasons why we decided to not regulate the collection of personal information—as this too is a win for consumers. I urge you to make your guidelines as clear as possible to ease the burden of compliance.

Thank you.

Senate Bill No. 1121

CHAPTER 735

An act to amend Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.185, 1798.192, 1798.196, and 1798.198 of, and to add Section 1798.199 to, the Civil Code, relating to personal information, and declaring the urgency thereof, to take effect immediately.

[Approved by Governor September 23, 2018. Filed with Secretary of State September 23, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

SB 1121, Dodd. California Consumer Privacy Act of 2018.

(1) Existing law, the California Consumer Privacy Act of 2018, grants, commencing on January 1, 2020, a consumer various rights with regard to personal information relating to that consumer that is held by a business, including the right to request a business to delete any personal information about the consumer collected by the business, and requires the business to comply with a verifiable consumer request to that effect, unless it is necessary for the business or service provider to maintain the customer's personal information in order to carry out specified acts. The act requires a business that collects personal information about a consumer to disclose the consumer's right to delete personal information described above on its Internet Web site or in its online privacy policy or policies.

This bill would modify that requirement by requiring a business that collects personal information about a consumer to disclose the consumer's right to delete personal information in a form that is reasonably accessible to consumers and in accordance with a specified process.

(2) The act establishes several exceptions to the requirements imposed, and rights granted, by the act, including prohibiting the act from being interpreted to restrict the ability of a business to comply with federal, state, or local laws, and by providing that the act does not apply if it is in conflict with the California Constitution.

This bill would provide that the rights afforded to consumers and the obligations imposed on any business under the act does not apply if those rights or obligations would infringe on the noncommercial activities of people and entities described in a specified provision of the California Constitution addressing activities related to newspapers and periodicals. The bill would also prohibit application of the act to personal information collected, processed, sold, or disclosed pursuant to a specified federal law relating to banks, brokerages, insurance companies, and credit reporting agencies, among others, and would also except application of the act to that information pursuant to the California Financial Information Privacy Act. The bill would provide that these

exceptions, and the exception provided to information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994, do not apply to specific provisions of the act related to unauthorized theft and disclosure of information. The bill would revise and expand the exception provided for medical information, would except a provider of health care or a covered entity, and would also except information collected as part of clinical trials, as specified. The bill would also clarify that the act does not apply if it is in conflict with the United States Constitution.

(3) The act generally provides for its enforcement by the Attorney General, but also provides for a private right of action in connection with certain unauthorized access and exfiltration, theft, or disclosure of a consumer's nonencrypted or nonredacted personal information, as defined for this purpose, provided that the consumer bringing an action notify the Attorney General of the action in accordance with a specified process. The act provides that a business, service provider, or other person who violates its provisions, and fails to cure those violations within 30 days, is liable for a civil penalty under laws relating to unfair competition in an action to be brought by the Attorney General. The act prescribes a formula for allocating civil penalties and settlements assessed in these actions with 80% to be allocated to the jurisdictions of the behalf of which the action was brought.

This bill would clarify that the only private right of action permitted under the act is the private right of action described above for violations of unauthorized access and exfiltration, theft, or disclosure of a consumer's nonencrypted or nonredacted personal information and would delete the requirement that a consumer bringing a private right of action notify the Attorney General. The bill would remove references to laws relating to unfair competition in connection with Attorney General actions described above. The bill would limit the civil penalty to be assessed in an Attorney General action in this context to not more than \$2,500 per violation or \$7,500 per each intentional violation and would specify that an injunction is also available as remedy. The bill would eliminate the formula for allocating penalties and settlements and would instead provide that all of these moneys be deposited in the Consumer Privacy Fund with the intent to offset costs incurred by the courts and the Attorney General in connection with the act. The bill would also revise timelines and requirements regarding the promulgation of regulations by the Attorney General in connection with the act.

(4) The act makes its provisions operative on January 1, 2020, provided a specified contingency is satisfied. Provisions of the act supersede and preempt laws adopted by local entities regarding the collection and sale of a consumer's personal information by a business.

This bill would make the provisions of the act that supersede and preempt laws adopted by local entities, as described above, operative on the date the bill becomes effective.

(5) This bill would also make various technical and clarifying changes to the act.

(6) This bill would declare that it is to take effect immediately as an urgency statute.

DIGEST KEY

Vote: 2/3 Appropriation: no Fiscal Committee: yes Local Program: no

BILL TEXT

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS
FOLLOWS:

SECTION 1.

Section 1798.100 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.100.

(a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

(b) A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.

(d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered—per the consumer's preference— by mail or electronically, and if provided electronically or delivered by mail, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

(e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

SEC. 2.

Section 1798.105 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.105.

(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

(c) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.

(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

(6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(8) Comply with a legal obligation.

(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

SEC. 3.

Section 1798.110 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.110.

(a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer any or all of the following:

(1) The categories of personal information it has collected about that consumer.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) The specific pieces of personal information it has collected about that consumer.

(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer.

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The categories of personal information it has collected about ~~that~~ consumers.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) The specific pieces of personal information the business has collected about that consumer.

(d) This section does not require a business to do the following:

(1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.

(2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

SEC. 4.

Section 1798.115 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.115.

(a) A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

(1) The categories of personal information that the business collected about the consumer.

(2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose.

(b) A business that sells personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to paragraph (4) of

subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

(c) A business that sells consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The category or categories of consumers' personal information it has sold, or if the business has not sold consumers' personal information, it shall disclose that fact.

(2) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.

SEC. 5.

Section 1798.120 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.120.

(a) A consumer or a person authorized by the consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out.

(b) A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt-in."

(d) A business that has received direction from a consumer or a person authorized by the consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited, pursuant to paragraph (4) of subdivision (a) of Section 1798.135, from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.

SEC. 6.

Section 1798.125 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.125.

(a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under ~~this title~~ 1798.100, 1798.110 or 1798.115, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data.

(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer-business by the consumer's data.

(2) A business that offers any financial incentives pursuant to subdivision (a), shall notify consumers of the financial incentives pursuant to Section 1798.135 and shall clearly define the value provided to the business by the consumer's data.

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.135 which clearly describes the material terms of the financial incentive program, the value provided to the business by the consumer's data, and which may be revoked by the consumer at any time.

(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

SEC. 7.

Section 1798.130 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.130.

(a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.

(2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business's duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business's receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business shall not require the consumer to create an account with the business in order to make a verifiable consumer request.

(3) For purposes of subdivision (b) of Section 1798.110:

(A) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its Internet Web site, and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.

(B) For purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact.

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Sections 1798.110, 1798.115, 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business's verification of the consumer's request solely for the purposes of verification.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.110 and 1798.115 shall follow the definition of personal information in Section 1798.140.

SEC. 8.

Section 1798.135 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.135.

(a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

(2) Include a description of a consumer's rights pursuant to Section 1798.120, along with a separate link to the "Do Not Sell My Personal Information" Internet Web page in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers' privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer.

(5) For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information.

(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(b) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

(c) A consumer may authorize another person solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General.

SEC. 9.

Section 1798.140 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.140.

For purposes of this title:

(a) "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

(b) "Biometric information" means an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a

faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) "Business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) Has annual gross revenues in excess of twenty-five million dollars (\$25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark.

(d) "Business purpose" means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.

(5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.

(6) Undertaking internal research for technological development and demonstration.

(7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

(e) "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving

information from the consumer, either actively or passively, or by observing the consumer's behavior.

(f) "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. "Commercial purposes" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

(g) "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

(h) "Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(2) Has implemented business processes that specifically prohibit reidentification of the information.

(3) Has implemented business processes to prevent inadvertent release of deidentified information.

(4) Makes no attempt to reidentify the information.

(i) "Designated methods for submitting requests" means a mailing address, email address, Internet Web page, Internet Web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

(j) "Device" means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.

(k) "Health insurance information" means a consumer's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer's application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.

(l) "Homepage" means the introductory page of an Internet Web site and any Internet Web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information," or settings page, and any other location that allows consumers to review the notice required by subdivision (a) of Section 1798.145, including, but not limited to, before downloading the application.

(m) "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(n) "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(o) (1) "Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

Psychometric information

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(2) "Personal information" does not include publicly available information. For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. "Publicly available" does not include consumer information that is deidentified or aggregate consumer information.

(p) "Probabilistic identifier" means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(q) "Processing" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.

(r) "Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(s) "Research" means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes shall be:

(1) Compatible with the business purpose for which the personal information was collected.

(2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

- (4) Subject to business processes that specifically prohibit reidentification of the information.
- (5) Made subject to business processes to prevent inadvertent release of deidentified information.
- (6) Protected from any reidentification attempts.
- (7) Used solely for research purposes that are compatible with the context in which the personal information was collected.
- (8) Not be used for any commercial purpose.
- (9) Subjected by the business conducting the research to additional security controls limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.
- (t) (1) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.
- (2) For purposes of this title, a business does not sell personal information when:
 - (A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.
 - (B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.
 - (C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:
 - (i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.
 - (ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.
 - (D) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).
- (u) "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.
- (v) "Service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise

permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

(w) "Third party" means a person who is not any of the following:

(1) The business that collects personal information from consumers under this title.

(2) (A) A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:

(i) Prohibits the person receiving the personal information from:

(I) Selling the personal information.

(II) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.

(III) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

(ii) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

(B) A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.

(x) "Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

(y) "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

SEC. 10.

Section 1798.145 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.145.

(a) The obligations imposed on businesses by this title shall not restrict a business's ability to:

(1) Comply with federal, state, or local laws.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(4) Exercise or defend legal claims.

(5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.

(6) Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

(b) The obligations imposed on businesses by Sections 1798.110 to 1798.135, inclusive, shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c) (1) This title shall not apply to any of the following:

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

(2) For purposes of this subdivision, the definitions of "medical information" and "provider of health care" in Section 56.05 shall apply and the definitions of "business associate," "covered entity," and "protected health information" in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) This title shall not apply to the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined by subdivision (d) of Section 1681a of Title 15 of the United States Code, and use of that information is limited by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

(e) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code). This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This subdivision shall not apply to Section 1798.150.

(g) Notwithstanding a business's obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to any verified consumer request may be extended by up to 90 additional days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.

(h) A business that discloses personal information to a service provider shall not be liable under this title if the service provider receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title.

(i) This title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(j) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.

(k) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.

SEC. 11.

Section 1798.150 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.150.

(a) (1) Any consumer whose nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the

misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(b) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

(c) The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

SEC. 12.

Section 1798.155 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.155.

(a) Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title.

(b) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars (\$2,500) for each violation or seven thousand five hundred dollars (\$7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.

(c) Any civil penalty assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (b), shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with this title.

SEC. 13.

Section 1798.185 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.185.

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

(1) Updating as needed additional categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (o) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Updating as needed the definition of unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and additional categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to Section 1798.130.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.

(4) Establishing rules and procedures for the following:

(A) To facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information pursuant to paragraph (1) of subdivision (a) of Section 1798.145.

(B) To govern business compliance with a consumer's opt-out request.

(C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

(5) Adjusting the monetary threshold in subparagraph (A) of paragraph (1) of subdivision (c) of Section 1798.140 in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter.

(7) Establishing rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received by a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

(b) The Attorney General may adopt additional regulations as necessary to further the purposes of this title.

(c) The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.

SEC. 14.

Section 1798.192 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.192.

Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt-out of a business's sale of the consumer's personal information, or authorizing a business to sell the consumer's personal information after previously opting out.

SEC. 15.

Section 1798.196 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.196.

This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.

SEC. 16.

Section 1798.198 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.198.

(a) Subject to limitation provided in subdivision (b), and in Section 1798.199, this title shall be operative January 1, 2020.

(b) This title shall become operative only if initiative measure No. 17-0039, The Consumer Right to Privacy Act of 2018, is withdrawn from the ballot pursuant to Section 9604 of the Elections Code.

SEC. 17.

Section 1798.199 is added to the Civil Code, to read:

1798.199.

Notwithstanding Section 1798.198, Section 1798.180 shall be operative on the effective date of the act adding this section.

SEC. 18.

This act is an urgency statute necessary for the immediate preservation of the public peace, health, or safety within the meaning of Article IV of the California Constitution and shall go into immediate effect. The facts constituting the necessity are:

In order to prevent the confusion created by the enactment of conflicting local laws regarding the collection and sale of personal information, it is necessary that this act take immediate effect.

Message

From: Angelena Bradfield [REDACTED]
Sent: 3/8/2019 2:55:03 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: BPI comments on CCPA
Attachments: BPI Pre-Rulemaking Comments concerning the CCPA.pdf

Hello:

Please find attached a letter from the Bank Policy Institute (BPI) responding to the California Attorney General's request for preliminary rulemaking comments on implementing the California Consumer Privacy Act.

We appreciate your consideration of our comments. Please don't hesitate to reach out to me with any questions.

Sincerely,

Angelena

Angelena Bradfield

Vice President, AML/BSA, Sanctions & Privacy



www.bpi.com





March 8, 2019

Via Electronic Mail

California Department of Justice
Attn: Privacy Regulations Coordinator
300 South Spring Street
Los Angeles, CA 90013

Re: Preliminary Rulemaking Request for Comment concerning the California Consumer Privacy Act

Ladies and Gentlemen:

The Bank Policy Institute¹ appreciates the opportunity to respond to the California Attorney General's request for preliminary rulemaking comments on implementing the California Consumer Privacy Act ("CCPA").² BPI member banks are dedicated to protecting customer data and have adopted robust privacy and information security programs with administrative, technical, and physical safeguards to assist in such efforts. These programs are designed pursuant to and consistent with the requirements of state, federal and international laws – notably the Gramm-Leach-Bliley Act ("GLBA") and its implementing regulations.³ Therefore, BPI member banks already adhere to notice and disclosure requirements, protect the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of customer information, and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to customers.⁴ These programs are tailored to the size, complexity, activity, and overall risk profile of a bank as contemplated under federal law.⁵

¹ The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

² Cal. Civ. Code § 1798.100 *et seq.*

³ 15 U.S.C. §§ 6800 *et seq.* and implementing regulations.

⁴ As noted by President Clinton, the GLBA requires banks to "clearly disclose their privacy policies to customers up front...consumers will have an absolute right to know if their financial institution intends to share or sell their personal financial data, either within the corporate family or with an unaffiliated third-party [and]...will have the right to "opt out" of such information sharing with unaffiliated third parties...[and] allows privacy protection to be included in regular bank examinations...[and] grants regulators full authority to issue privacy rules and to use the full range of their enforcement powers in case of violations." See William J. Clinton, Statement on Signing the Gramm-Leach-Bliley Act, November 1999. Available at web.archive.org/web/20160322081604/http://www.presidency.ucsb.edu/ws/?pid=56922; accessed March 1, 2019.

⁵ Interagency Guidelines, 12 C.F.R. pt. 30, app. B, § II.A.

As an initial matter, data transparency is inherent in a bank's business model. Banks provide customers with account information through statements or other written notices, online services, mobile banking applications, and other tools that allow customers direct access to categories of information the bank collects on them. In addition, financial institutions provide disclosures to their customers and the general public that detail the categories and types of data they collect, the ways in which it is used, and how to further inquire about collected information.⁶

Banks use a wide range of physical and technical safeguards regarding the collection, storage, use, access, and delivery of information, including physical access restrictions, firewalls, intrusion detection and threat monitoring tools, and encryption technologies. These safeguards are carefully tailored to reflect the scope of individual bank activities and the sensitivity of the personal information collected and stored. Furthermore, bank GLBA-compliant privacy programs are tested and continually updated and subject to evaluation and review by compliance, IT and internal audit professionals as well as executive management and boards of directors. Finally, both in scale and scope and in terms of the already existing regulatory framework, such programs are also subject to exams conducted by federal and state regulators.

Given the extensive privacy and data security programs banks already employ, which differ from those utilized by other sectors of the economy, it is important that any rulemaking undertaken by the California Attorney General recognize and align with these long-standing and effective frameworks in the financial institution space.⁷ This is particularly important when determining the law's implementation date and further clarifying the definition of covered information.

I. Any rule should focus on protecting information that a customer provides to a business in their personal capacity, consistent with the CCPA's legislative intent, and account for the robust privacy frameworks financial institutions already have in place.

Both the preamble to the CCPA and its legislative history make clear that the purpose of the law is to protect information relating to a consumer's relationship with a business for personal, family or household purposes. As noted in the preamble, "[m]any businesses collect personal information from California consumers. They may know where a consumer lives and how many children a consumer has, how fast a consumer drives, a consumer's personality, sleep habits, biometric and health information, financial information, precise geolocation information, and social networks...California consumers should be able to exercise control over their personal information, and they want to be certain that there are safeguards against misuse of their personal information." This focus is reinforced by the law's definition of personal information which is tied to the ability to reasonably link data to "a particular consumer or household,"⁸ as well as the law's focus on the rights a customer has to understand how a business collects and uses its information.

Such expectations should be made clear through the rulemaking process in order to clarify that data collected outside of the interaction a customer has with a business in their personal capacity, notably through commercial and other relationships, is not covered by the law given its broad definitions of consumer and personal information. Ensuring clarity on this point is particularly important in the context of the definition of personal information as presently it could be, albeit inappropriately, read to grant members of a consumer's household rights intended for only an individual consumer – including information access, disclosure and deletion rights. Such a result

⁶ Under the GLBA, financial institutions must provide notice of its privacy policies and practices, and in certain circumstances, allow the consumer to opt out of the disclosure of its nonpublic personal information to affiliates and nonaffiliated third parties. 15 U.S.C. § 6802(b). We note that covered financial institutions are also required to obtain consent prior to sharing information with nonaffiliated parties under the California Financial Information Privacy Act.

⁷ Indeed, the CCPA acknowledges the strength of this federal framework in Section 1798.145(e).

⁸ Section 1798.140(o)(1).

would clearly be inconsistent with the legislative intent of the CCPA and therefore should be further clarified in any rulemaking.

In addition, as presently drafted, the CCPA could be read to capture data collected outside of the relationship a business has with a consumer, like employee, contractor, or job applicant data. Employee information is already covered by state and federal laws that govern its protection and confidentiality. For example, it is subject to the Health Insurance Portability and Accountability Act ("HIPAA"), which protects health-related data, and California's breach notification laws⁹ which protects such data from unauthorized disclosure and affords substantial protections to that data. Furthermore, as described above, such relationships appear to be outside the scope of the legislative intent of the law. The CCPA contemplates this and similar circumstances by providing the Attorney General with the authority to "[e]stablish[] any exceptions necessary to comply with state or federal law including, but not limited to, those relating to trade secrets and intellectual property rights within one year of passage of this title and as needed thereafter."¹⁰ Therefore, given the protections already afforded this information and the Attorney General's clear statutory authority to exempt such information from being covered by the CCPA, we strongly recommend that any rulemaking defer to the privacy frameworks that banks already have in place for safeguarding employee information.

II. CCPA compliance requirements and enforcement activity should commence 12 months after regulatory standards are finalized.

As acknowledged by Attorney General Becerra in his August 22, 2018 letter to members of the California legislature, the promulgation of regulations requires a "sufficient and realistic amount of time" for rulemaking to be conducted.¹¹ The same is true for companies subject to such regulations, as they will have to review their existing processes against the requirements of the law and any implementing regulations, develop plans to adapt their programs – both technologically and administratively – to address new or different expectations, and test those new processes prior to implementing the revised program. This analysis is further complicated by a consumer's right to request from a business "categories and specific pieces of personal information the business has collected," and once the request has been verified, the obligation of the business to disclose the personal information collected in the preceding 12 months.¹² As the CCPA's effective date is January 1, 2020, and the deadline for rulemaking is July 1, 2020, there is ambiguity as to when businesses need to be in compliance with the law, much less its 12-month look-back period. Given the operational components banks will be required to put in place to address the Attorney General's regulations, a transitional implementation period of a minimum of 12 months ("implementation date") should be provided to firms to establish and test compliance procedures that reflect the regulations promulgated under the statute. Furthermore, any "look back" requirements and enforcement activity should commence upon the implementation date of the CCPA's regulations. This approach is not unprecedented, the federal government has set similar precedents on data subject to "look back" and enforcement provisions.¹³

* * * * *

⁹ Cal. Civ. Code §§ 1798.82 and 1798.84.

¹⁰ Section 1798.185(a)(3).

¹¹ Letter from Attorney General Xavier Becerra re "California Consumer Privacy Act," August 22, 2018. *Available at* digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2801&context=historical; accessed March 1, 2019.

¹² Section 1798.100(a) and 1798.130(a)(2).

¹³ For example, in 2016, the Financial Crimes Enforcement Network chose not to require identification of beneficial owners on a "look back" basis, prior to the May 11, 2018 implementation date of its Customer Due Diligence rule as it felt it would be "unduly burdensome" due to the "significant changes to processes and systems that [covered institutions were] required to implement" under the rule. *See* 81 Fed. Reg. at 29, 404.

The Bank Policy Institute appreciates the opportunity to submit preliminary rulemaking comments concerning the CCPA. If you have any questions, please contact the undersigned by phone at [REDACTED] or by email at [REDACTED]

Respectfully submitted,

A handwritten signature in cursive script that reads "Angelena Bradfield".

Angelena Bradfield
Vice President, AML/BSA, Sanctions & Privacy
Bank Policy Institute

Message

From: Shelton Leipzig, Dominique (Perkins Coie) [REDACTED]
Sent: 3/8/2019 5:39:17 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Boot, Sarah [REDACTED]; Amlani, Natasha (Perkins Coie) [REDACTED]; Ratican, Sari (Perkins Coie) [REDACTED]
Subject: California Chamber of Commerce's Comments on Rulemaking Re: The California Consumer Privacy Act
Attachments: California Chamber of Commerce - CCPA Rulemaking Comments 03-08-2019.pdf

To the Office of the Attorney General:

On behalf of the California Chamber of Commerce ("CalChamber"), please find attached a report containing the CalChamber's comments regarding the California Consumer Privacy Act. Note that attached to the report, we have excerpted all of the CalChamber's regulatory proposals into an appendix for your convenience. If helpful, we would be happy to provide a word version of the appendix.

We wish to thank the Office of the Attorney General for giving the public this opportunity to comment and participate in the process.

With very best regards,

Dominique

Dominique Shelton Leipzig | Perkins Coie LLP

PARTNER PRIVACY & SECURITY

CO-CHAIR AD TECH PRIVACY & DATA MANAGEMENT

1888 Century Park East Suite 1700

Los Angeles, CA 90067-1721



NOTICE: This communication may contain privileged or other confidential information. If you have received it in error, please advise the sender by reply email and immediately delete the message and any attachments without copying or disclosing the contents. Thank you.



California Chamber of Commerce Comments to the California Attorney General's Office for CCPA Rulemaking March 8, 2019

SARAH BOOT

POLICY ADVOCATE

DOMINIQUE SHELTON LEIPZIG

PARTNER

SARI RATCAN

SENIOR COUNSEL

NATASHA AMLANI

ASSOCIATE

Executive Summary

The California Chamber of Commerce (“CalChamber”) submits this Report to the California Attorney General’s (“AG”) office as part of the AG’s rulemaking process for the California Consumer Privacy Act (“CCPA”). The observations in this Report are designed primarily to clarify existing law under the CCPA. CalChamber is cognizant of the AG’s February 25, 2019 press release¹ accompanying the introduction of SB 561² expressing the need to focus efforts on efficient enforcement strategies. Consistent with this goal, CalChamber offers these comments to render enforcement of the CCPA as efficient as possible for the AG, California consumers, and CalChamber members by clarifying existing law under the CCPA to avoid needless litigation and complaints regarding issues that are clearly articulated within the statute or for which there is no a dispute between businesses and consumers. Accordingly, the comments here are offered to assist consumers, regulators, and businesses develop a common parlance vis-a-vis the CCPA.

Each comment is presented separately in four parts: (1) the header which synthesizes the issue or concern with the current law, (2) the text and citation to the relevant CCPA section, (3) an illustrative use case to demonstrate the issue or concern with the current law, and (4) proposed regulatory language to solve or mitigate the issue or concern raised.

Perkins Coie organized CalChamber’s comments into the Section 1798.185 AG rulemaking mandates to address the following issues:

- **Update the categories of personal information:** Requesting clarification that: (1) forcing businesses to comply with consumer rights requests relating to household or device data, could easily cause other consumers’ personal information from within a shared household or device to be exposed; (2) the definition of personal information will exclude information not “reasonably” capable of being associated with a consumer; (3) pseudonymous information is not reasonably linkable to individual consumers and that businesses are not required to re-link pseudonymized information to comply with a consumer request; and (4) the definition of deidentified information should include recognized deidentification practices.
- **Establish exceptions to comply with state or federal law:** Requesting clarification that: responding to a consumer’s request does not require the business to expose its protected intellectual property. Requesting expansion of: (1) the fraud exemption to include many proactive fraud prevention programs that businesses currently undertake; and (2) the “publicly available information” definition beyond the use of government records “compatible with the purposes for which it is maintained.”
- **Establish rules and procedures:** Requesting the promulgation of rules and procedures relating to: (1) consumers’ opt-out rights; (2) the submission of consumer opt-out requests; and (3) use of a recognizable and uniform opt-out logo or button.

¹ Press Release, Office of California Attorney General, Attorney General Becerra, Senator Jackson Introduce Legislation to Strengthen, Clarify California Consumer Privacy Act (Feb. 25, 2019) <https://oag.ca.gov/news/press-releases/attorney-general-becerra-senator-jackson-introduce-legislation-strengthen>.

² S.B. 561, 2019-2020 Leg. Reg. Sess. (Cal. 2019), http://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201920200SB561

- **Establish rules, procedures, and exceptions:** Requesting the promulgation of rules, notices, and information regarding (1) financial incentive offerings; and (2) verifying consumer requests.

All matters are important, but of significant importance are the following issues below, each shaded pink in the text of the report:

Section	Title
I.A	Issue: Literal adherence to the CCPA would require businesses to respond to consumer rights requests by providing personal information about an entire household or device, thereby reducing privacy protections
VI.A	Issue: CCPA clearly states that January 1, 2020 is the effective date; therefore, the 12-month lookback period should not be misinterpreted by consumers or regulators to begin prior to the effective date
VI.I	Issue: Reasonable Security and Private Right of Action



Name: **Sarah Boot**

Title: **California Chamber of Commerce,
Policy Advocate**

Date: **March 8, 2019**

Biographies



SARAH BOOT | POLICY ADVOCATE | CAL CHAMBER

<https://advocacy.calchamber.com/bios/sarah-boot/>

Sarah R. Boot joined the California Chamber of Commerce staff in March 2018 as a policy advocate specializing in privacy/technology, telecommunications, economic development, and taxation issues.

From August 2015 until joining CalChamber, Boot was a top adviser to now-Senate President Pro Tem Toni G. Atkins. Boot served as the senator's legislative director and also acted as lead staffer on legal, privacy, telecommunications, business, and technology issues, among many others.

Boot was principal consultant to Atkins during her time as Assembly Speaker and Speaker Emeritus, spearheading a working group to draft multiple human trafficking bills and acting as lead staffer on all women-focused legislation, as well as liaison to the Legislative Women's Caucus.

Before working for Atkins, Boot practiced law in San Diego for seven years. Boot served for three years as an assistant U.S. attorney for the General Crimes Unit of the U.S. Attorney's Office, Southern District of California. She prosecuted a broad array of federal crimes, including bank robbery, sex trafficking of minors, and narcotics trafficking.

In private practice, Boot spent three years litigating cases for Cooley LLP, an AmLaw Top 50 international law firm. There, she focused on complex civil and intellectual property litigation, primarily representing Internet and technology companies. She also worked for Blood Hurst & O'Reardon LLP, litigating consumer class action lawsuits in state and federal courts nationwide.

Boot has significant political campaign experience. She has been a party-endorsed candidate for the San Diego City Council. Before law school, Boot managed fundraising for the campaign of a Washington D.C. councilman at large and served as a regional field director for a New Hampshire presidential primary campaign.



DOMINIQUE SHELTON LEIPZIG | PARTNER | LOS ANGELES, CA

www.perkinscoie.com/DSheltonLeipzig/

Privacy and cybersecurity attorney Dominique Shelton co-chairs the firm's Ad Tech Privacy & Data Management group. She provides strategic privacy and cyber-preparedness compliance counseling, and defends, counsels and represents companies on privacy, global data security compliance, data breaches and investigations with an eye towards helping clients avoid litigation. Dominique frequently conducts trainings for senior leadership, corporate boards and audit committees regarding risk identification and mitigation in the areas of privacy and cyber.

She leads companies in legal assessments of data security, cyber preparedness and compliance with such regulations as the California Confidentiality of Medical Information Act (CMIA), HIPAA, the Video Privacy Protection Act (VPPA), the Children's Online Privacy Protection Act (COPPA) and the NIST Cybersecurity Framework.

Dominique has significant experience leading investigations related to data and forensic breaches. She has steered investigations for a range of companies, including for national retailers, financial institutions, health and wellness enterprises, media companies and others.

Dominique also advises companies on global privacy and data security, particularly on EU General Data Protection Regulation (GDPR). Her background includes advising on European, Asian and South American privacy and security compliance projects for U.S.-based and overseas companies. In addition, she counsels on strategies for related legal compliance and vendor management in cross-border transfers.



SARI RATICAN | SENIOR COUNSEL | LOS ANGELES, CA

www.perkinscoie.com/SRatican/

Sari Ratican's global privacy and data protection practice focuses on providing practical advice tailored to each client's unique needs. Her advice reflects her extensive in-house experience as the first Chief Privacy Officer for Amgen, Inc., the world's largest biotechnology company, where she built and implemented the company's global privacy program across more than 75 countries.

Sari is a Certified Information Privacy Professional (EU and US) and has been actively involved in several global privacy and data protection organizations including the International Association of Privacy Professionals, the International Pharmaceutical Privacy Consortium, and the International Medical Device Privacy Consortium.

In addition to global privacy and data protection matters, Sari has extensive experience in disciplines including healthcare fraud and abuse, compliance and ethics. Prior to specializing in global privacy and data protection, Sari was in private practice as a corporate healthcare lawyer and was also Legislative Counsel for the American Medical Association's Government Relations Department where she worked with national and state professional medical associations on various legislative matters both at the state and federal level.



NATASHA AMLANI | ASSOCIATE | LOS ANGELES, CA

www.perkinscoie.com/NAmlani/

Natasha Amlani has experience with privacy counseling, litigation and data breach response. She counsels clients on compliance efforts with state, federal and international privacy laws and regulations, including the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). Natasha is also familiar with the Stored Communications Act and helps global technology companies respond to subpoenas and other requests for user information.

Natasha earned her J.D. from UCLA School of Law, where she was a representative on the UCLA Privacy and Data Protection Board, served as executive articles editor for the UCLA Journal of Law & Technology, received Moot Court Honors and volunteered at the law school's reentry legal clinic. Natasha also spent time as an internet public interest opportunities program clerk at the Electronic Privacy Information Center in Washington, D.C.

TABLE OF CONTENTS

	Page
I. ATTORNEY GENERAL MANDATE: UPDATE CATEGORIES OF PERSONAL INFORMATION (§ 1798.185(A)(1))	1
A. ISSUE: LITERAL ADHERENCE TO THE CCPA WOULD REQUIRE BUSINESSES TO RESPOND TO CONSUMER RIGHTS REQUESTS BY PROVIDING PERSONAL INFORMATION ABOUT AN ENTIRE HOUSEHOLD OR DEVICE, THEREBY REDUCING PRIVACY PROTECTIONS	1
1. Current Law: § 1798.140(o)(1)(A); § 1798.140(x)	1
2. Problem with Current Law: Privacy of Household Members and Users of Shared Devices	2
3. [Proposed] Regulatory Solution to Problem	3
B. ISSUE: INCLUSION OF “CAPABLE OF BEING ASSOCIATED WITH A CONSUMER” IN THE DEFINITION OF PERSONAL INFORMATION IS TOO BROAD TO PROVIDE GUIDANCE FOR BUSINESS.....	3
1. Current Law: § 1798.140(o)(1); § 1798.145(i); FTC Definition of Personal Information (best practice).....	3
2. Problem with Current Law: Sweeps Too Broadly and is Unworkable.....	4
3. [Proposed] Regulatory Solution to Problem	5
C. ISSUE: PSEUDONYMIZED INFORMATION IS NOT REASONABLY LINKABLE TO A SPECIFIC CONSUMER, SO BUSINESSES SHOULD NOT BE REQUIRED TO RE-LINK IT	5
1. Current Law: § 1798.140(r), § 1798.145(i)	6
2. Problem with Current Law: Inconsistent Provisions Could Result in Businesses Reducing Privacy Protections for Consumers by Re-identifying Unidentifiable Data That Was Not Otherwise Linked to a Consumer	6
3. [Proposed] Regulatory Solution to Problem	7
D. ISSUE: CLARIFICATION OF DEIDENTIFIED DEFINITION IS NEEDED TO COVER EXISTING DEIDENTIFICATION EFFORTS UNDERTAKEN BY COMPANIES THAT RENDER DATA NOT REASONABLY LINKABLE TO AN INDIVIDUAL	7
1. Current Law: § 1798.140(h)	7
2. Problem with Current Law: Narrow Definition of Deidentified	8
3. [Proposed] Regulatory Solution to Problem:.....	8
II. ATTORNEY GENERAL MANDATE: ESTABLISH EXCEPTIONS TO COMPLY WITH STATE OR FEDERAL LAW (§ 1798.185(A)(3))	9

TABLE OF CONTENTS
(continued)

	Page
A. ISSUE: LACK OF INTELLECTUAL PROPERTY EXCEPTION DISINCENTIVIZES BUSINESS INNOVATION.....	9
1. Current Law: § 1798.185(a)(3).....	9
2. Problem with Current Law: Exposure of Business’ Intellectual Property.....	9
3. [Proposed] Regulatory Solution to Problem	10
B. ISSUE: FRAUD EXEMPTION DOES NOT EXPRESSLY INCORPORATE ENOUGH OF THE LAWS AND REGULATIONS BUSINESSES USE TO KEEP CONSUMER INFORMATION SAFE	10
1. Current Law: § 1798.105(d)(2) and (8); § 1798.140(d)(2); § 1798.145(a).....	10
2. Problem with Current Law: Fraud Exemption Does Not Expressly Enable Proactive Fraud or Other Crime Prevention or Compliance with State/Federal Regulations	11
3. [Proposed] Regulatory Solution to Problem	12
C. ISSUE: NARROW DEFINITION OF “PUBLICLY AVAILABLE INFORMATION” MINIMALLY PROTECTS PRIVACY to THE EXCLUSION OF BUSINESSES THAT PROVIDE SOCIETAL AND STATE BENEFITS	13
1. Current Law: § 1798.140(o)(1)(K)(2).....	13
2. Problem with Current Law: The Law Arguably Blocks Legitimate and Beneficial Business Functions	13
3. [Proposed] Regulatory Solution to Problem	14
III. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES RELATING TO CONSUMER OPT-OUT RIGHTS (§ 1798.185(A)(4)).....	14
A. ISSUE: ADDITIONAL LOCATIONS TO SOLICIT OPT-OUT REQUESTS ARE NEEDED	14
1. Current Law: § 1798.120(b); § 1798.135(a)(1); § 1798.135(b) § 1798.140(l).....	15
2. Problem with Current Law: The Obligations Associated with Each “Homepage” are Overly Burdensome	15
3. [Proposed] Regulatory Solution to Problem	16
IV. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES: (1) TO FACILITATE AND GOVERN THE SUBMISSION OF A CONSUMER OPT-OUT REQUEST; AND (2) FOR THE DEVELOPMENT AND USE OF A RECOGNIZABLE AND UNIFORM OPT-OUT LOGO OR BUTTON (§ 1798.185(A)(4)(A) AND (C)).....	16

TABLE OF CONTENTS
(continued)

	Page
A. ISSUE: CREATE A SANCTIONED “DO NOT SELL” LOGO FOR CONSUMERS TO EASILY RECOGNIZE HOW TO OPT OUT OF THE SALE OF THEIR PERSONAL INFORMATION.....	16
1. Current Law: § 1798.135(a)(1)	17
2. Problem with Current Law: Obstacles to Implementation	17
3. [Proposed] Regulatory Solution to Problem	17
B. ISSUE: BUSINESSES ARE NOT ABLE TO OFFER CONSUMERS THE CHOICE TO OPT-OUT OF SPECIFIC SALES OF PERSONAL INFORMATION.....	17
1. Current Law: § 1798.135(a)(1)	17
2. Problem with Current Law: A One-Size Fits All “Do Not Sell” Link is Over-Inclusive	18
3. [Proposed] Regulatory Solution to Problem	18
C. ISSUE: CONSUMERS AFFIRMATIVELY OPTING-IN SHOULD NOT BE INCLUDED IN THE GLOBAL “DO NOT SELL MY PERSONAL INFORMATION” REQUIREMENT	18
1. Current Law: § 1798.135(a)(1)	18
2. Problem with Current Law: The Global “Do Not Sell” Choice Disincentivizes Businesses from Offering Opt-In Choices	18
3. [Proposed] Regulatory Solution to Problem	19
D. ISSUE: NEW AGE CATEGORY (AGES 13-16) FOR OPT-IN CONSENT CREATES POTENTIAL BURDEN ON BUSINESSES TO IDENTIFY AGE OF CONSUMERS, JEOPARDIZING PRIVACY, AND CREATES INCONSISTENCIES WITH FEDERAL LAW	19
1. Current Law: § 1798.120(c).....	19
2. Problem with Current Law: Burdensome to Implement.....	20
3. [Proposed] Regulatory Solution to Problem	20
V. ATTORNEY GENERAL MANDATE: ESTABLISH RULES, PROCEDURES AND EXCEPTIONS RELATING TO NOTICES AND INFORMATION TO CONSUMERS, INCLUDING FINANCIAL INCENTIVE OFFERINGS (§ 1798.185(A)(6))	20
A. ISSUE: BUSINESSES SHOULD BE ABLE TO INFORM CONSUMERS OF THEIR PERSONAL INFORMATION PRACTICES AT, OR BEFORE, THE POINT OF COLLECTION THROUGH THEIR PRIVACY POLICIES	20
1. Current Law: § 1798.100(b)	21

TABLE OF CONTENTS
(continued)

	Page
2. Problem with Current Law: Notification Directly to Consumers Can be Impracticable or Impossible where Personal Information is Collected from Physical Locations or Public Sources as Opposed to Online Interactions.....	21
3. [Proposed] Regulatory Solution to Problem	22
B. ISSUE: GUIDANCE NEEDED ON CCPA-COMPLIANT FINANCIAL INCENTIVES	22
1. Current Law: § 1798.125(b)(4).....	22
2. Problem with Current Law: Obstacles to Implementation	22
3. [Proposed] Regulatory Solution to Problem	23
VI. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES FOR VERIFYING CONSUMER REQUESTS AND OTHER NECESSARY REGULATIONS TO FURTHER PURPOSES OF THE TITLE (§ 1798.185(A)(7))	23
A. Issue: CCPA clearly states that January 1, 2020 is the effective date; therefore, the 12-month lookback period should not be misinterpreted by consumers or regulators to begin prior to the effective date.....	23
1. Current Law: § 1798.130(a)(3)(B) see also § 1798.130(a)(4)(B)-(C); § 1798.130(a)(5).....	23
2. Problem with Current Law: Confusion Regarding Start of Lookback Period	24
3. [Proposed] Regulatory Solution to Problem	24
B. ISSUE: REGULATIONS NEEDED RELATING TO HOW TO VERIFY AUTHORIZATION OF THIRD-PARTIES WHO MAKE CONSUMER REQUESTS SO CONSUMER PRIVACY IS NOT UNDERMINED.....	25
1. Current Law: § 1798.135(c) and § 1798.140(y)	25
2. Problem with Current Law: Lack of Guidance for Businesses.....	25
3. [Proposed] Regulatory Solution to Problem	26
C. ISSUE: REGULATIONS NEEDED ON HOW CONSUMER REQUESTS CAN BE SUBMITTED AND PROCESSED TO MAINTAIN THE CONFIDENTIALITY AND SECURITY OF PERSONAL INFORMATION.....	26
1. Current Law: § 1798.140(y)	26
2. Problem with Current Law: Lack of Guidance for Businesses.....	27
3. [Proposed] Regulatory Solution to Problem:.....	27

TABLE OF CONTENTS
(continued)

	Page
D. ISSUE: ALLOWING DISCLOSURE OF “SPECIFIC PIECES OF INFORMATION” FOR CONSUMER RIGHTS OTHER THAN THE RIGHT TO ACCESS REQUESTS WOULD CREATE UNNECESSARY CYBERSECURITY RISKS AND CONTRADICT THE TEXT OF THE STATUTE.....	28
1. Current Law: § 1798.100(a), § 1798.110(a)(5), § 1798.110(c)(5)	28
2. Problem with Current Law: Privacy and Cybersecurity Risks by Disclosure of Personal Information	28
3. [Proposed] Regulatory Solution to Problem	29
E. ISSUE: THIRD PARTIES WHO DO NOT HAVE DIRECT RELATIONSHIPS WITH CONSUMERS CANNOT NOTIFY THEM THAT THEIR PERSONAL INFORMATION HAS BEEN SOLD.....	29
1. Current Law: § 1798.115(d)	29
2. Problem with Current Law: Third Parties Do Not Have Direct Relationship with Consumers	29
3. [Proposed] Regulatory Solution to Problem	30
F. ISSUE: CLARIFYING THAT BUSINESSES ARE NOT REQUIRED TO RETAIN PERSONAL INFORMATION SOLELY TO COMPLY WITH CONSUMER REQUESTS; ALSO DATA RETENTION TO COMPLY WITH THE 12-MONTH LOOKBACK PERIOD COULD VIOLATE DATA MINIMIZATION BEST PRACTICES	30
1. Current Law: § 1798.100(e); § 1798.130(a)(3)(B)	30
2. Problem with Current Law: Privacy and Security Risks	30
3. [Proposed] Regulatory Solution to Problem	31
G. ISSUE: EMPLOYMENT AND BUSINESS-RELATED DATA	31
1. Current Law: § 1798.140(g)	31
2. Problem with Current Law: Employees Should Not Be Considered Consumers, and business-to-business communications should not be covered	31
3. [Proposed] Regulatory Solution to Problem	32
H. ISSUE: OBSTACLES TO DETERMINING WHO IS A CALIFORNIA CONSUMER	33
1. Current Law: § 1798.140(g); 18 CCR § 17014	33
2. Problem with Current Law: No Streamlined Way to Determine Who is a California Consumer.....	33
3. [Proposed] Regulatory Solution to Problem	33

TABLE OF CONTENTS
(continued)

	Page
I. ISSUE: REASONABLE SECURITY AND PRIVATE RIGHT OF ACTION	34
1. Current Law: § 1798.150(a)(1)	34
2. Problem with Current Law: Discourages Compliance with Reasonable Security	34
3. [Proposed] Regulatory Solution to Problem	34
J. ISSUE: RIGHT TO CURE ALLEGED VIOLATIONS DOES NOT COMPORT WITH BEST SECURITY PRACTICES	35
1. Current Law: § 1798.150(b) and Various Security Frameworks	35
2. Problem with Current Law: Businesses Following Recommended Guidance May Find Themselves Subject to Claims They Have Violated a Written Statement	35
3. [Proposed] Regulatory Solution to Problem	36
K. ISSUE: “SERVICE PROVIDERS,” “THIRD PARTIES,” AND “PERSONS” SERVICE PROVIDERS (§ 1798.140 (v)), THIRD PARTIES (§ 1798.140 (w)) AND (LIABILITY SHIFTED) PERSONS (1798.140(w)(2)) SHOULD ALL BE TREATED THE SAME FOR PURPOSES OF § 1798.140 (t)(2), MEANING THAT THE EXCEPTIONS TO “SALE” APPLY EQUALLY TO TRANSFERS TO “SERVICE PROVIDERS,” “THIRD PARTIES,” AND “PERSONS”	36
1. Current Law: § 1798.140(w)(2)	36
2. Problem with Current Law: Overly Burdensome on Businesses to Sign Vendor Contracts Substantially Similar to Those Signed under GDPR and Treats “Service Providers,” “Third Parties,” and “Natural Persons” Unequally	37
3. [Proposed] Regulatory Solution to Problem	37
L. ISSUE: GUIDANCE NEEDED ON HOW SERVICE PROVIDERS SHOULD RESPOND TO VERIFIABLE CONSUMER REQUESTS	38
1. Current Law: § 1798.105(c)	38
2. Problem with Current Law: No Clear Guidance for Service Providers	38
3. [Proposed] Regulatory Solution to Problem	38

I. ATTORNEY GENERAL MANDATE: UPDATE CATEGORIES OF PERSONAL INFORMATION (§ 1798.185(A)(1))

A. ISSUE: LITERAL ADHERENCE TO THE CCPA WOULD REQUIRE BUSINESSES TO RESPOND TO CONSUMER RIGHTS REQUESTS BY PROVIDING PERSONAL INFORMATION ABOUT AN ENTIRE HOUSEHOLD OR DEVICE, THEREBY REDUCING PRIVACY PROTECTIONS

The definition of personal information goes beyond information tied to a particular consumer. It includes information tied to a household and information tied to devices. Therefore, a consumer that makes a verifiable consumer rights request for personal information may be technically entitled to personal information about themselves, *as well as* household members, or others with whom they share devices. Disclosing personal information to one member of that household or one user of a shared device undermines the privacy of other household members and shared device users and may restrict their rights under this title (e.g., their right to access if another household consumer already requested deletion). Confirming that businesses do not have to provide information related to “households” and “devices” when responding to individual consumer requests under the title protects the privacy of all consumers as it is more in line with the privacy-protective spirit of the CCPA.

1. Current Law: § 1798.140(o)(1)(A); § 1798.140(x)

a. “Personal information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or *household*. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or *household*: Identifiers such as a real name, alias, postal address, *unique personal identifier*, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers...[.]” (Emphasis added)

b. “Unique identifier” or “Unique personal identifier” means a persistent identifier that can be used to recognize a consumer, a family, or a *device* that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, “family” means a custodial parent or guardian and any minor children over which the parent or guardian has custody. (Emphasis added)

2. Problem with Current Law: Privacy of Household Members and Users of Shared Devices

a. Requiring the disclosure of data associated to a household or a shared device risks compromising the privacy of consumers within that household or that share the device. Consider roommates, adult children living with their parents, or elderly parents living with their adult children: If a consumer requests information related to his/her household such as from a delivery service (e.g., an online food delivery service), it may expose the personal information beyond that individual requestor. The exposed personal information of household members or shared device users may include financial, health, political, or other information that the non-requesting individuals may not wish to share with others they live with such as use of alcohol or other controlled substances, sexual activity, reading interests (e.g., political, health conditions, or other specific periodicals), or payment activity (e.g., credit card numbers or government assistance programs). For example, a household member may request information from a grocery delivery service itemizing orders for that entire household based on address that then exposes a household member's purchase of birth control or a pregnancy test.

b. A request for information related to a household could also expose private information from previous household owners or residents and short-term rental guests.

c. The safety of household members may also be placed at risk if a consumer can access household information. In domestic violence situations, consumer rights requests that go to the household might expose an abused spouse's research for safe houses to relocate to avoid abuse. The scenarios for other compromises of consumer safety are limitless.³

d. Not only does this compromise the privacy of consumers but could also infringe on consumer rights and choices of other past and present household members or device users. One household member or device user may make a deletion request to delete all data associated with a household or device. Another household member or device user may subsequently make an access request. This requesting consumer would be unable to access the household or device information that pertains specifically to him/her, rendering video streaming feed customization, loyalty program points accumulated, or other information wiped out without his/her instruction or consent.

³ See e.g., Nellie Bowles, "Thermostats, Locks and Lights: Digital Tools of Domestic Abuse," *New York Times* (June 23, 2018), available at: <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html> for a discussion of how smart home technology is being used as a domestic abuse tool, including for harassment, monitoring, revenge, and control.

e. Consider also a household with shared devices, including a television, for which multiple users of the television password protect the apps they use to stream videos. If video streaming information of all device users is disclosed to one user, this violates the privacy of all users of the shared device by disclosing personal information, as defined by the FTC. Information that could be exposed in connection with a shared device may include photos, browsing history, app downloads, etc.

3. [Proposed] Regulatory Solution to Problem

a. The AG's office will insert clarification language as follows: "Clarification of § 1798.140(o)(1)(A); (x): The CCPA contemplates business compliance activities associated with responding to verifiable consumer requests with personal information pertaining only to the verifiable consumer. Further, the CCPA does not require businesses when, complying with a consumer rights request, to expose the personal information of household members or device users that cannot be differentiated from the requesting consumer, including situations where there are multiple profiles or other indications of multi-user activity."

B. ISSUE: INCLUSION OF "CAPABLE OF BEING ASSOCIATED WITH A CONSUMER" IN THE DEFINITION OF PERSONAL INFORMATION IS TOO BROAD TO PROVIDE GUIDANCE FOR BUSINESS

Personal information as defined in the CCPA includes data that is "capable of being associated with a consumer," no matter how remote or difficult the possibility of association might be. This definition of personal information undermines consumer privacy by encouraging businesses to go to lengths to attempt to link data that is not reasonably associated with a consumer. In addition, it imposes significant operational and financial burdens on businesses with no clear guidance on when enough is enough in terms of trying to associate data with a consumer. Narrowing the scope of the definition of personal information to exclude information that is not "reasonably" capable of being associated with a consumer more appropriately captures information tied to a consumer and creates more pragmatic business obligations.

1. Current Law: § 1798.140(o)(1); § 1798.145(i); FTC Definition of Personal Information (best practice)⁴

a. "Personal information" means information that identifies, relates to, describes, is *capable of being associated with*, or could reasonably be linked, directly or indirectly, with *a particular consumer* or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is *capable of being associated with*, or could be reasonably linked, directly or indirectly, with *a particular consumer* or household...[.] (Emphasis added)

⁴ ["Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,"](#) Federal Trade Commission (March 2012) at 18.

b. § 1798.145(i): “This title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.”

c. During the Obama Administration, the FTC defined personal information as “consumer data that can be *reasonably* linked to a specific consumer, computer, or other device.”⁵ (Emphasis added)

2. Problem with Current Law: Sweeps Too Broadly and is Unworkable

a. “Capable of being associated with” an individual, household, or device arguably sweeps so broadly as to be meaningless as every piece of data could potentially be “capable of being associated with” an individual, household, or device. Thus, by sweeping so broadly, businesses could be exposed to consumer requests requiring a business to respond with personal information beyond what is reasonably capable of being associated with a particular consumer. This runs a significant risk of (a) undermining privacy-protective business practices (e.g., via aggregating or pseudonymizing data); (b) potentially exposing other consumers’ personal information; and (c) imposing significant operational and financial costs and burdens on businesses.

b. According to a recent Forbes magazine article: “There are 2.5 quintillion bytes of data created each day at our current pace, but that pace is only accelerating with the growth of the Internet of Things (IoT). Over the last two years alone 90 percent of the data in the world was generated.”⁶ By 2020, experts estimate that “1.7MB of data will be created every second for every person on earth.”⁷ Furthermore, small businesses may not even have the capacity to identify individual consumers. The small business might get an analytic report from a vendor that contains unique identifiers assigned by the vendor that are not synced with the business’ unique identifiers. To identify its consumers, notwithstanding Section 1798.145(i), the business would need to obtain more personal information about the consumer from a vendor, obtain the vendor’s look up-table, or hire a forensic investigator to re-identify the consumer’s personal information, none of which are practical options. So, even though it might be possible to reidentify consumer information, to require businesses doing business in California to plow through petabytes of data in order to reidentify data that was only scientifically “capable” of being associated with an individual, but has no “reasonable” capability of doing so, is inefficient and cost/technologically-prohibitive for most

⁵ *Id.*

⁶ Bernard Marr, “[How Much Data Do We Create Every Day - The Mind Blowing Stats Everyone Should Read](#)” Forbes (May 21, 2018).

⁷ [Data Never Sleeps 6.0](#), domo.com, (2018).

businesses and not privacy protective for consumers whose data may be subject to re-linking and reidentification needlessly.

3. [Proposed] Regulatory Solution to Problem

a. The AG's office will provide instruction and clarification for businesses as follows:

(1) "Clarification of § 1798.140(o)(1); § 1798.145(i): The CCPA contemplates business compliance activities associated with pseudonymous and other data not reasonably capable of association with a consumer. Further, the CCPA contemplates that consistent with California Civil Code Section 1798.145(a)(5), the obligations imposed on businesses by this title shall not restrict a business's ability to collect, use, retain, sell, or disclose consumer information that is not reasonably capable of being associated with, or linked, directly or indirectly, with a particular consumer, such as data held by a business in pseudonymous form."

(2) "Clarification of § 1798.140(o)(1); § 1798.145(i): The CCPA contemplates business compliance activities associated with the implementation of a comprehensive privacy program and compliance with the FTC's definition of personal information.

(3) "Clarification of Section 1798.145(a)(1): Businesses that have (a) a comprehensive privacy program, (b) otherwise comply with FTC publications and guidance related to personal information that is reasonably linkable to an individual, and/or (c) treat consumer's personal information in alignment with the FTC's definition of personal information are in compliance with this title."

C. **ISSUE: PSEUDONYMIZED INFORMATION IS NOT REASONABLY LINKABLE TO A SPECIFIC CONSUMER, SO BUSINESSES SHOULD NOT BE REQUIRED TO RE-LINK IT**

Pseudonymization is a method of enhancing an individual's privacy by replacing the personal information within a dataset with fake identifiers, or pseudonyms, so that the data can no longer be reasonably linked to a specific individual. The CCPA recognizes that pseudonymized information *"...renders the personal information no longer attributable to a specific consumer."* Because pseudonymized data cannot be reasonably linked to a specific person, it is an effective data minimization tool in furtherance of the CCPA's intent. Requiring businesses to re-link pseudonymized data to specific consumers will not only be very burdensome on businesses, but will result in data maximization thereby undermining the CCPA's primary goal of protecting personal information.

1. Current Law: § 1798.140(r), § 1798.145(i)

The CCPA recognizes that pseudonymized information is no longer attributable to a specific person and that unidentifiable information should not be re-linked to personal information to comply with the statute.

a. § 1798.140(r): “Pseudonymize” or “Pseudonymization” means the processing of personal information in a *manner that renders the personal information no longer attributable to a specific consumer* without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer. (Emphasis added)

b. § 1798.145(i): “This title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.”

2. Problem with Current Law: Inconsistent Provisions Could Result in Businesses Reducing Privacy Protections for Consumers by Re-identifying Unidentifiable Data That Was Not Otherwise Linked to a Consumer

a. Pursuant to Section 1798.140(r), “pseudonymized information” is data that has been subject to an information security protocol rendering it no longer attributable to a specific individual. To re-link pseudonymized information to a specific consumer in order to comply with a consumer’s deletion request imposes significant technical and administrative burdens on businesses (both large and small) and could also expose the personal information to risk once it is no longer pseudonymized. Consumer privacy would be harmed by requiring reidentification and since the intent of this law is to enhance privacy, it is consistent with this intent to not require re-identification.

b. Pursuant to Section 1798.145(i), the re-linking of data that is not otherwise identifiable to a person is contrary to the CCPA’s provisions that make it clear that data should not be re-linked. Consider a small business, such as a family-owned restaurant, that conducts on average 12 transactions per hour in each 12-hour day. If, on average, that restaurant has 137 visitors per day it would meet the CCPA requirements of a business that processes personal information of 50,000 or more California consumers. To comply with the privacy protective spirit of the CCPA, this small business chooses to pseudonymize the personal information it collects on its website with the intent of protecting its consumers from cybersecurity risks by making the data unidentifiable to a person. To require this family-owned restaurant to re-link the pseudonymized data to identify it with specific individuals would be contrary to the spirit of

protecting consumer privacy by masking personal information. Further, it is unlikely that small businesses would have the internal staff or means to devote potentially hundreds of hours to re-link data that was not otherwise readily identifiable to a person. Additionally, to re-link the pseudonymized data to a consumer would potentially expose such consumer's personal information to risk and be contrary to the purpose of the CCPA.

c. Consider also a business that invested heavily in privacy-protective pseudonymization techniques such as a SHA-256 hash to convert personal information into an alpha-numeric number that on its own is not identifiable to a person, and maintains a separate lookup table in an entirely different repository (e.g., maintained in a separate database with access controls, strict policies; or is maintained by a vendor on the businesses behalf). In order to respond to a consumer request, the AG should clarify that the business should not have to re-link these two entirely separate databases, eliminating the protection provided to the personal information to respond to consumer requests.

3. [Proposed] Regulatory Solution to Problem

a. The AG's office will insert clarification language: "Clarification of § 1798.140(o)(1)(A); § 1798.140(r); (x): For purposes of this title, businesses maintaining personal information in a manner that renders personal information no longer reasonably linkable to a specific consumer (e.g., pseudonymized data) are not required to re-identify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information."

D. ISSUE: CLARIFICATION OF DEIDENTIFIED DEFINITION IS NEEDED TO COVER EXISTING DEIDENTIFICATION EFFORTS UNDERTAKEN BY COMPANIES THAT RENDER DATA NOT REASONABLY LINKABLE TO AN INDIVIDUAL

1. Current Law: § 1798.140(h)

a. "Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

- (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
- (2) Has implemented business processes that specifically prohibit reidentification of the information.

- (3) Has implemented business processes to prevent inadvertent release of deidentified information.
- (4) Makes no attempt to reidentify the information.

2. Problem with Current Law: Narrow Definition of Deidentified

a. Many companies have followed Federal Trade Commission (“FTC”) guidance from the Obama Administration regarding anonymized data that is very similar to Section 1798.140(h). It is also similar to the definition of aggregate data under the European General Data Protection Regulation (“GDPR”). The FTC states that if: (1) a given data set is not reasonably identifiable, (2) the company publicly commits not to re-identify it, and (3) the company contractually requires any downstream users of the data to keep it in de-identified form, that data will fall outside the scope of the framework.⁸

b. As another point of comparison, the GDPR does not consider aggregate data to be personal information⁹ as it is data that is expressed in summary form and, while arguably capable of being associated with, it is unable to identify an individual. Yet, the CCPA includes “capable of being associated” as part of the definition of personal information which arguably does not account for situations in which the data is not reasonably able to identify an individual; thus, the AG should clarify that, under the CCPA, “capable of being associated” with a consumer does not include data that is not reasonably able to identify an individual.

3. [Proposed] Regulatory Solution to Problem:

a. The AG’s office will insert clarification language:

- (1) “Clarification of § 1798.140(h): A company will be deemed to deidentify data if it meets recognized practices for deidentifying (e.g., FTC, HIPAA, or others). Also, for purposes of 1798.140(h)(2)-(3), “business processes” may include contractual requirements that prohibit reidentification and are designed to prevent inadvertent release of deidentified information.”

⁸ [“Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,”](#) Federal Trade Commission (March 2012) at 22.

⁹ See e.g., General Data Protection Regulation, Recital 162.

II. ATTORNEY GENERAL MANDATE: ESTABLISH EXCEPTIONS TO COMPLY WITH STATE OR FEDERAL LAW (§ 1798.185(A)(3))

A. ISSUE: LACK OF INTELLECTUAL PROPERTY EXCEPTION DISINCENTIVIZES BUSINESS INNOVATION

The CCPA does not provide an express exception for intellectual property which threatens to disincentivize and undermine business innovation. Creating an exception for intellectual property subject to copyright, patent, trade or service mark, or trade secret protection, including any formula, pattern, compilation, program, device, method, technique, or process developed to process or analyze personal information, and any information derived from such process or analysis will not undermine consumer privacy protections and will ensure that California remains a leader in technology and business innovation.

1. Current Law: § 1798.185(a)(3)

a. Absence of intellectual property exception.

b. § 1798.185. (a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:
.... (3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.

2. Problem with Current Law: Exposure of Business' Intellectual Property

a. Many businesses' collection of data occurs in such a specific, granular manner that to provide it to a requesting consumer in a readily-useable format capable of being transmitted to other businesses would be burdensome as it would require businesses to protect against disclosure of trade secret or other intellectual property in responses to consumer inquiries (e.g., a business need not reveal its "secret ingredient" in response to a consumer request).

b. Consider a business whose proprietary algorithm is powered by personal information: If a business' obligation to delete personal information upon a consumer's request impacts the proprietary algorithm's efficacy or validity, businesses may be less inclined or incentivized to innovate in California or include California consumers' in potentially life-saving/enhancing or cost-saving innovations. In addition, if California consumers' personal information is deleted and, therefore, unavailable to "train" the algorithms, it may result in algorithms that are biased for lack of a representative sample.

c. Consider a health-tech vendor analyzing big data to identify a predictive cancer gene. If California data could be subject to deletion requests that would slow down the analysis or prevent use of the data for predictive purposes, scientific innovators may be inclined to exclude California residents from studies and technology that could be beneficial to Californian's health.

3. [Proposed] Regulatory Solution to Problem

a. The AG's office will insert clarification language as follows:
“Clarification of § 1798.185(a)(3): The CCPA contemplates business compliance activities associated with the protection of intellectual property. The CCPA does not require a business to comply with a consumer request, when such request would adversely affect or require disclosure of intellectual property subject to copyright, patent, trade or service mark, or trade secret protection, including any formula, pattern, compilation, program, device, method, technique, or process developed to process or analyze personal information, or any information derived from such process or analysis.”

B. ISSUE: FRAUD EXEMPTION DOES NOT EXPRESSLY INCORPORATE ENOUGH OF THE LAWS AND REGULATIONS BUSINESSES USE TO KEEP CONSUMER INFORMATION SAFE

The existing fraud exemption does not expressly preclude opt-out of personal information that is or may be necessary to comply with state, federal, or local laws, rules, and regulations prohibiting fraudulent activity and state, federal, and local anti-corruption, anti-money laundering, export control, and “know your consumer” laws, rules, and regulations. Although fraud is mentioned in the “business purpose” definition, the current definition of “business purpose” and “service provider” both arguably fall short in that they appear to apply to a business conveying information to a service provider; it does not clearly cover information going from the service provider to the business, as is the case with identity verification and fraud prevention services. Further, the law is not clear regarding what the requirements are for a service provider, other than they receive information for a business purpose and process information on behalf of a business. When identity verification and fraud prevention services are provided to a government agency or a bank, the company doesn't typically receive their data. They are provided with the identity verification company's data. Confirming that the fraud exemption applies to opt out rights and ensuring that bad actors are not free to “opt out” of data uses designed to stop them from illegal activities (such as identity theft and money laundering) is critical and would serve the purposes of the CCPA.

1. Current Law: § 1798.105(d)(2) and (8); § 1798.140(d)(2); § 1798.145(a)

a. § 1798.105(d): A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider

to maintain the consumer's personal information in order to: (2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity... (8) Comply with a legal obligation.

b. § 1798.140(d): "Business purpose" means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are: (2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

c. § 1798.145(a): The obligations imposed on businesses by this title shall not restrict a business's ability to:

- (1) Comply with federal, state, or local laws.
- (2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.
- (3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.
- (4) Exercise or defend legal claims.
- (5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.

2. Problem with Current Law: Fraud Exemption Does Not Expressly Enable Proactive Fraud or Other Crime Prevention or Compliance with State/Federal Regulations

a. Many businesses proactively undertake fraud prevention activities in connection with pre-screening consumers for fraudulent activities (e.g., "know your customer" procedures for financial institutions) that are in accordance with regulations promulgated in support of federal, state or local laws, but are arguably not taken to "comply with federal, state, or local laws," or "comply with a civil criminal or regulatory inquiry..." (§ 1798.140(a)(1) and (2)). While § 1798.140(a)(1) covers a business' ability to comply with "laws," it does not cover a business' ability to comply with "rules and regulations." Similarly, while § 1798.140(a)(2)

would cover fraud investigations in response to a government inquiry, investigation, or summons, it arguably does not cover fraud investigations absent government initiative. Accordingly, the fraud exemption arguably does not preclude opt-out or deletion of personal information that is or may be necessary to comply with state, federal, or local, rules and regulations prohibiting fraudulent activity and state, federal, and local anti-corruption, anti-money laundering, export control, and “know your customer” rules, and regulations. Data necessary to comply with state, federal, local laws, rules, and regulations includes firmographic data, linkage data, and other trade data.

b. Without this exception, the CCPA threatens to undermine government safety-net programs and harm California’s most vulnerable populations. Many California governmental entities utilize data supplied by private companies to fulfil their mission. If a consumer’s personal information is unavailable for such use, the effectiveness of the associated government program will suffer. Additionally, increased instances of identity theft caused by the CCPA will undermine the stability of these government programs that rely on identity verification and fraud prevention tools. State and local government programs that could suffer unintended consequences due to the current language of the CCPA include: Healthcare agencies that review third party medical provider data provided by businesses to keep excluded Providers out of the system and protect citizens; Program Integrity Divisions of government benefit programs; State and County Tax Fraud Prevention and Detection programs; programs ensuring payment of child support (data used to locate non-custodial parents); and foster youth programs (data used to connect children with family members, which reduces the number of children in foster care). Corporate crime prevention efforts would be similarly affected with a resulting impact on consumers who become identity theft victims. As mentioned above, financial institutions – securities firms and also other types of financial services – have obligations under the Bank Secrecy Act/Anti Money Laundering regime to know who their customers are, understand the activity in their customers’ accounts, and monitor for, investigate, and report suspicious activity. They use customer data to do this and may need to access third-party data or data from other financial institutions to fulfill these obligations.

3. [Proposed] Regulatory Solution to Problem

a. The AG’s office will provide clarification as follows:

(1) “Clarification of § 1798.105(d)(2) and (8); § 1798.140(d)(2); § 1798.145(a): The CCPA contemplates business compliance activities associated or those with crime and fraud prevention activities including when it is necessary for a business

or service provider to maintain the consumer's personal information in order to:

- (a) comply with corresponding federal, state, or local laws, rules and regulations; or
- (b) collect, use, retain, sell, authenticate, or disclose personal information in order to: (i) exercise, defend, or protect against legal claims; (ii) protect against or prevent security incidents; (iii) protect against or investigate, report, or prosecute those responsible for malicious, deceptive, or illegal activity; (iv) prevent, detect, or mitigate fraudulent activity; or (v) assist another person or government agency to conduct any of the activities specified in this section."

C. ISSUE: NARROW DEFINITION OF "PUBLICLY AVAILABLE INFORMATION" MINIMALLY PROTECTS PRIVACY TO THE EXCLUSION OF BUSINESSES THAT PROVIDE SOCIETAL AND STATE BENEFITS

Limiting the definition of personal information to information from government records "compatible with the purposes for which it is maintained" may arguably restrict many legitimate business purposes (such as assisting the government and consumers with collecting unpaid child support), is a confusing standard that is difficult to apply in practice, and limits use of publicly available data in a way that is, on balance, more harmful than beneficial. Clarifying the definition to confirm that information that is only used for a purpose not compatible with the purpose for which the data is maintained where the government agency publishing the data puts lawful limitations on use of published data will provide needed clarity to businesses and avoid claims that public information cannot be used for legitimate purposes.

1. Current Law: § 1798.140(o)(1)(K)(2)

- a. "Personal information" does not include publicly available information defined by the title to mean information that is lawfully made available from federal, state, or local *government records*. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. *Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.* "Publicly available" does not include consumer information that is deidentified or aggregate consumer information. (Emphasis added)

2. Problem with Current Law: The Law Arguably Blocks Legitimate and Beneficial Business Functions

- a. As written, "publicly available" information not subject to CCPA obligations is limited only to the use of government records "compatible

with the purposes for which it is maintained” which is far too narrow for California businesses to continue operating for appropriate public benefit. For example, a California real estate-related business that displays the last sale price for houses on its website should have clarity that the purpose of doing so is compatible with the publication of such information because the lack of a clear exemption for publicly available information may impede their ability to provide vital services to consumers along with state and local governments, including, for example, collection of unpaid child support, collection of state, local, and federal tax liens, as well as coordinate with district attorneys and law enforcement authorities, where appropriate. While these may be permissible business purposes under Section 1798.140(a)(4), the AG should clarify that these businesses operating for a public benefit are not restricted due to the narrow definition of “publicly available.”

3. [Proposed] Regulatory Solution to Problem

a. The AG’s office will include clarification as follows:

(1) “Publicly Available Information Guidance; § 1798.140(o)(1)(K)(2): Publicly available information is any information that is lawfully made available to the general public from federal, state, or local government records including disclosures to the general public that are required to be made by federal, state, or local law, rules, or regulations.”

(2) Government Records Guidance: Government records include any data made available to the public by the government voluntarily or as a matter of law.”

(3) “Use of Public Information Guidance in Section 1798.140(o)(2): In the absence of an express limitation of use by the government entity holding that data, data collected subject to Section 1798.140(o)(2) may be used for any lawful purpose.”

III. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES RELATING TO CONSUMER OPT-OUT RIGHTS (§ 1798.185(A)(4))

A. ISSUE: ADDITIONAL LOCATIONS TO SOLICIT OPT-OUT REQUESTS ARE NEEDED

Requiring businesses to place a “Do Not Sell My Personal Information” link on the business’ Internet homepage may cause confusion among California consumers as they have become accustomed to looking at a business’ posted privacy policy for instructions for exercising their rights under the California Shine the Light Law¹⁰, which has been in effect for over 10 years. To reduce consumer confusion and to support consumers in exercising their CCPA-provided rights,

¹⁰ [Cal. Civ. Code § 1798.83.](#)

the AG should seek to align the CCPA with existing and California-provided consumer rights by permitting a business to place the “Do Not Sell My Personal Information” link on either its homepage *or* within its posted privacy policy.

1. Current Law: § 1798.120(b); § 1798.135(a)(1); § 1798.135(b) § 1798.140(l)

a. A business that sells consumers’ personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the “right to opt-out” of the sale of their personal information.

(1) § 1798.135(a)(1): “A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:… [p]rovide a clear and conspicuous link on the business’s Internet *homepage*, titled “Do Not Sell My Personal Information,” to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer’s personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer’s personal information. (Emphasis added)

b. § 1798.135(b) “Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, *if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers* and not the homepage made available to the public generally.” (Emphasis added)

c. § 1798.140(l): “Homepage” means the introductory page of an Internet Web site and *any Internet Web page where personal information is collected.*” (Emphasis added)

2. Problem with Current Law: The Obligations Associated with Each “Homepage” are Overly Burdensome

a. The CCPA’s “homepage” definition includes both the home page of a website as well as every web page at which a business collects personal information. The result is to require an “opt-out” button *on every single web page where a business collects any personal information, including an IP address*, since IP addresses are considered personal information. Read literally, this would require special California right-to-know notices on virtually every single business web page amounting to a substantial burden on impacted businesses.

b. Alternatively, the CCPA states that businesses may develop a California-specific home page, but as California consumers are not accustomed to looking for information practices there but, instead to posted privacy policies, this may be counter to privacy-protective best practices.

c. When a business or a brand does not maintain what may be traditionally perceived as a “homepage,” flexibility is needed as to where the “Do Not Sell My Personal Information” link should be placed in order to best reach consumers. For example, the opt-out choice may be more accessible to consumers if it is offered alongside or in conjunction with a business’ privacy policy or page, as that is the location that consumers generally visit to learn about their choices and manage any offered preferences.

3. [Proposed] Regulatory Solution to Problem

a. The AG’s office will insert clarification language as follows:

(1) “Clarification of § 1798.135(a)(1) and (b): For purposes of this title, businesses shall develop and implement a method or methods to solicit consumer opt-out requests on the initial landing page or within the privacy policy posted on its website(s) and/or mobile application(s). For purposes of this title, businesses that clearly and conspicuously state in their privacy policy that they do not sell personal information to third parties for the third parties’ own business purposes are not required to provide a “Do Not Sell My Personal Information” link or logo on their homepage to consumers.”

IV. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES: (1) TO FACILITATE AND GOVERN THE SUBMISSION OF A CONSUMER OPT-OUT REQUEST; AND (2) FOR THE DEVELOPMENT AND USE OF A RECOGNIZABLE AND UNIFORM OPT-OUT LOGO OR BUTTON (§ 1798.185(A)(4)(A) AND (C))

A. ISSUE: CREATE A SANCTIONED “DO NOT SELL” LOGO FOR CONSUMERS TO EASILY RECOGNIZE HOW TO OPT OUT OF THE SALE OF THEIR PERSONAL INFORMATION

Consumers may find it easier to locate and use a recognizable “Do Not Sell My Personal Information” logo (similar to the popular AdChoices logo used to link consumers to their choices about website cookies and tracking technologies) in place of or in addition to the required Internet homepage link language.

1. Current Law: § 1798.135(a)(1)

a. A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers: ... [p]rovide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

2. Problem with Current Law: Obstacles to Implementation

a. Implementation of the CCPA would best be served by familiarity and ease of use. Logos are often more readily identifiable by consumers and allowing optional use of a logo may enhance implementation of the CCPA. Use of such a logo may enhance the "clear and conspicuous" disclosure of the opt out option similar to the AdChoices logo. The logo would serve as a safe harbor for businesses, similar to the template GLBA notices created by the FTC, for example.

3. [Proposed] Regulatory Solution to Problem

a. The AG's office will insert clarification language: "Clarification of § 1798.135(a)(1) and § 1798.135 (b): For purposes of this title, businesses will be deemed to be in compliance with this requirement by clearly and conspicuously inserting the "Do Not Sell My Personal Information" link, icon developed by the AG, or other opt-out procedure on their homepage or within the privacy policy posted on its website(s) and/or mobile application(s)."

B. ISSUE: BUSINESSES ARE NOT ABLE TO OFFER CONSUMERS THE CHOICE TO OPT-OUT OF SPECIFIC SALES OF PERSONAL INFORMATION

Consumers may wish to allow businesses to sell their personal information for some reasons, but not others. Clarifying that businesses may offer consumers choices instead of an "all or nothing" approach will give consumers greater control over their personal information.

1. Current Law: § 1798.135(a)(1)

a. A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers: ... [p]rovide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. A business shall not require a

consumer to create an account in order to direct the business not to sell the consumer's personal information.

2. Problem with Current Law: A One-Size Fits All “Do Not Sell” Link is Over-Inclusive

a. Consider a consumer who would like to receive promotional messages from some, but not every, third party to which a business sells personal information (for example, in their specific areas of interest). Providing the consumer with choices for opting out of some or all sales respects the consumer's choice.

3. [Proposed] Regulatory Solution to Problem

a. The AG's office will insert clarifying language: “Clarification of § 1798.135: A business shall be deemed in compliance with Section 1798.135 if it provides consumers with choices from which to opt out including the choice to ‘Opt Out of All Sales of My Personal Information.’”

C. ISSUE: CONSUMERS AFFIRMATIVELY OPTING-IN SHOULD NOT BE INCLUDED IN THE GLOBAL “DO NOT SELL MY PERSONAL INFORMATION” REQUIREMENT

1. Current Law: § 1798.135(a)(1)

a. A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers: ... [p]rovide a clear and conspicuous link on the business's Internet homepage, titled “Do Not Sell My Personal Information,” to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

2. Problem with Current Law: The Global “Do Not Sell” Choice Disincentivizes Businesses from Offering Opt-In Choices

a. If a business engages in the sale of personal information pursuant only to a consumer's opt-in consent, such sales should not need to be included as part of any “Do Not Sell My Personal Information” choice. Any interpretation to the contrary would result in a disincentive for businesses to offer opt-in options. For example, if a consumer's specific choice to opt-in could be reversed by a global “Do Not Sell My Personal Information” choice, consumers will be confused and businesses will lack an incentive to offer opt-in choices. Consumers would not expect that if they had affirmatively opted-in to a particular program, that it would be “undone” by a global “Do Not Sell My Personal Information” choice. A

consumer would expect to interface with the business specifically as it relates to that program if they later decide to opt out. Accordingly, so long as businesses provide consumers with a mechanism to subsequently opt-out of sales for which they had previously opted in, such opt-out need not be included as a global “Do Not Sell My Personal Information” choice. This suggestion is similar to operation of do not call lists, whereby consumers who consent to a business calling them are not subject to do not call prohibitions.

3. [Proposed] Regulatory Solution to Problem

a. The AG’s office will insert clarifying language: “Clarification of § 1798.35(a)(1): Where consumers’ opt-in consent has been obtained and such consumers are subsequently provided with a mechanism to opt out, businesses shall be deemed to be in compliance with Section 1798.135 and shall not need to provide consumers with the ability to opt-out of such program through a ‘Do Not Sell My Personal Information’ link or logo.”

D. ISSUE: NEW AGE CATEGORY (AGES 13-16) FOR OPT-IN CONSENT CREATES POTENTIAL BURDEN ON BUSINESSES TO IDENTIFY AGE OF CONSUMERS, JEOPARDIZING PRIVACY, AND CREATES INCONSISTENCIES WITH FEDERAL LAW

This title could arguably impose obligations on businesses to verify that its consumers are not children, even if a business does not target children or offer goods and services to children. Clarification is needed that businesses that do not target or offer goods or services to children or have actual knowledge that the information they are collecting is from an individual under 16 do not need to comply with these obligations. Doing so will better align with the federal Children’s Online Privacy Protection Act¹¹ (“COPPA”) and remove any incentive businesses may otherwise have to collect additional information.

1. Current Law: § 1798.120(c)

a. Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer’s parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer’s personal information. A business that willfully disregards the consumer’s age shall be deemed to have had actual knowledge of the consumer’s age. This right may be referred to as the “right to opt-in.”

¹¹ Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505.

2. Problem with Current Law: Burdensome to Implement

a. Consider a business that sells goods (e.g., cars, homes, landscaping products, pesticides, etc.) or services (e.g., financial products, accounting services, home remodeling, etc.) targeted at consumers aged 16 years or older. As the only consumers entitled to purchase these items are above 16 years of age, such businesses should not be required to identify consumers by age.

b. As the term “willfully disregards” is not defined within the statute, the AG is encouraged to clarify in its rulemaking that “willfully disregards” means that a business intentionally or deliberately disregards or ignores information a consumer provides about his/her age. The AG should not encourage general audience services to require users to provide their date of birth to help protect against liability, which would be contrary to well-established privacy principles.

3. [Proposed] Regulatory Solution to Problem

a. The AG’s office will clarify existing language as follows:

(1) “Clarification of § 1798.120(c): The CCPA contemplates that businesses not targeting or offering goods or services of interest to children under the age of 16 and who do not have actual knowledge that a consumer is under 16 are not required to comply with the obligations of this section.”

(2) “Clarification of § 1798.120(c): The CCPA contemplates that a business that processes personal information in accordance with the federal Children’s Online Privacy Protection Act (“COPPA”) will not be deemed in violation of this title with regard to the processing of personal information of children under the age of 13 years.”

V. ATTORNEY GENERAL MANDATE: ESTABLISH RULES, PROCEDURES AND EXCEPTIONS RELATING TO NOTICES AND INFORMATION TO CONSUMERS, INCLUDING FINANCIAL INCENTIVE OFFERINGS (§ 1798.185(A)(6))

A. ISSUE: BUSINESSES SHOULD BE ABLE TO INFORM CONSUMERS OF THEIR PERSONAL INFORMATION PRACTICES AT, OR BEFORE, THE POINT OF COLLECTION THROUGH THEIR PRIVACY POLICIES

Businesses are required to provide notice of their personal information practices to consumers at or before the point of collection; however, this can be burdensome for transactions in a physical space or when businesses do not have a direct relationship with consumers. Allowing businesses

to provide notice by placing the information in their online privacy policies may be the only way that many businesses can practically comply with this requirement.

1. Current Law: § 1798.100(b)

a. A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

2. Problem with Current Law: Notification Directly to Consumers Can be Impracticable or Impossible where Personal Information is Collected from Physical Locations or Public Sources as Opposed to Online Interactions

a. For transactions occurring in a physical space, such as a store, movie theater, or amusement park, it may be burdensome for the business to reliably and efficiently provide the consumer with the categories of personal information collected.

b. Businesses that do not have direct consumer accounts or otherwise maintain relationships with consumers cannot provide privacy notices on their websites and may therefore arguably be unable to be in compliance with the CCPA. Allowing businesses to provide notice on their website solves this problem and is consistent with this title's specification of homepage notice to meet the additional pre-sale notice requirement of subsection 1798.115(d).

c. If the law requires that full, detailed notices be given every single time personal information is collected, this would be an administrative and ineffective burden for businesses and an unpleasant customer service experience for consumers. Due to the broad definition of personal information and collection under this title, businesses that collect information through security cameras, in store purchases, or other sources like public social media profiles would need to give detailed notices regarding such collection. It may be difficult and, if attempted, ineffective to provide notice at each point of collection and providing consumers with too many notices would likely result in consumer fatigue, where consumers become frustrated and gloss over the notices, which means such notices will lack their intended impact. For example, consider a consumer walking into a physical store. The store has a CCTV camera to identify and prevent fraud. The consumer entering the store has a mobile app that alerts the store of the consumer's presence and location within the store. The consumer makes a purchase with a credit card. If each one of

these personal information collection points requires detailed notice to the consumer, retail space would be cluttered, and the consumer may be frustrated and experience notice fatigue. In these circumstances, a short notice at each point of collection that directs users to the full online notice should suffice.

3. [Proposed] Regulatory Solution to Problem

a. The AG's office will insert clarifying language: "Clarification of Section 1798.100(b): Privacy policies posted online are considered adequate notice under § 1798.100(b) where they contain the required information. Businesses with which consumers do not maintain accounts may comply with the information and notice requirement of § 1798.100(b) by providing the required information and notice on the businesses' Internet homepage or within their posted privacy policy. Businesses without Internet websites may comply by posting such information and notice, including short notices that direct consumers to online notices, in a clear and conspicuous location at their places of business."

B. ISSUE: GUIDANCE NEEDED ON CCPA-COMPLIANT FINANCIAL INCENTIVES

Businesses and consumers would benefit from examples of permitted financial incentives, including those incentive programs -- like loyalty cards, gift cards, and coupons -- that have long been enjoyed by businesses and consumers alike. Having the AG provide examples of permitted financial incentives would provide much needed guidance.

1. Current Law: § 1798.125(b)(4)

a. A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

2. Problem with Current Law: Obstacles to Implementation

a. There are many consumer loyalty programs that have been developed in the past twenty years that could arguably be challenged under this provision. Both businesses and consumers have come to rely on and enjoy such loyalty programs that provide benefits to both businesses and consumers, and such programs do not appear to have been intended to be targeted by the CCPA. In the absence of clarity on this issue, however, businesses may be reluctant to innovate and add new programs to the marketplace if they perceive significant risk under CCPA.

b. Businesses also use gift cards and coupons as incentives to get consumers to provide more information to help provide better service to consumers (e.g., fill out a survey and receive a \$20 gift card; sign up for a newsletter and receive a \$5 promo code).

3. [Proposed] Regulatory Solution to Problem

a. The AG's office will insert clarifying language: "Clarification of Section 1798.125(b)(4): A business may offer financial incentives, including payments to consumers as compensation or discounts for the collection, sale, or deletion of personal information. A business may decline to offer financial incentives or price, rate, level, or quality of goods or services differentials to consumers who opt out of the sale of personal information related to provision of such benefits. The following are examples of financial practices that would not be unjust, unreasonable, coercive, or usurious:

- (1) Loyalty programs
- (2) Gift cards and the use of gift cards as financial incentives
- (3) Coupons and the use of gift cards as financial incentives
- (4) Direct payments to consumers as compensation."

b. The AG's office will insert clarifying language: "Clarification of Section 1798.125(a): A business may decline to offer financial incentives to consumers when a consumer refuses such financial incentives, fails to consent to the collection of personal information, or requests deletion of personal information related to provision of such incentives."

VI. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES FOR VERIFYING CONSUMER REQUESTS AND OTHER NECESSARY REGULATIONS TO FURTHER PURPOSES OF THE TITLE (§ 1798.185(A)(7))

A. ISSUE: CCPA CLEARLY STATES THAT JANUARY 1, 2020 IS THE EFFECTIVE DATE; THEREFORE, THE 12-MONTH LOOKBACK PERIOD SHOULD NOT BE MISINTERPRETED BY CONSUMERS OR REGULATORS TO BEGIN PRIOR TO THE EFFECTIVE DATE

1. Current Law: § 1798.130(a)(3)(B)¹² *see also* § 1798.130(a)(4)(B)-(C); § 1798.130(a)(5)

a. § 1798.130(a)(3)(B): "For purposes of subdivision (b) of Section 1798.110...[i]dentify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected."

¹² *See also* § 1798.130(a)(4)(B)-(C); § 1798.130(a)(5).

b. § 1798.130(a)(4): “For purposes of subdivision (b) of Section 1798.115....

(1) § 1798.130(a)(4)(B): “Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer’s personal information was sold in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold.

(2) § 1798.130(a)(4)(C): “Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer’s personal information was disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed.”

2. Problem with Current Law: Confusion Regarding Start of Lookback Period

a. As currently written, the CCPA becomes effective January 1, 2020; however, there remains confusion among consumers regarding the applicability of the 12-month lookback period (Section 1798.130(a)). As the effective date is clearly stated as January 1, 2020, Section 1798.130(a) should not be misinterpreted by consumers to apply prior to the title’s effective date or the effective date of AG regulations.

3. [Proposed] Regulatory Solution to Problem

a. The AG’s office will insert clarifying language: “Clarification of the Lookback Period (§ 1798.130(a)(3)(B)), § 1798.130(a)(4)(B)-(C); § 1798.130(a)(5)): The 12-month lookback period shall apply from the effective date of this title, such that it will not encompass processing activities taking place prior to January 1, 2020 [or the effective date of AG regulations].”

B. ISSUE: REGULATIONS NEEDED RELATING TO HOW TO VERIFY AUTHORIZATION OF THIRD-PARTIES WHO MAKE CONSUMER REQUESTS SO CONSUMER PRIVACY IS NOT UNDERMINED

Since consumers' personal information is at risk when information is transmitted in response to consumer requests, businesses need guidance on how to verify and comply with third-party requests.

1. Current Law: § 1798.135(c) and § 1798.140(y)

a. § 1798.135(c): A consumer may *authorize another person* solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt-out request *received from a person authorized by the consumer to act on the consumer's behalf*, pursuant to regulations adopted by the Attorney General. (Emphasis added)

b. § 1798.140(y): "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, *authorized by the consumer to act on the consumer's behalf*, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf. (Emphasis added)

2. Problem with Current Law: Lack of Guidance for Businesses

a. Businesses need guidance on ways to verify that third parties are authorized agents acting on behalf of consumers, otherwise businesses risk disclosing information to unauthorized representatives of consumers.

b. Businesses also need to be protected from the inherent risks accompanying the disclosure of personal information to third parties. For example, if a business uses a reliable or sanctioned method to verify third party authorization, the business should not be found to be in violation of the CCPA if the consumer did not actually authorize the disclosure.

3. [Proposed] Regulatory Solution to Problem

a. The AG's office shall clarify existing language as follows:
“Clarification of § 1798.135 and § 1798.140(y): § 1798.135 and § 1798.140(y) of the CCPA contemplate that when businesses respond to consumer requests made by third-party agents registered with the California Secretary of State, they are not in violation of this title to the extent they rely on such registration. The Secretary of State's registry must correlate the permissions granted by the consumer to the registered agent.”

b. The AG's office shall clarify existing language as follows:
“Clarification of § 1798.135 and § 1798.140(y): § 1798.135 and § 1798.140(y) of the CCPA contemplate that when businesses respond to consumer requests when provided proof of appointment as a consumer's legal guardian, conservator, fiduciary, or similar legally authorized and recognized person, they are not in violation of this title. Where a third-party requestor has not sufficiently demonstrated that it is authorized to make a request on the consumer's behalf, a business shall not be obligated to comply with the request.”

C. **ISSUE: REGULATIONS NEEDED ON HOW CONSUMER REQUESTS CAN BE SUBMITTED AND PROCESSED TO MAINTAIN THE CONFIDENTIALITY AND SECURITY OF PERSONAL INFORMATION**

Businesses need guidance and protection from claims of liability when responding to consumer requests. Since personal information is at risk of being exposed, setting a reasonableness requirement and allowing businesses to provide different verification methods for account holders and non-account holders will provide businesses with necessary guidance, flexibility, and protection to mitigate risks to personal information.

1. **Current Law: § 1798.140(y)**

a. § 1798.140(y): “Verifiable consumer request” means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, *authorized by the consumer to act on the consumer's behalf*, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a

person authorized by the consumer to act on such consumer's behalf.
(Emphasis added)

2. Problem with Current Law: Lack of Guidance for Businesses

a. Verification is critically important to ensure that a consumer's personal information is released only after the consumer's identity can be confirmed. Businesses should have flexibility in how they verify such consumers and their requests, and specific methods should not be delineated. This will allow for the development of innovative methods to ensure personal information is not improperly disclosed.

b. Considering the potential harm if personal information is improperly disclosed, businesses should have discretion to determine whether a consumer has been properly verified, particularly when the consumer does not hold an account with the business. Very often, businesses verify individuals during the course of account formation – when an account is not present or lacking in necessary information, verification is more difficult. Businesses should be permitted to err on the side of caution and not disclose information when a consumer has not been properly verified.

3. [Proposed] Regulatory Solution to Problem:

a. The AG's office will provide guidance for businesses as follows: "Guidance for Submitting Requests for Account Holders and Non-Account Holders: Businesses may provide a self-service portal for consumers to view or extract their personal information. For businesses maintaining consumer accounts, businesses may assume that a consumer request submitted through a password-protected account maintained with the business is sufficient to consider it reasonably verified. For businesses not maintaining consumer accounts, businesses may use personal information supplied by the consumer in the self-serve portal to verify their identity through their own means or the use of a third-party identity verification service. If consumer identity cannot be verified, the business is not obligated to provide access to the requested personal information."

b. The AG's office shall clarify existing language as follows: "Clarification of § 1798.140(y): § 1798.140(y) of the CCPA contemplates that when businesses maintain a reasonable, documented procedure to verify the identity of a consumer who has submitted a request to exercise a right granted under this title, or the authority of a person making the request on behalf of a consumer, businesses shall not be held liable, in either an action by the Attorney General or a private action, for the unauthorized disclosure of personal information in connection to any response to such request. A procedure shall be considered *per se* reasonable if it calls for any of the following, either exclusively or in the

alternative: the verification of identity through the collection of a government-issued identification; or the verification of identity by matching of at least three of the following types of information provided by the consumer, or the person authorized to make a request on behalf of a consumer, with a consumer profile maintained by the business: full name, email address, telephone number, mailing address, and something the business provides to a consumer, e.g., a pin code.”

c. The AG’s office will provide guidance for businesses as follows: “Guidance for Processing Consumer Requests: If a business does not automate verification, it can consider a single team to broker consumer requests.”

D. ISSUE: ALLOWING DISCLOSURE OF “SPECIFIC PIECES OF INFORMATION” FOR CONSUMER RIGHTS OTHER THAN THE RIGHT TO ACCESS REQUESTS WOULD CREATE UNNECESSARY CYBERSECURITY RISKS AND CONTRADICT THE TEXT OF THE STATUTE

Businesses may collect sensitive information (e.g., social security numbers, credit cards, health information). Delivery of this sensitive information to consumers in response to a request to know information collected, sold, or disclosed for a business purpose may present unnecessary cybersecurity risks that can be avoided by providing a response describing the sensitive data collected rather than requiring its disclosure.

1. Current Law: § 1798.100(a), § 1798.110(a)(5), § 1798.110(c)(5)

a. § 1798.100(a): “A consumer shall have the right to request that a business that collects a consumer’s personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.”

b. § 1798.110(a)(5): “A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following... [t]he specific pieces of personal information it has collected about that consumer.”

c. § 1798.110(c)(5): “A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130... [t]he specific pieces of personal information the business has collected about that consumer.”

2. Problem with Current Law: Privacy and Cybersecurity Risks by Disclosure of Personal Information

a. Consider a business providing specific pieces of personal information in response to a consumer’s request: By responding to the consumer’s request with specific pieces of personal information (e.g., the

consumer's social security number, credit card numbers, passport number, health information, and driver's license information), the business' disclosure may actually expose such personal information to potential cybersecurity risks. The potential harm to consumers associated with business disclosing specific pieces of personal information far outweighs the slight benefit to consumers receiving such information as they are already aware of the specific numbers and other information they may be requesting.

b. Consider a business providing specific pieces of personal information in response to a consumer's request for information relating to his/her household: By providing specific pieces of personal information relating to the requesting consumer's household, the business could expose another household member's personal information.

3. [Proposed] Regulatory Solution to Problem

a. The AG's office will insert clarifying language: "Clarification of Disclosure Obligations Relating to Specific Categories of Personal Information (§ 1798.100(a), (c), and (d); § 1798.110 (a) and (c):

(1) A business may comply with consumer requests pertaining to "specific pieces" of personal information by describing the personal information at issue or effectively masking the same without transmitting precise pieces of personal information that would fall into the categories in Section 1798.81.5 (e.g., social security numbers, credit card numbers, financial account numbers, health information). For example, rather than provide the exact social security number it has collected, a business may provide a report advising that it has collected the consumer's social security number."

E. ISSUE: THIRD PARTIES WHO DO NOT HAVE DIRECT RELATIONSHIPS WITH CONSUMERS CANNOT NOTIFY THEM THAT THEIR PERSONAL INFORMATION HAS BEEN SOLD

1. Current Law: § 1798.115(d)

a. "A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120."

2. Problem with Current Law: Third Parties Do Not Have Direct Relationship with Consumers

a. Under the CCPA, a third party does not have a direct relationship with the consumer and, therefore, must rely on the businesses collecting

the personal information to provide consumers with the explicit notice regarding the third party's intent to sell the personal information in order to ensure compliance with this CCPA provision.

3. [Proposed] Regulatory Solution to Problem

a. The AG's office will insert clarifying language: "Clarification of Third Party's Consumer Notice Obligations (§ 1798.115(d)): To comply with Section 1798.115(d), third parties may rely on a business' written attestation that it has provided consumers with: (1) 'explicit' notice of the third party's intent to sell personal information, and (2) the opportunity to exercise the CCPA right to opt out of such sale."

F. ISSUE: CLARIFYING THAT BUSINESSES ARE NOT REQUIRED TO RETAIN PERSONAL INFORMATION SOLELY TO COMPLY WITH CONSUMER REQUESTS; ALSO DATA RETENTION TO COMPLY WITH THE 12-MONTH LOOKBACK PERIOD COULD VIOLATE DATA MINIMIZATION BEST PRACTICES

1. Current Law: § 1798.100(e); § 1798.130(a)(3)(B)¹³

a. § 1798.100(e): This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

b. § 1798.130(a)(3)(B): Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

2. Problem with Current Law: Privacy and Security Risks

a. Although § 1798.100(e) states that a business is not required to retain certain personal information, the AG should issue a clarification to confirm that the CCPA does not require businesses in any instance to retain personal information (e.g., to comply with potential, future, consumer requests). Any interpretation to the contrary would create additional privacy and security risks to consumers' personal information by potentially requiring businesses to retain personal information that they otherwise would not.

b. The law arguably requires businesses to maintain information for 12 months in order to comply with the lookback period when they may not

¹³ See also § 1798.130(a)(4)(B)-(C); § 1798.130(a)(5).

ordinarily retain data for 12 months. This encourages retention of data that may not otherwise be kept and potentially subjects consumers to higher risks of data exposure if a breach were to occur.

3. [Proposed] Regulatory Solution to Problem

a. The AG's office shall clarify as follows: "Clarification of § 1798.100(e): Businesses are not required to retain personal information solely to fulfill a consumer request. Under no circumstances is a business required to retain personal information solely for the purpose of fulfilling a consumer request made under this title."

b. The AG's office shall clarify as follows: "Clarification of § 1798.130 (a)(3)-(4): The 12-month lookback provisions do not require businesses to retain data longer than necessary. Further, businesses need not retain data that they would otherwise delete in anticipation of responding to 12-month lookback inquiries."

c. The AG's office will clarify existing language as follows: "Clarification of § 1798.100(e): § 1798.100(e) of the CCPA contemplates that when businesses retain data associated with the processing a consumer request in accordance with its records retention schedule, they will not be deemed violation of this section."

G. ISSUE: EMPLOYMENT AND BUSINESS-RELATED DATA

1. Current Law: § 1798.140(g)

a. "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

2. Problem with Current Law: Employees Should Not Be Considered Consumers, and business-to-business communications should not be covered

a. **Employees should not be covered.** Section 1798.125 makes it clear that this title relates to businesses providing goods and services *to consumers*. An interpretation that this title applies to employees risks inconsistencies with the already existing California state framework relating to employees and their access to employment information, including the following from the California Labor Code: Section 1198.5 (personnel files); Section 226(b) (payroll records); and Section 432 (employee access to signed instruments). Excluding employees and

related commercial actors in the business context is consistent with similar proposed legislation in other states.¹⁴

b. In the absence of an interpretation that excludes employees from the definition of consumer, a business, upon request from a consumer/employee, might mistakenly think it is required to delete and/or provide access to investigative records related to employee misconduct, including, without limitation, sexual harassment.

c. An employee data exemption should include proactive marketing activities associated with employee/contractor recruitment. Consider a circumstance where a business' human resources team proactively promotes job opportunities within the company. This should not be considered marketing because of its fundamental HR objective.

d. **Business-to-business communications should not be covered.** Section 1798.125 relates only to businesses providing goods and services to consumers, not other businesses. These types of communications are used to facilitate business communications, such as for invoices, and are not the type of transactions that could compromise the privacy of any one customer. Consider the situation of an office supply company from which a business orders pencils, pens, and paper. In order to do so, a business employee exchanges emails with the office supplier's employee on the office supplier employee's personal email. After the office supplier has completed the delivery, the business asks to have all of its data deleted before the invoice is delivered, thereby preventing proper invoicing for the goods delivered. This type of transaction does not fall within any reasonable interpretation of the CCPA.

e. The AG should clarify that the definition of "consumer" does not include individual business owners acting in their commercial capacity, employees, and agents of businesses. There are first amendment concerns with limiting access to information about business owners, officers, directors, employees, and their representatives. Publishers of such information (e.g., online review services) have a right to free speech under the US and California constitutions. California consumers have a legitimate interest in information about individually-owned businesses in their community, which outweighs business owners' right to privacy.

3. [Proposed] Regulatory Solution to Problem

a. The AG's office shall clarify as follows: "Clarification of § 1798.140(o): Definition of Personal Information: The rights in this title do not extend to personal information collected by a business in

¹⁴ See e.g., proposed Washington bill Senate Bill 5376 Section 3(3) which explicitly excludes natural persons acting in a commercial or employment context, available at <http://lawfilesexternal.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/5376-S2.pdf>

connection with: (i) an individual's application or role as an employee, contractor, or agent, or (ii) a business counterparty in a business-to-business relationship. Such interpretations are consistent with this title."

b. The AG's office shall clarify as follows: "Clarification of § 1798.140(g): Definition of Consumer: The definition of consumer shall exclude current and former employees, prospective employees, recruitment candidates, owners, directors, contractors, vendors, agents, or authorized representative of the business, such as directors, or of any other legal or government entity, acting in the capacity of these roles."

H. ISSUE: OBSTACLES TO DETERMINING WHO IS A CALIFORNIA CONSUMER

1. Current Law: § 1798.140(g); 18 CCR § 17014

a. "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

b. The term "resident," as defined in the law, includes (1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. All other individuals are nonresidents.

2. Problem with Current Law: No Streamlined Way to Determine Who is a California Consumer

a. Businesses do not have a method to determine: 1) every individual who is in the State for other than a temporary or transitory purpose, and 2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose that would qualify then to be consumer under Section 1798.140(g). Moreover, businesses do not have a method to determine who is a California "income tax payer."

3. [Proposed] Regulatory Solution to Problem

a. The AG's office shall clarify as follows: "Clarification of § 1798.140(g): Definition of Personal Information: Consumers can prove that they are California consumers by providing a California mailing address and/or or any other proof of residency that may be requested by business."

I. ISSUE: REASONABLE SECURITY AND PRIVATE RIGHT OF ACTION

1. Current Law: § 1798.150(a)(1)

a. Any consumer whose nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following...[.]

2. Problem with Current Law: Discourages Compliance with Reasonable Security

a. Since the AG has created standards for personal data protection (*see e.g.*, California Data Breach Report), compliance with those standards should protect a business from claims of liability. Such a safe harbor would confirm that the AG standards amount to reasonable security. Note that CIS Critical Security Controls overlap significantly with other accepted data security standards such as the NIST Cybersecurity Framework and ISO 27001.

b. Similarly, compliance with commonly accepted data security “best practices” standards should protect a business from liability for unauthorized access, exfiltration, theft, or disclosure of personal information – similar to Ohio’s recently enacted safe harbor for businesses maintaining a recognized cybersecurity program (Ohio Rev. Code § 1354.02).

3. [Proposed] Regulatory Solution to Problem

a. The AG’s office will clarify existing language as follows:
“Clarification of § 1798.150: § 1798.150 of the CCPA contemplates that when businesses maintain compliance with a recognized data security standard (e.g., CIS Critical Security Controls, NIST Cybersecurity Framework or NIST 800-53, ISO 27001 *et. seq.*, or PCI), businesses are immune from suit under § 1798.150. Implementation of such recognized data security standards is a defense to enforcement actions or suits under § 1798.150.”

b. The AG’s office shall clarify existing language as follows:
“Clarification of § 1798.150(a)(1): § 1798.150(a)(1) of the CCPA contemplates that when businesses maintain personal information within a recognized cybersecurity program conforming to the requirements of Ohio Rev. Code § 1354.02, such businesses shall not be deemed to be in violation of this title.”

J. ISSUE: RIGHT TO CURE ALLEGED VIOLATIONS DOES NOT COMPORT WITH BEST SECURITY PRACTICES

1. Current Law: § 1798.150(b) and Various Security Frameworks

a. Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

b. Established security resources and frameworks (e.g., NIST, SANS, ISO, CIS) recommend that businesses take certain steps to remediate security risks (e.g., root cause analysis, impact assessment, plans to prevent reoccurrence of the incident).

2. Problem with Current Law: Businesses Following Recommended Guidance May Find Themselves Subject to Claims They Have Violated a Written Statement

a. Consider the situation where a business has suffered a security breach based upon a cybercriminal's unauthorized access to the business' system. The business follows recognized best practices for incident response, including completing a zero-sum analysis concluding that risks have been mitigated. Unbeknownst to the business, the initial malware contained a "poison pill" that was programmed to lie dormant in the business' system until six months after the original incident was mitigated. Under the current law, a consumer could take the position that the "written statement" provided by the business was "violated" because the business was breached again. This is true, even though there would have been no way to detect this strain. Sophisticated cybercriminals are often

experienced in pre-programming malware to contain variants that make new strains of the malware very difficult to detect.¹⁵

3. [Proposed] Regulatory Solution to Problem

a. The AG's office shall clarify existing language as follows:
“Clarification of § 1798.150(b): § 1798.150(b) of the CCPA contemplates that when businesses document adherence to accepted cybersecurity remediation steps including: (1) a root cause investigation; (2) an impact assessment; and (3) development and implementation of plans to prevent reoccurrence of the event, such documentation shall represent *prima facie* evidence of curing the incident.”

K. ISSUE: “SERVICE PROVIDERS,” “THIRD PARTIES,” AND “PERSONS” SERVICE PROVIDERS (§ 1798.140 (V)), THIRD PARTIES (§ 1798.140 (W)) AND (LIABILITY SHIFTED) PERSONS (1798.140(W)(2)) SHOULD ALL BE TREATED THE SAME FOR PURPOSES OF § 1798.140 (T)(2), MEANING THAT THE EXCEPTIONS TO “SALE” APPLY EQUALLY TO TRANSFERS TO “SERVICE PROVIDERS,” “THIRD PARTIES,” AND “PERSONS”

1. Current Law: § 1798.140(w)(2)¹⁶

a. A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:

(1) Prohibits the person receiving the personal information from:

(a) Selling the personal information.

(b) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.

(c) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

¹⁵ Newtec Services, *Malware & Exploit Attacks Explained*, Nov. 8, 2017, <https://newtecservices.com/malware-exploit-attacks-explained/>

¹⁶ See also § 1798.140(w)(2), § 1798.140(v), and § 1798.140(t)(1)(C).

(1) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

(d) A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.

2. Problem with Current Law: Overly Burdensome on Businesses to Sign Vendor Contracts Substantially Similar to Those Signed under GDPR and Treats “Service Providers,” “Third Parties,” and “Natural Persons” Unequally

a. Many businesses have expended significant resources and some are still struggling to execute data protection agreements with vendors that contain the necessary GDPR Article 28 requirements. These requirements are substantially similar to the requirements in § 1798.140(v) and § 1798.140(w)(2).

b. The CCPA only exempts service providers and third parties under certain circumstances from the definition of sale. The exemptions should be uniformly applied to service providers, third parties and persons that meet the requirements of § 1798.140(w)(2).

c. The AG should also clarify that service providers (§ 1798.140(v)), persons that meet the requirements under § 1798.140(w)(2), and third parties (§ 1798.140(w)) shall all be exempt from the definition of sale as described in § 1798.140(t)(2), meaning that the exceptions to “sale” apply equally to transfers to “service providers,” “third parties,” and “persons,” all bound not to use personal information for unrelated purposes.

3. [Proposed] Regulatory Solution to Problem

a. The AG’s office shall clarify as follows: “Clarification of § 1798.140(w)(2): § 1798.140(w)(2) of the CCPA contemplates that when businesses have executed contracts with processors in compliance with Article 28 of the General Data Protection Regulation, they shall not be in violation of § 1798.140(w)(2)(B).”

b. The AG's office shall clarify as follows: "Clarification of §1798.140(t)(2): §1798.140(t)(2) of the CCPA contemplates that §1798.140(t)(2) shall apply equally to service providers (as defined in 1798.140(v), third parties (as defined in § 1798.140(w), and persons that meet the requirements § 1798.140(w)(2), as long as the service providers, third parties and persons satisfy the conditions of § 1798.140(t)(2)."

L. ISSUE: GUIDANCE NEEDED ON HOW SERVICE PROVIDERS SHOULD RESPOND TO VERIFIABLE CONSUMER REQUESTS

Since service providers have indirect obligations under the CCPA, guidance is needed on how they should respond to consumers who send requests directly to them instead of businesses, and how service providers can assist businesses with their obligations in ways that support the objectives of the CCPA. Requiring that service providers: (1) inform consumers that they need to direct their requests to businesses promotes the objectives of the CCPA by informing consumers of the appropriate way to make requests, and (2) reasonably assist businesses ensures that consumers do not experience unnecessary hurdles when requesting from businesses information held by third-party service providers.

1. Current Law: § 1798.105(c)

a. A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

2. Problem with Current Law: No Clear Guidance for Service Providers

a. Service providers have indirect obligations under the CCPA and need guidance on how to fulfill their role under the CCPA. AG guidance on this issue will also allow businesses to provide clearer and more direct direction to service providers.

3. [Proposed] Regulatory Solution to Problem

a. The AG's office should provide guidance as follows: "Guidance for Service Providers When Responding to Consumer Requests: If a service provider receives a request from a consumer, the service provider will have no obligation to respond to a request from a consumer where the service provider does not have a direct relationship, as a business, with the consumer. The service provider may respond with an explanation that the request should be submitted to the business with whom the consumer has the direct relationship."

APPENDIX OF PROPOSED REGULATORY LANGUAGE IN SUPPORT OF CALCHAMBER REPORT

This appendix is a compendium of all the regulatory proposals included in the CalChamber Report and is provided for the AG Office convenience, only.



Appendix of Proposed Regulatory Solutions in Support of California Chamber of Commerce Comments to the California Attorney General’s Office for CCPA Rulemaking March 8, 2019

SARAH BOOT

DOMINIQUE SHELTON LEIPZIG

SARI RATCAN

NATASHA AMLANI

POLICY ADVOCATE

PARTNER

SENIOR COUNSEL

ASSOCIATE

Table of Contents

	Page
I. ATTORNEY GENERAL MANDATE: UPDATE CATEGORIES OF PERSONAL INFORMATION (§ 1798.185(A)(1))	1
A. [Proposed] Regulatory Solution to Problem Re: Literal Adherence to The CCPA Would Require Businesses To Respond To Consumer Rights Requests By Providing Personal Information About An Entire Household Or Device, Thereby Reducing Privacy Protections (CalChamber Report, Section I.A.3)	1
B. [Proposed] Regulatory Solution to Problem Re: Inclusion Of “Capable of Being Associated With A Consumer” In The Definition Of Personal Information Is Too Broad To Provide Guidance For Business (CalChamber Report, Section I.B.3)	1
C. [Proposed] Regulatory Solution to Problem Re: Pseudonymized Information Is Not Reasonably Linkable to A Specific Consumer, So Businesses Should Not Be Required to Re-Link It (CalChamber Report, Section I.C.3)	2
D. [Proposed] Regulatory Solution to Problem Re: Clarification of Deidentified Definition Is Needed To Cover Existing Deidentification Efforts Undertaken By Companies That Render Data Not Reasonably Linkable To An Individual (CalChamber Report, Section I.D.3)	2
II. ATTORNEY GENERAL MANDATE: ESTABLISH EXCEPTIONS TO COMPLY WITH STATE OR FEDERAL LAW (§ 1798.185(a)(3))	2
A. [Proposed] Regulatory Solution to Problem Re: Lack of Intellectual Property Exception Disincentivizes Business Innovation (CalChamber Report, Section II.A.3)	2
B. [Proposed] Regulatory Solution to Problem Re: Fraud Exemption Does Not Expressly Incorporate Enough of The Laws and Regulations Businesses Use To Keep Consumer Information Safe (CalChamber Report, Section II.B.3)	3
C. [Proposed] Regulatory Solution to Problem Re: Narrow Definition Of “Publicly Available Information” Minimally Protects Privacy to The Exclusion of Businesses That Provide Societal and State Benefits (CalChamber Report, Section II.C.3)	3
III. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES RELATING TO CONSUMER OPT-OUT RIGHTS (§ 1798.185(A)(4))	4

A.	[Proposed] Regulatory Solution to Problem Re: Additional Locations to Solicit Opt-Out Requests Are Needed (CalChamber Report, Section III.A.3)	4
IV.	ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES: (1) TO FACILITATE AND GOVERN THE SUBMISSION OF A CONSUMER OPT-OUT REQUEST; AND (2) FOR THE DEVELOPMENT AND USE OF A RECOGNIZABLE AND UNIFORM OPT-OUT LOGO OR BUTTON (§ 1798.185(A)(4)(A) AND (C))	4
A.	[Proposed] Regulatory Solution to Problem Re: Create A Sanctioned “Do Not Sell” Logo for Consumers to Easily Recognize How To Opt Out Of The Sale Of Their Personal Information (CalChamber Report, Section IV.A.3)	4
B.	[Proposed] Regulatory Solution to Problem Re: Businesses Are Not Able to Offer Consumers the Choice To Opt-Out Of Specific Sales Of Personal Information (CalChamber Report, Section IV.B.3)	4
C.	[Proposed] Regulatory Solution to Problem Re: Consumers Affirmatively Opting-In Should Not Be Included in The Global “Do Not Sell My Personal Information” Requirement (CalChamber Report, Section IV.C.3)	4
D.	[Proposed] Regulatory Solution to Problem Re: New Age Category (Ages 13-16) For Opt-In Consent Creates Potential Burden on Businesses to Identify Age of Consumers, Jeopardizing Privacy, And Creates Inconsistencies With Federal Law (CalChamber Report, Section IV.D.3)	6
V.	ATTORNEY GENERAL MANDATE: ESTABLISH RULES, PROCEDURES AND EXCEPTIONS RELATING TO NOTICES AND INFORMATION TO CONSUMERS, INCLUDING FINANCIAL INCENTIVE OFFERINGS (§ 1798.185(A)(6))	6
A.	[Proposed] Regulatory Solution to Problem Re: Businesses Should Be Able to Inform Consumers of Their Personal Information Practices At, Or Before, The Point of Collection Through Their Privacy Policies (CalChamber Report, Section V.A.3)	6
B.	[Proposed] Regulatory Solution to Problem Re: Guidance Needed on CCPA-Compliant Financial Incentives (Cal.Chamber Report, Section V.B.3)	6
VI.	ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES FOR VERIFYING CONSUMER REQUESTS AND OTHER NECESSARY REGULATIONS TO FURTHER PURPOSES OF THE TITLE (§ 1798.185(A)(7))	7
A.	[Proposed] Regulatory Solution to Problem Re: CCPA Clearly States That January 1, 2020 Is the Effective Date; Therefore, The 12-Month Lookback Period Should Not Be Misinterpreted By Consumers Or Regulators To Begin Prior To The Effective Date (CalChamber Report, Section VI.A.3)	7

B. [Proposed] Regulatory Solution to Problem Re: Regulations Needed Relating to How to Verify Authorization of Third-Parties Who Make Consumer Requests So Consumer Privacy Is Not Undermined (CalChamber Report, Section VI.B.3).....	7
C. [Proposed] Regulatory Solution to Problem Re: Regulations Needed on How Consumer Requests Can Be Submitted and Processed To Maintain The Confidentiality And Security Of Personal Information (CalChamber Report, Section VI.C.3)	8
D. [Proposed] Regulatory Solution to Problem Re: Allowing Disclosure Of “Specific Pieces of Information” For Consumer Rights Other Than the Right to Access Requests Would Create Unnecessary Cybersecurity Risks And Contradict The Text Of The Statute (CalChamber Report, Section VI.D.3)	8
E. [Proposed] Regulatory Solution to Problem Re: Third Parties Who Do Not Have Direct Relationships with Consumers Cannot Notify Them That Their Personal Information Has Been Sold (CalChamber Report, Section VI.E.3)	9
F. [Proposed] Regulatory Solution to Problem Re: Clarifying That Businesses Are Not Required to Retain Personal Information Solely to Comply with Consumer Requests; also Data Retention To Comply With The 12-Month Lookback Period Could Violate Data Minimization Best Practices (CalChamber Report, Section VI.F.3)	9
G. [Proposed] Regulatory Solution to Problem Re: Employment and Business Related Data (CalChamber Report, VI.G.3).....	9
H. [Proposed] Regulatory Solution to Problem Re: Obstacles to Determining Who Is a California Consumer (CalChamber Report, Section VI.H.3)	10
I. [Proposed] Regulatory Solution to Problem Re: Reasonable Security and Private Right Of Action (CalChamber Report, Section VI.I.3).....	10
J. [Proposed] Regulatory Solution to Problem Re: Right to Cure Alleged Violations Does Not Comport with Best Security Practices (CalChamber Report, Section VI.J.3)	10
K. [Proposed] Regulatory Solution to Problem Re: “Service Providers,” “Third Parties,” And “Persons” Service Providers (§ 1798.140 (V)), Third Parties (§ 1798.140 (W)) And (Liability Shifted) Persons (1798.140(W)(2)) Should All Be Treated The Same For Purposes Of § 1798.140 (T)(2), Meaning That The Exceptions To “Sale” Apply Equally To Transfers To “Service Providers,” “Third Parties,” And “Persons” (CalChamber Report, Section VI.K.3).....	10
L. [Proposed] Regulatory Solution to Problem Re: Guidance Needed on How Service Providers Should Respond to Verifiable Consumer Requests (CalChamber Report, Section VI.L.3).....	11

[Proposed] Regulatory Appendix

I. ATTORNEY GENERAL MANDATE: UPDATE CATEGORIES OF PERSONAL INFORMATION (§ 1798.185(A)(1))

A. [Proposed] Regulatory Solution to Problem Re: Literal Adherence to The CCPA Would Require Businesses To Respond To Consumer Rights Requests By Providing Personal Information About An Entire Household Or Device, Thereby Reducing Privacy Protections (CalChamber Report, Section I.A.3)

1. The AG's office will insert clarification language as follows:

“Clarification of § 1798.140(o)(1)(A); (x): The CCPA contemplates business compliance activities associated with responding to verifiable consumer requests with personal information pertaining only to the verifiable consumer. Further, the CCPA does not require businesses when, complying with a consumer rights request, to expose the personal information of household members or device users that cannot be differentiated from the requesting consumer, including situations where there are multiple profiles or other indications of multi-user activity.”

B. [Proposed] Regulatory Solution to Problem Re: Inclusion Of “Capable of Being Associated With A Consumer” In The Definition Of Personal Information Is Too Broad To Provide Guidance For Business (CalChamber Report, Section I.B.3)

1. The AG's office will provide instruction and clarification for businesses as follows:

- a. Clarification of § 1798.140(o)(1); § 1798.145(i): The CCPA contemplates business compliance activities associated with pseudonymous and other data not reasonably capable of association with a consumer. Further, the CCPA contemplates that consistent with California Civil Code Section 1798.145(a)(5), the obligations imposed on businesses by this title shall not restrict a business's ability to collect, use, retain, sell, or disclose consumer information that is not reasonably capable of being associated with, or linked, directly or indirectly, with a particular consumer, such as data held by a business in pseudonymous form.”
- b. “Clarification of § 1798.140(o)(1); § 1798.145(i): The CCPA contemplates business compliance activities associated with the implementation of a comprehensive privacy program and compliance with the FTC's definition of personal information.
- c. “Clarification of Section 1798.145(a)(1): Businesses that have (a) a comprehensive privacy program, (b) otherwise comply with FTC publications and guidance related to personal information that is reasonably linkable to an individual, and/or (c) treat consumer's personal information in alignment with the FTC's definition of

personal information are in compliance with this title.”

C. [Proposed] Regulatory Solution to Problem Re: Pseudonymized Information Is Not Reasonably Linkable to A Specific Consumer, So Businesses Should Not Be Required to Re-Link It (CalChamber Report, Section I.C.3)

1. The AG’s office will insert clarification language:

“Clarification of § 1798.140(o)(1)(A); § 1798.140(r); (x): For purposes of this title, businesses maintaining personal information in a manner that renders personal information no longer reasonably linkable to a specific consumer (e.g., pseudonymized data) are not required to re-identify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.”

D. [Proposed] Regulatory Solution to Problem Re: Clarification of Deidentified Definition Is Needed To Cover Existing Deidentification Efforts Undertaken By Companies That Render Data Not Reasonably Linkable To An Individual (CalChamber Report, Section I.D.3)

1. The AG’s office will insert clarification language:

“Clarification of § 1798.140(h): A company will be deemed to deidentify data if it meets recognized practices for deidentifying (e.g., FTC, HIPAA, or others). Also, for purposes of 1798.140(h)(2)-(3), “business processes” may include contractual requirements that prohibit reidentification and are designed to prevent inadvertent release of deidentified information.”

II. ATTORNEY GENERAL MANDATE: ESTABLISH EXCEPTIONS TO COMPLY WITH STATE OR FEDERAL LAW (§ 1798.185(A)(3))

A. [Proposed] Regulatory Solution to Problem Re: Lack of Intellectual Property Exception Disincentivizes Business Innovation (CalChamber Report, Section II.A.3)

The AG’s office will insert clarification language as follows: “Clarification of § 1798.185(a)(3): The CCPA contemplates business compliance activities associated with the protection of intellectual property. The CCPA does not require a business to comply with a consumer request, when such request would adversely affect or require disclosure of intellectual property subject to copyright, patent, trade or service mark, or trade secret protection, including any formula, pattern, compilation, program, device, method, technique, or process developed to process or analyze personal information, or any information derived from such process or analysis.”

B. [Proposed] Regulatory Solution to Problem Re: Fraud Exemption Does Not Expressly Incorporate Enough of The Laws and Regulations Businesses Use To Keep Consumer Information Safe (CalChamber Report, Section II.B.3)

1. The AG's office will provide clarification as follows:

"Clarification of § 1798.105(d)(2) and (8); § 1798.140(d)(2); § 1798.145(a): The CCPA contemplates business compliance activities associated or those with crime and fraud prevention activities including when it is necessary for a business or service provider to maintain the consumer's personal information in order to:

- (a) comply with corresponding federal, state, or local laws, rules and regulations; or
- (b) collect, use, retain, sell, authenticate, or disclose personal information in order to: (i) exercise, defend, or protect against legal claims; (ii) protect against or prevent security incidents; (iii) protect against or investigate, report, or prosecute those responsible for malicious, deceptive, or illegal activity; (iv) prevent, detect, or mitigate fraudulent activity; or (v) assist another person or government agency to conduct any of the activities specified in this section

C. [Proposed] Regulatory Solution to Problem Re: Narrow Definition Of "Publicly Available Information" Minimally Protects Privacy to The Exclusion of Businesses That Provide Societal and State Benefits (CalChamber Report, Section II.C.3)

1. The AG's office will include clarification as follows:

(1) "Publicly Available Information Guidance; § 1798.140(o)(1)(K)(2): Publicly available information is any information that is lawfully made available to the general public from federal, state, or local government records including disclosures to the general public that are required to be made by federal, state, or local law, rules, or regulations."

(2) "Government Records Guidance: Government records include any data made available to the public by the government voluntarily or as a matter of law."

(3) "Use of Public Information Guidance in Section 1798.140(o)(2): In the absence of an express limitation of use by the government entity holding that data, data collected subject to Section 1798.140(o)(2) may be used for any lawful purpose."

III. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES RELATING TO CONSUMER OPT-OUT RIGHTS (§ 1798.185(A)(4))

A. [Proposed] Regulatory Solution to Problem Re: Additional Locations to Solicit Opt-Out Requests Are Needed (CalChamber Report, Section III.A.3)

1. The AG's office will insert clarification language as follows:

(1) The AG's office will insert clarification language: "Clarification of § 1798.135(a)(1) and § 1798.135 (b): For purposes of this title, businesses will be deemed to be in compliance with this requirement by clearly and conspicuously inserting the "Do Not Sell My Personal Information" link; icon developed by the AG; or other opt-out procedure on their homepage or within the privacy policy posted on its website(s) and/or mobile application(s)."

IV. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES: (1) TO FACILITATE AND GOVERN THE SUBMISSION OF A CONSUMER OPT-OUT REQUEST; AND (2) FOR THE DEVELOPMENT AND USE OF A RECOGNIZABLE AND UNIFORM OPT-OUT LOGO OR BUTTON (§ 1798.185(A)(4)(A) AND (C))

A. [Proposed] Regulatory Solution to Problem Re: Create A Sanctioned "Do Not Sell" Logo for Consumers to Easily Recognize How To Opt Out Of The Sale Of Their Personal Information (CalChamber Report, Section IV.A.3)

The AG's office will insert clarification language: "Clarification of § 1798.135(a)(1) and § 1798.135 (b): For purposes of this title, businesses will be deemed to be in compliance with this requirement by clearly and conspicuously inserting the "Do Not Sell My Personal Information" link, icon developed by the AG, or other opt-out procedure on their homepage or within the privacy policy posted on its website(s) and/or mobile application(s)."

B. [Proposed] Regulatory Solution to Problem Re: Businesses Are Not Able to Offer Consumers the Choice To Opt-Out Of Specific Sales Of Personal Information (CalChamber Report, Section IV.B.3)

The AG's office will insert clarifying language: "Clarification of § 1798.135: A business shall be deemed in compliance with Section 1798.135 if it provides consumers with choices from which to opt out including the choice to 'Opt Out of All Sales of My Personal Information.'"

C. [Proposed] Regulatory Solution to Problem Re: Consumers Affirmatively Opting-In Should Not Be Included in The Global "Do Not Sell My Personal Information" Requirement (CalChamber Report, Section IV.C.3)

1. The AG's office will insert clarifying language:

- a. "Clarification of § 1798.35(a)(1): Where consumers' opt-in consent has been obtained and such consumers are subsequently provided with a mechanism to opt out, businesses shall be deemed

to be in compliance with Section 1798.135 and shall not need to provide consumers with the ability to opt-out of such program through a ‘Do Not Sell My Personal Information’ link or logo.”

D. [Proposed] Regulatory Solution to Problem Re: New Age Category (Ages 13-16) For Opt-In Consent Creates Potential Burden on Businesses to Identify Age of Consumers, Jeopardizing Privacy, And Creates Inconsistencies With Federal Law (CalChamber Report, Section IV.D.3)

1. The AG's office will clarify existing language as follows:

(1) "Clarification of § 1798.120(c): The CCPA contemplates that businesses not targeting or offering goods or services of interest to children under the age of 16 and who do not have actual knowledge that a consumer is under 16 are not required to comply with the obligations of this section."

(2) "Clarification of § 1798.120(c): The CCPA contemplates that a business that processes personal information in accordance with the federal Children's Online Privacy Protection Act ("COPPA") will not be deemed in violation of this title with regard to the processing of personal information of children under the age of 13 years."

V. ATTORNEY GENERAL MANDATE: ESTABLISH RULES, PROCEDURES AND EXCEPTIONS RELATING TO NOTICES AND INFORMATION TO CONSUMERS, INCLUDING FINANCIAL INCENTIVE OFFERINGS (§ 1798.185(A)(6))

A. [Proposed] Regulatory Solution to Problem Re: Businesses Should Be Able to Inform Consumers of Their Personal Information Practices At, Or Before, The Point of Collection Through Their Privacy Policies (CalChamber Report, Section V.A.3)

The AG's office will insert clarifying language: "Clarification of Section 1798.100(b): Privacy policies posted online are considered adequate notice under § 1798.100(b) where they contain the required information. Businesses with which consumers do not maintain accounts may comply with the information and notice requirement of § 1798.100(b) by providing the required information and notice on the businesses' Internet homepage or within their posted privacy policy. Businesses without Internet websites may comply by posting such information and notice, including short notices that direct consumers to online notices, in a clear and conspicuous location at their places of business."

B. [Proposed] Regulatory Solution to Problem Re: Guidance Needed on CCPA-Compliant Financial Incentives (Cal.Chamber Report, Section V.B.3)

a. The AG's office will insert clarifying language: "Clarification of Section 1798.125(b)(4): A business may offer financial incentives, including payments to consumers as compensation or discounts for the collection, sale, or deletion of personal information. A business may decline to offer financial incentives or price, rate, level, or quality of goods or services differentials to consumers who opt out of the sale of personal information related to provision of such benefits. The following are examples of financial practices that would not be unjust, unreasonable, coercive, or usurious:

- (1) Loyalty programs
- (2) Gift cards and the use of gift cards as financial incentives
- (3) Coupons and the use of gift cards as financial incentives.
- (4) Direct payments to consumers as compensation.”

b. The AG’s office will insert clarifying language: “Clarification of Section 1798.125(a): A business may decline to offer financial incentives to consumers when a consumer refuses such financial incentives, fails to consent to the collection of personal information, or requests deletion of personal information related to provision of such incentives.”

VI. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES FOR VERIFYING CONSUMER REQUESTS AND OTHER NECESSARY REGULATIONS TO FURTHER PURPOSES OF THE TITLE (§ 1798.185(A)(7))

A. [Proposed] Regulatory Solution to Problem Re: CCPA Clearly States That January 1, 2020 Is the Effective Date; Therefore, The 12-Month Lookback Period Should Not Be Misinterpreted By Consumers Or Regulators To Begin Prior To The Effective Date (CalChamber Report, Section VI.A.3)

“Clarification of the Lookback Period (§ 1798.130(a)(3)(B)), § 1798.130(a)(4)(B)-(C); § 1798.130(a)(5)”: The 12-month lookback period shall apply from the effective date of this title, such that it will not encompass processing activities taking place prior to January 1, 2020 [or the effective date of AG regulations].”

B. [Proposed] Regulatory Solution to Problem Re: Regulations Needed Relating to How to Verify Authorization of Third-Parties Who Make Consumer Requests So Consumer Privacy Is Not Undermined (CalChamber Report, Section VI.B.3)

a. “Clarification of § 1798.135 and § 1798.140(y)”: § 1798.135 and § 1798.140(y) of the CCPA contemplate that when businesses respond to consumer requests made by third-party agents registered with the California Secretary of State, they are not in violation of this title to the extent they rely on such registration. The Secretary of State’s registry must correlate the permissions granted by the consumer to the registered agent.”

b. “Clarification of § 1798.135 and § 1798.140(y)”: § 1798.135 and § 1798.140(y) of the CCPA contemplate that when businesses respond to consumer requests when provided proof of appointment as a consumer’s legal guardian, conservator, fiduciary, or similar legally authorized and recognized person, they are not in violation of this title. Where a third-party requestor has not sufficiently demonstrated that it is authorized to make a request on the consumer’s behalf, a business shall not be obligated to comply with the request.”

C. [Proposed] Regulatory Solution to Problem Re: Regulations Needed on How Consumer Requests Can Be Submitted and Processed To Maintain The Confidentiality And Security Of Personal Information (CalChamber Report, Section VI.C.3)

a. The AG's office will provide guidance for businesses as follows: "Guidance for Submitting Requests for Account Holders and Non-Account Holders: Businesses may provide a self-service portal for consumers to view or extract their personal information. For businesses maintaining consumer accounts, businesses may assume that a consumer request submitted through a password-protected account maintained with the business is sufficient to consider it reasonably verified. For businesses not maintaining consumer accounts, businesses may use personal information supplied by the consumer in the self-serve portal to verify their identity through their own means or the use of a third-party identity verification service. If consumer identity cannot be verified, the business is not obligated to provide access to the requested personal information."

b. The AG's office shall clarify existing language as follows: "Clarification of § 1798.140(y): § 1798.140(y) of the CCPA contemplates that when businesses maintain a reasonable, documented procedure to verify the identity of a consumer who has submitted a request to exercise a right granted under this title, or the authority of a person making the request on behalf of a consumer, businesses shall not be held liable, in either an action by the Attorney General or a private action, for the unauthorized disclosure of personal information in connection to any response to such request. A procedure shall be considered *per se* reasonable if it calls for any of the following, either exclusively or in the alternative: the verification of identity through the collection of a government-issued identification; or the verification of identity by matching of at least three of the following types of information provided by the consumer, or the person authorized to make a request on behalf of a consumer, with a consumer profile maintained by the business: full name, email address, telephone number, mailing address, and something the business provides to a consumer, e.g., a pin code."

c. The AG's office will provide guidance for businesses as follows: "Guidance for Processing Consumer Requests: If a business does not automate verification, it can consider a single team to broker consumer requests."

D. [Proposed] Regulatory Solution to Problem Re: Allowing Disclosure Of "Specific Pieces of Information" For Consumer Rights Other Than the Right to Access Requests Would Create Unnecessary Cybersecurity Risks And Contradict The Text Of The Statute (CalChamber Report, Section VI.D.3)

a. "Clarification of Disclosure Obligations Relating to Specific Categories of Personal Information (§ 1798.100(a), (c), and (d); § 1798.110 (a) and (c):

(1) A business may comply with consumer requests pertaining to "specific pieces" of personal information by describing the personal information at issue or effectively masking the same without transmitting precise pieces of personal information that would fall into the categories in Section 1798.81.5 (e.g., social security numbers, credit card numbers, financial account numbers, health information). For example, rather than

provide the exact social security number it has collected, a business may provide a report advising that it has collected the consumer's social security number."

E. [Proposed] Regulatory Solution to Problem Re: Third Parties Who Do Not Have Direct Relationships with Consumers Cannot Notify Them That Their Personal Information Has Been Sold (CalChamber Report, Section VI.E.3)

a. The AG's office will insert clarifying language: "Clarification of Third Party's Consumer Notice Obligations (§ 1798.115(d)): To comply with Section 1798.115(d), third parties may rely on a business' written attestation that it has provided consumers with: (1) 'explicit' notice of the third party's intent to sell personal information, and (2) the opportunity to exercise the CCPA right to opt out of such sale."

F. [Proposed] Regulatory Solution to Problem Re: Clarifying That Businesses Are Not Required to Retain Personal Information Solely to Comply with Consumer Requests; also Data Retention To Comply With The 12-Month Lookback Period Could Violate Data Minimization Best Practices (CalChamber Report, Section VI.F.3)

a. The AG's office shall clarify as follows: "Clarification of § 1798.100(e): Businesses are not required to retain personal information solely to fulfill a consumer request. Under no circumstances is a business required to retain personal information solely for the purpose of fulfilling a consumer request made under this title."

b. The AG's office shall clarify as follows: "Clarification of § 1798.130 (a)(3)-(4): The 12-month lookback provisions do not require businesses to retain data longer than necessary. Further, businesses need not retain data that they would otherwise delete in anticipation of responding to 12-month lookback inquiries."

c. The AG's office will clarify existing language as follows: "Clarification of § 1798.100(e): § 1798.100(e) of the CCPA contemplates that when businesses retain data associated with the processing of a consumer request in accordance with its records retention schedule, they will not be deemed violation of this section."

G. [Proposed] Regulatory Solution to Problem Re: Employment and Business Related Data (CalChamber Report, VI.G.3)

a. The AG's office shall clarify as follows: "Clarification of § 1798.140(o): Definition of Personal Information: The rights in this title do not extend to personal information collected by a business in connection with: (i) an individual's application or role as an employee, contractor, or agent, or (ii) a business counterparty in a business-to-business relationship. Such interpretations are consistent with this title."

b. The AG's office shall clarify as follows: "Clarification of § 1798.140(g): Definition of Consumer: The definition of consumer shall exclude current and former employees, prospective employees, recruitment candidates, owners, directors, contractors, vendors, agents, or authorized representative of the business, such as directors, or of any other legal or government entity, acting in the capacity of these roles."

H. [Proposed] Regulatory Solution to Problem Re: Obstacles to Determining Who Is a California Consumer (CalChamber Report, Section VI.H.3)

a. The AG's office shall clarify as follows: "Clarification of § 1798.140(g): Definition of Personal Information: Consumers can prove that they are California consumers by providing a California mailing address and/or any other proof of residency that may be requested by business."

I. [Proposed] Regulatory Solution to Problem Re: Reasonable Security and Private Right Of Action (CalChamber Report, Section VI.I.3)

a. The AG's office will clarify existing language as follows: "Clarification of § 1798.150: § 1798.150 of the CCPA contemplates that when businesses maintain compliance with a recognized data security standard (e.g., CIS Critical Security Controls, NIST Cybersecurity Framework or NIST 800-53, ISO 27001 *et. seq.*, or PCI), businesses are immune from suit under § 1798.150. Implementation of such recognized data security standards is a defense to enforcement actions or suits under § 1798.150."

b. The AG's office shall clarify existing language as follows: "Clarification of § 1798.150(a)(1): § 1798.150(a)(1) of the CCPA contemplates that when businesses maintain personal information within a recognized cybersecurity program conforming to the requirements of Ohio Rev. Code § 1354.02, such businesses shall not be deemed to be in violation of this title."

J. [Proposed] Regulatory Solution to Problem Re: Right to Cure Alleged Violations Does Not Comport with Best Security Practices (CalChamber Report, Section VI.J.3)

a. The AG's office shall clarify existing language as follows: "Clarification of § 1798.150(b): § 1798.150(b) of the CCPA contemplates that when businesses document adherence to accepted cybersecurity remediation steps including: (1) a root cause investigation; (2) an impact assessment; and (3) development and implementation of plans to prevent reoccurrence of the event, such documentation shall represent *prima facie* evidence of curing the incident."

K. [Proposed] Regulatory Solution to Problem Re: "Service Providers," "Third Parties," And "Persons" Service Providers (§ 1798.140 (V)), Third Parties (§ 1798.140 (W)) And (Liability Shifted) Persons (1798.140(W)(2)) Should All Be Treated The Same For Purposes Of § 1798.140 (T)(2), Meaning That The Exceptions To "Sale" Apply Equally To Transfers To "Service Providers," "Third Parties," And "Persons" (CalChamber Report, Section VI.K.3)

a. The AG's office shall clarify as follows: "Clarification of § 1798.140(w)(2): § 1798.140(w)(2) of the CCPA contemplates that when businesses have executed contracts with processors in compliance with Article 28 of the General Data Protection Regulation, they shall not be in violation of § 1798.140(w)(2)(B)."

b. The AG's office shall clarify as follows: "Clarification of §1798.140(t)(2): §1798.140(t)(2) of the CCPA contemplates that §1798.140(t)(2) shall apply equally to service providers (as defined in 1798.140(v), third parties (as defined in § 1798.140(w), and persons that meet the requirements § 1798.140(w)(2), as long as the service providers, third parties and persons satisfy the conditions of § 1798.140(t)(2)."

L. [Proposed] Regulatory Solution to Problem Re: Guidance Needed on How Service Providers Should Respond to Verifiable Consumer Requests (CalChamber Report, Section VI.L.3)

a. The AG's office should provide guidance as follows: "Guidance for Service Providers When Responding to Consumer Requests: If a service provider receives a request from a consumer, the service provider will have no obligation to respond to a request from a consumer where the service provider does not have a direct relationship, as a business, with the consumer. The service provider may respond with an explanation that the request should be submitted to the business with whom the consumer has the direct relationship.

Message

From: Abby Robinson Vollmer [REDACTED]
Sent: 3/8/2019 4:20:46 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: California Consumer Privacy Act (CCPA) rulemaking
Attachments: GitHub-CCPA-comments-to-CA-AG.pdf

Dear Attorney General Becerra:

Please find attached comments from GitHub, Inc. in response to your call for written comments regarding CCPA rulemaking.

Thanks,
Abby



88 Colin P. Kelly Jr. Street
San Francisco, CA 94107

March 8, 2019

To: Attorney General Becerra
Via email: privacyregulations@doj.ca.gov

Re: Comments on CCPA rulemaking

Dear Attorney General Becerra:

GitHub provides these comments in response to the comment period on regulations to implement the California Consumer Privacy Act (CCPA). Our comments reflect four primary objectives, which are to:

- Harmonize standards and requirements with existing laws, where possible
- Clarify definition of “personal information”
- Retain time-to-cure provision
- Establish that “Do Not Sell My Personal Information” logo or button be designed in accordance with standards and accessibility best practices and clarify expectations on translation and use of alt-text

About GitHub

GitHub is where software is built. With its headquarters in San Francisco and over 31 million users worldwide, GitHub is the world’s largest software development platform, enabling people and businesses to collaboratively develop open-source and proprietary software projects. GitHub’s global community includes individual developers, students, startups, small businesses, large businesses, NGOs, and governments. GitHub-hosted software projects include applications designed for web or mobile devices, as well as the source code that powers entire businesses.

GitHub offers these comments from the perspective of software developers, who are building the programs, websites, and applications that power industries all across California (and the world). Ensuring a high level of data protection is crucial to developers’ ability to build and offer products in today’s digital world. Developers understand that people need to be able to trust businesses with their data, and developers themselves tend to care about privacy. Developers are often the ones implementing data protection rules, if not making choices related to user privacy. We therefore support robust data privacy protections. At the same time, developers are better equipped to build and innovate when they do not face unnecessarily burdensome requirements and when they have legal clarity. These comments thus focus on places in which your office’s rules can help reduce operational costs of



compliance for developers—for example, by harmonizing standards and clarifying definitions of terms—without compromising the overall aim of ensuring user privacy and data protection.

Harmonize Standards

The CCPA will enter the regulatory landscape amid existing privacy and data protection laws, such as U.S. state laws and the EU General Data Protection Regulation (GDPR). Even though GDPR is an EU law, countless developers in California need to comply with it given that they build software for sites or products with EU users. Likewise, developers in California need to comply with other U.S. states laws where users of their products or services are in those states. Thus, developers in California invariably need to implement the CCPA, along with user privacy laws in other states or jurisdictions. In many cases, a provision of the CCPA shares intent with provision(s) of one or more of those laws. Wherever possible, the CCPA should align with existing requirements so as to prevent unnecessary expenditure of resources to track, categorize, and respond to requests for information. Below are examples.

1. The GDPR's obligations correlate with a business's role as a "processor" or "controller" of personally identifying information. While the CCPA does not use these terms to determine the scope of requirements, it uses "collect" in some of the same ways as the GDPR essentially uses "process." Currently, the CCPA would require a business to process and enforce requests for which it isn't the "controller" under GDPR. For example, a business that only acts as a "processor" of certain personal information under the GDPR may, under the current CCPA language, be required to delete that information at a customer's request per 1798.105(c), even though it lacks control of that information. Currently, this dilemma is only mitigated if the business can justify retaining that data under 1798.105(d)'s list of exceptions, which do not cover all the potential limits on a processor's control of controllers' or clients' data. Aligning a business's obligation as a business that collects information with that of a processor would help reduce circumstances in which it would be impossible for businesses to comply, like the example above. One way to better align those obligations would be to harmonize, where appropriate, definitions of "service provider" in the CCPA with "processor" in GDPR; and definitions of "third party" in the CCPA and other privacy laws like GDPR.

2. The CCPA exceptions to the requirement to comply with a consumer's deletion request includes business purposes that are security-related. See section 1798.105(d)(2); see also security-related circumstances in definition of "business purpose" in section 1798.140(d)(2) and (3). Similarly, the GDPR's Article 32 also addresses security of processing. This presents an opportunity to align the CCPA and GDPR, in particular, to make sure businesses can do monitoring related to availability of their services. Below are our proposed revisions:

- 1798.105(d)(2): Detect, **protect against, resolve, or take legal action in response to** security incidents; **or** protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
- 1798.140(d)(2): Detecting, **protecting against, resolving, or taking legal action in response to** security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

Clarify Definition of "Personal Information"

The definition of "personal information" (section 1798.140) warrants greater clarity.



This definition is at the core of defining *what* is in scope of the CCPA:

information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household....

We suggest aligning the CCPA's definition with existing laws where there might be ambiguity. For example, the GDPR's definition of "personal data" also describes information in relation to a person:

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

The inclusion of information that "could be reasonably linked, directly or indirectly" may expand the scope beyond identifiable boundaries. Under this current broad language, developers will be left guessing whenever they encounter information that could be linked to a person under tenuous circumstances.

We recommend

- harmonizing the definition along the lines of

"information that identifies, relates to, **or** describes, ~~is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household~~"
- providing illustrative examples of what would fall within the scope of those terms to give developers the clarity they need as to what data to treat as "personal information" when building software.

Retain Time-to-Cure Provision

The CCPA requires a consumer to provide a business with 30 days written notice of specific alleged violations before filing a legal action for damages so that the business has time to cure the alleged violations (section 1798.150(b)(1)). This provision is especially important to businesses given the difficulty in defining the exact scope of many of the requirements. In addition, our experience responding to other user requests—such as under the Digital Millennium Copyright Act DMCA, where we notify alleged infringers before taking action in response to a DMCA takedown notice—demonstrates that complaints can be resolved in many cases by giving the alleged infringer a chance to respond. Likewise, requiring complainants to give a business a chance to resolve violations under the CCPA before filing suit should help reduce unnecessary litigation. Thus, we respectfully request that you to reconsider your proposal to amend the CCPA through [Senate Bill 561](#), as it would remove this provision.



Establish that “Do Not Sell My Personal Information” Logo or Button be Designed in Accordance with Accessibility Standards and Best Practices and Clarify Expectations on Translation and Use of Alt-text

Section 1798.195(a)(4)(C) states that your office will solicit input regarding

The development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt out of the sale of personal information.

Our comments here aim to ensure that the “Do Not Sell My Personal Information” Logo or Button requirement is designed and implemented in a way that incentivizes design standards that promote diversity and inclusion. To that end, we recommend that (1) the design of this button reflect accessibility standards and best practices; and (2) the requirements provide that businesses serving non-English speaking groups can translate “Do Not Sell My Personal Information.”

Regarding the design of this logo or button, software developers will be required to include this button in webpage design and builds. We thus encourage your office to ensure that accessibility is taken into account in its design in order to reach users with disabilities. We also request that your office clarify whether businesses can meet this requirement by using the forthcoming logo conspicuously, along with “Do Not Sell My Personal Information” as alt text rather than also “Do Not Sell My Personal Information” as link text. With a view to accessibility and universal adoption of the logo or button, this combination would enable this requirement to be meaningful for a broader range of users, including those who are visually impaired.

As for translation, given that there many Californians do not speak English, many businesses serving Californians may not be able effectively reach their consumers if the button or logo must be in English. We encourage your office to allow businesses that serve non-English speaking consumers to translate “Do Not Sell My Personal Information.”

* * *

GitHub again wishes to thank you for your attention to this important issue and encourages you to follow up with us should you have any questions or seek any additional information.

Message

From: Gorsline, Ronald [REDACTED]
Sent: 1/14/2019 1:02:51 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Gorsline, Ronald [REDACTED]
Subject: California Consumer Privacy Act ("CCPA")

It is our understanding that the Department of Justice ("DOJ") indicated that it will be promulgating regulations to implement the California Consumer Privacy Act ("CCPA") related to the following issues:

1. Categories of personal information;
2. Definition of unique identifiers;
3. Exceptions to the CCPA;
4. Submitting and complying with requests;
5. Uniform opt-out logo/button;
6. Notices and information to consumers; and
7. Verification of consumers' requests.

In addition, your office has requested all interested persons and parties submit comments regarding the CCPA regulations.

Although it our understanding that businesses subject to the CCPA may ask the DOJ for guidance on issues of compliance after implementation, we are writing to ask you clarify in the regulations that an "employee" of a business subject to the CCPA is exempt from the definition of "consumer."

The rule focuses on "commercial conduct" which takes place within California by businesses collecting that consumer information while the consumer is in California, and also contemplates the information relates to transactions involving consumer goods or services. For example, arguably the provisions of the statute which authorizes a businesses to offer "a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data" would not apply in an employer/employee relationship.

Therefore, we request that in promulgating rules regarding "exceptions to the CCPA" that you clarify the definition of consumer does not include employees.

Best regards.

Ronald D. Gorsline

Ronald D. Gorsline

Partner / Admitted in Tennessee and Georgia

Hudson Cook, LLP



9431 Bradmore Lane | Suite 201 | Ooltewah, Tennessee 37363

HUDSON
COOK

The information contained in this transmission may be privileged and may constitute attorney work product. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact Ronald D. Gorsline at [REDACTED] or [REDACTED] and destroy all copies of the original message and any attachments.

Message

From: Patack, Melissa [REDACTED]
Sent: 3/8/2019 2:52:26 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Eleanor Blume [REDACTED]
[REDACTED]; Fuentes, Felipe [REDACTED]
Subject: California Consumer Privacy Act - Comment Letter
Attachments: CA.CCPA.MPAA.comments.final.030819.pdf

Attached please find comments submitted by MPAA. Many thanks for your consideration.

Melissa Patack

Vice President & Sr. Counsel

State Government Affairs

Motion Picture Association of America, Inc.

[REDACTED]



MOTION PICTURE ASSOCIATION OF AMERICA, INC.
15301 VENTURA BOULEVARD, BUILDING E
SHERMAN OAKS, CA 91403

MELISSA PATAACK
VICE PRESIDENT & SR. COUNSEL
State Government Affairs

March 8, 2019

The Honorable Xavier Becerra
Attorney General
State of California
P.O. Box 944255
Sacramento CA 94244

Delivered via email: privacyregulations@doj.ca.gov

Dear General Becerra:

On behalf of the Motion Picture Association of America, Inc. and our member companies, enclosed please find comments your office has invited with regard to the regulatory process in accordance with the California Consumer Privacy Act, Civil Code Section 1798.185.

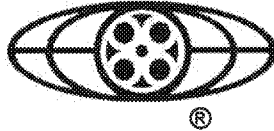
If your or your staff has any questions or needs further information, please don't hesitate to contact me, or our legislative advocate in Sacramento, Felipe Fuentes, who can be reached at [REDACTED]

We appreciate your consideration.

Sincerely,

A handwritten signature in cursive script that reads "Melissa Pataack".

cc: Felipe Fuentes, The Apex Group



MOTION PICTURE ASSOCIATION OF AMERICA, INC.

15301 VENTURA BOULEVARD, BUILDING E
SHERMAN OAKS, CA 91403
[REDACTED]

The Motion Picture Association of America (“MPAA”) respectfully submits these comments in accordance with the California Attorney General’s (“AG”) upcoming rulemaking, pursuant to Civil Code Section 1798.185, to implement the California Consumer Privacy Act (“CCPA”).

MPAA represents leading companies¹ in the creative community, including film, television, streaming content, video gaming and other content producers. We are proud to bring good jobs, high-quality entertainment and other benefits to California’s economy and its consumers. Each year, we invest billions of dollars in our brands and in our trusted relationship with audiences here and globally.² We know that earning and maintaining consumers’ trust is critical to our mission as businesses and good corporate citizens. Thus, we fully support efforts to ensure that consumers’ personal information is handled responsibly and safely by businesses delivering desired products and services to those consumers. Regrettably, the CCPA could stifle the continued growth of the creative economy and actually work to undermine existing practices designed to protect consumer information.

We write to highlight a few of these significant CCPA implementation issues that could impact the creative community in California.

I. Background on the Creative Economy Ecosystem

Audiences in California and around the world engage with an ever-expanding array of movies, TV shows, games and digital content made possible by creators of all types – actors, musicians, choreographers, writers, directors, programmers, designers, animators, crafts people and engineers. The creative community is characterized by a high degree of collaboration thanks, in part, to a diverse and dynamic network of businesses, joint ventures, consulting and contractual relationships and a wide variety of arrangements that share talent, brands and other resources.

¹ MPAA member companies include: The Walt Disney Studios Motion Pictures; Netflix Studios, LLC; Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Twentieth Century Fox Film Corporation; Universal City Studios LLC; and Warner Bros. Entertainment Inc. CBS Corporation is an associate member.

² Motion picture, television and digital entertainment production and distribution supports 2.1 million jobs, and more than \$139 billion in total wages. More than 200,000 Californians make their careers in this industry, generating over \$22 billion in wages. In addition, this sector registers a positive balance of trade in nearly every country in the world with \$16.5 billion in exports worldwide. See <https://www.mpa.org/what-we-do/driving-economic-growth/>

The creative community also is characterized by a high degree of customization. Each movie, show, game or website is in many respects unique, and consumers expect the look, feel and ways of discovering and interacting with that content to be unique as well. Thus, it is quite common for creators to tailor how each movie, game or other piece of content is developed and distributed so that it stands apart from the many other choices audiences currently enjoy. The distribution network for getting these products to market is complex, with niche players serving individual roles in the ecosystem.

Given these characteristics, we are concerned that the CCPA could be interpreted in ways that would pose a variety of practical problems for the creative community – problems we think can be avoided without undermining our shared goal of protecting consumers.

II. Overly-Broad Definition of “Sale” Should be Clarified to Allow for Continued Delivery of Desired Services and Products to Consumers

As explained above, it is common in the creative community to enter into collaborative arrangements that involve collecting, using and sharing personal information for a variety of business purposes, such as jointly developing, provisioning, customizing and improving content offerings and other services. Content companies, such as MPAA members, also rely on a range of analytics service providers, and other services and tools to run websites to market their movies and to make content available to consumers on a variety of platforms, including some no cost ad-supported platforms. While these arrangements may entail “making available” or “transferring” personal information, the underlying business purposes for the information sharing relate to jointly enabling and supporting services for consumers, not obtaining monetary consideration for selling the personal information itself.

MPAA members and other California creative businesses need flexibility to enter into partnerships, joint ventures and other collaborative business arrangements as we develop innovative content and services for consumers.

If interpreted too broadly, the definition of “sale” in the CCPA will undermine the entire creative output and distribution ecosystem by misclassifying a common interest activity to get a product into market that does not undermine safety of consumer data as activity that compromises consumer privacy.

Accordingly, the AG should issue guidance that personal information is not sold in cases where personal information is shared and used for content and service-related purposes as part of a joint venture, partnership or similar arrangement. Such an interpretation is consistent with the goals and structure of the CCPA, which is intended to give consumers the right to opt out of the sale of their personal information to a third party which may put it to unexpected and undisclosed uses. It also is consistent with the definition of “business purpose” in the CCPA, which gives businesses and service providers flexibility to use and share personal information for a variety of operational purposes.

III. Definition of “Personal Information” Should be Clarified to Avoid Undermining Existing Data Protection Practices

MPAA also supports clarification of the definition of “personal information.” If interpreted too broadly, the definition of personal information in the CCPA could have unintended negative consequences for consumers and businesses alike. For example, current business practices of de-identifying data benefits consumers and increases data security. The implementing regulations should clarify that the broad language included in the definition of “personal information” -- specifically “relates to,” “is capable of being associated with,” “or could reasonably be linked, directly or indirectly, with” -- was not intended to prevent or undermine the provisions in the law that permit de-identification.

IV. Incentive and Rewards Programs Should be Protected as Mutually Beneficial Service

The CCPA broadly provides that businesses are prohibited from discriminating against a consumer because a consumer exercised any of the consumer’s privacy rights under the Act. According to the Act, discrimination could take the form of denying goods or services, “charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposes penalties,” or differing levels of quality. The MPAA member companies often offer early previews, sneak peeks or bonus footage to consumers as part of customized marketing strategies for content. The MPAA respectfully asks for definitive clarification that such programs are not discriminatory.

MPAA and its members stand ready to work with you to develop implementation guidance that is consistent with consumer expectations and the statutory requirements of the CCPA. We have a shared interest in protecting consumers’ privacy and ensuring that the CCPA does not inadvertently undermine the creative community that has played such an important role in California’s culture and economy.

March 8, 2019

Message

From: Kevin Gould [REDACTED]
Sent: 3/8/2019 2:04:01 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: California Consumer Privacy Act of 2018 -- Pre-rulemaking Comment Letter
Attachments: California Consumer Privacy Act of 2018 Pre-rulemaking Letter.pdf

Thank you for the opportunity to provide written comments during the pre-rulemaking activities by the Attorney General relative to the California Consumer Privacy Act of 2018. Please find our comments attached. Please let us know if you have any questions. Thank you!



Kevin Gould
SVP, Director of Government Relations
California Bankers Association
1303 J Street, Suite 600 | Sacramento, CA 95814
[REDACTED]
Connect: [Website](#) | [Twitter](#) | [LinkedIn](#)



March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

RE: California Consumer Privacy Act of 2018 – Pre-rulemaking Comment Letter

Dear Sir or Madam:

The California Bankers Association (CBA), the California Credit Union League (CCUL), and the California Mortgage Bankers Association (California MBA) appreciate the invitation and the opportunity to submit written comments in response to the preliminary rulemaking activities undertaken by the California Department of Justice prior to the official rulemaking required by the California Consumer Privacy Act of 2018 (CCPA).

CBA is a division of the Western Bankers Association, one of the largest banking trade associations and regional educational organizations in the United States. CBA advocates on legislative, regulatory and legal matters on behalf of banks doing business in the state of California.

CCUL represents nearly 250 credit unions and their 11 million members in the state. The League is committed to helping credit unions change their members' lives through advocacy, innovation and by putting members first.

California MBA is a California corporation operating as a non-profit association that serves members of the real estate finance industry doing business in California. California MBA's membership consists of approximately three hundred companies representing a full spectrum of residential and commercial lenders, servicers, brokers, and a broad range of industry service providers.

While the Attorney General (AG) has been granted ongoing authority to adopt regulations as necessary to further the CCPA, California Civil Code Section 1798.185 specifically requires that "on or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations," on the following seven enumerated areas within the CCPA:

- (1) Updating as needed additional categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (o) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.
- (2) Updating as needed the definition of unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and additional categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to Section 1798.130.
- (3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.
- (4) Establishing rules and procedures for the following:
 - (A) To facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information pursuant to paragraph (1) of subdivision (a) of Section 1798.145.
 - (B) To govern business compliance with a consumer's opt-out request.
 - (C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.
- (5) Adjusting the monetary threshold in subparagraph (A) of paragraph (1) of subdivision (c) of Section 1798.140 in January of every odd-numbered year to reflect any increase in the Consumer Price Index.
- (6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter.
- (7) Establishing rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received by a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the

consumer's identity, within one year of passage of this title and as needed thereafter.

Accordingly, as your office prepares to issue regulations in accordance with the statute, we respectfully urge that you consider the following requests for clarity. These requests should not be considered an effort to undermine the CCPA but rather intended to assist in efforts to clarify aspects of the law.

➤ **Clarify what is necessary to authenticate a “verifiable consumer request.” (Subdivision (y) of Section 1798.140).**

The CCPA establishes a series of rights that are contingent upon the receipt and authentication of a “verifiable consumer request.” For example, the CCPA requires that “businesses that receive a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver” the personal information. (Subdivision (d) of Section 1798.100). The Act also requires a “business that receives a verifiable consumer request from a consumer to delete the consumer’s personal information from its records and direct any service providers to delete the consumer’s personal information from their records.” (Subdivision (c) of Section 1798.105). Further, a consumer has the right to request and receive, upon receipt of a verifiable consumer request, personal information that a business has collected and/or sold about the consumer. (Sections 1798.110 and 1798.115).

In order to comply with a consumer’s request to exercise his or her rights under the CCPA, the “business shall promptly take steps to determine whether the request is a verifiable consumer request.” (Subdivision (a)(2) of Section 1798.130). “Verifiable consumer request” is defined as a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer’s behalf. (Subdivision (y) of Section 1798.140).

As part of routine transactions with consumers, financial institutions collect personal information in order to facilitate customer requests. Furnishing personal information to consumers purporting to exercise their rights under the CCPA, in response to a verifiable

consumer request, may result in unintended risk and harm to the consumer, including misuse of personal information to perpetuate fraud and identity theft.

A business receiving a consumer's request will need sufficient data from the consumer as a safeguard to ensure the information provided in return is associated with the requesting individual. Regulations established by the AG should provide flexibility for a business to decline a consumer's request where the data presented by the consumer is insufficient to authenticate a request. Further, in circumstances where limited information is provided by the consumer, a business endeavoring to authenticate a request should have flexibility, but not be required, to furnish non-sensitive personal information (excluding personal information that if disclosed would otherwise result in a data breach) to the consumer as a means to satisfy its compliance and to protect the consumer against fraud and identity theft.

Pursuant to subdivision (y) of Section 1798.140, the AG has the opportunity to promulgate regulations that will assist a business in its efforts to 1) reasonably verify the consumer and 2) address circumstances where the business cannot verify the identity of the consumer making a request. Accordingly, we urge the AG to provide clear guidance on the means by which a business can verify a consumer request and to provide flexibility for those circumstances where the business will be unable to authenticate a verifiable consumer request.

As regulations are put forth on this topic, we encourage that they take into consideration a business' size and complexity, the nature and scope of its business activities, and the sensitivity of any personal information at issue. The AG may wish to consider utilizing principles such as those in existing authentication guidance issued by the Federal Financial Institutions Examination Council. Finally, we believe that a safe-harbor from liability should be granted to businesses that satisfy the criteria adopted pursuant to the promulgated regulations.

- **"Personal information" should not include pseudonymous information. (Subdivision (o)(1) of Section 1798.140).**

Section 1798.140 of the CCPA defines "personal information" and "pseudonymize" as follows:

(o)(1) "Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(2) "Personal information" does not include publicly available information. For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. "Publicly available" does not include consumer information that is deidentified or aggregate consumer information.

(r) "Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

In summary, “personal information” is information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer. In contrast, pseudonymized data is information in a manner that renders the personal information no longer attributable to a specific consumer.

Provisions throughout the CCPA indicate that businesses are not required to re-link or reidentify data that has been disassociated with a particular consumer in order to satisfy a request by a consumer wishing to exercise their rights under the Act. Subdivision (e) of Section 1798.100, indicates, that “this section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.” Subdivision (d)(2) of Section 1798.110 does not require a business to “reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.” Finally, subdivision (i) of Section 1798.145 underscores that “this title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.”

Given that pseudonymized data “renders the personal information no longer attributable to a specific consumer,” a business would need to re-link it to specific consumers in order to respond to a consumer rights request under the Act. We believe that requiring businesses to re-link pseudonymized data undermines a primary CCPA goal to protect personal information by forcing the re-linking of data that was not otherwise maintained for that purpose.

Accordingly, we urge rulemaking that clarifies that businesses are not required to re-link data that is no longer attributable to a specific consumer and therefore not personal information (as defined). We believe that such clarification is consistent with, and furthers the intent of the CCPA.

- **The CCPA should not apply to a covered entity’s intellectual property, or require a business to reveal data that would infringe on the rights of others. (Section 1798.145).**

Pursuant to subdivision (a)(3) of Section 1798.185, the CCPA grants the AG authority to establish “any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.”

In this regard, we urge rulemaking that establishes an exception from the Act for intellectual property or for data that, if disclosed, would have an adverse effect on the

rights or freedoms of others. The CCPA should not apply to information that is the protected intellectual property of a business, including information subject to copyright, patent, service mark and/or trade secret protections. A business should not be required to disclose any information that is subject to intellectual property protections, including any formula, pattern, compilation, program, device, method, technique, or process developed to process or analyze personal information, or any information derived from such process or analysis.

In considering this request, your office may wish to consider the approach taken in the European General Data Protection Regulation (GDPR) which places reasonable limitations on the consumer privacy right it grants. Both the intellectual property exclusion and the avoidance of infringement on the rights of others are embedded in the GDPR. We believe that there should be similar recognition in the CCPA of circumstances where a business' attempt to comply with a consumer's request would place it in the position of violating the rights of others or placing it in jeopardy with its competitors.

- **Clarify the definition of "sell" and the related elements of that definition, particularly in regard to service providers facilitating a consumer-requested transaction. (Subdivision (t) of Section 1798.140).**

The CCPA includes definitions for "sell" and "service provider" as follows:

(t)(1) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.

(2) For purposes of this title, a business does not sell personal information when:

(A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.

(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:

(i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.

(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

(D) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(v) "Service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

When an entity operates as a service provider to a business for an established business purpose, the service provider should be treated solely as a service provider and not be subject to the CCPA because that service provider might also be considered a business, as defined by the Act, when separately performing its core function. In situations where a service provider is also separately defined as a business, the Act should not be construed to conflate the actions taken when functioning as a service provider compared to the actions of a business subject to the Act. Such a result would mean that a service provider

could never be considered just a service provider even when it is performing in the limited role of a service provider.

We urge that the CCPA be clarified so that a service provider will be considered only a service provider when serving in that limited role and treated as a business solely in those circumstances where it independently qualifies as a business and maintains its own direct relationship with a consumer.

➤ **The concept of “household” needs clarification. (Subdivision (o)(1) of Section 1798.140).**

As described earlier, the definition of “personal information” applies not only to a consumer but also to a household. This is critical given the rights that may be exercised with respect to “households” under the CCPA, including the right to access and delete.

(o)(1) “Personal information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household: . . .

A consumer making a request for personal information pursuant to the CCPA seems to be entitled to personal information about themselves, as well as other household members, which may include non-family members. We have serious concerns with disclosing personal information to an individual consumer about other members of a household and the risks and harm this may present, financial or otherwise.

Ultimately, we urge the deletion of “household” from the definition of “personal information” or, at a minimum, the establishment of criteria and safeguards that, in general, personal information of one consumer may not be disclosed to another consumer.

➤ **The definition of “publicly available” should be clarified. (Subdivision (o)(2) of Section 1798.140).**

The definition of “personal information,” includes an exception for information that is “publicly available” that is so ambiguous to be meaningless.

(o)(2) “Personal information” does not include publicly available information. For these purposes, “publicly available” means information that is lawfully made available from federal, state, or local government records, if any conditions

associated with such information. “Publicly available” does not mean biometric information collected by a business about a consumer without the consumer’s knowledge. Information is not “publicly available” if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. “Publicly available” does not include consumer information that is deidentified or aggregate consumer information.

Limiting the definition of “personal information” to information from government records “compatible with the purpose for which the data is maintained” is too restrictive and requires a business to infer the purpose for which the information is maintained. In addition, publicly available information not subject to CCPA obligations is limited to government records, when, in fact, information may be publicly available when gleaned from other sources.

We believe that regulations should be adopted that expand the definition of “publicly available” to include data made available to the public by the government voluntarily or as a matter of law.

➤ **What is required to satisfy the “right to cure?” (Subdivision (b) of Section 1798.155).**

Subdivision (b) of Section 1798.155, establishes, in part, that a “business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance.” We urge the AG to establish specific criteria for what is necessary in order for a business to successfully “cure” a violation and therefore avoid liability.

Further, in circumstances where a cure cannot unwind the effects of a violation, guidance is needed as to other means in which the business could cure, or mitigate against, the violation through implementation of business practices designed to subsequently avoid the conditions that led to previous violations.

➤ **The “lookback” period should commence January 1, 2020. (Section 1798.130).**

As currently written, the CCPA appears to apply retroactively by requiring businesses to provide information subject to a consumer’s request covering the time period prior to the Act’s effective date and prior to publication of implementing regulations. We believe rulemaking should clarify that the 12 month lookback period provided for in Section 1798.130 applies from the effective date of the CCPA, thereby precluding its application to activities occurring before January 1, 2020.

- **Clarify that enforcement will be based on conduct occurring on or after an enforcement date and establish an enforcement date of not earlier than July 1, 2020. (Section 1798.185).**

The CCPA provides in subdivision (c) of Section 1798.185, that the “Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.”

We urge that the AG clarify that any enforcement undertaken by the AG will only be based on conduct or omissions occurring on or after the enforcement date. For example, if the enforcement date is July 1, 2020, because that is earlier than the six-month anniversary of final regulations, then clarity should be provided that any AG enforcement will be based only on conduct or omissions occurring July 1, 2020, or later, and not conduct or omissions occurring January 1, 2020, (the CCPA effective date) or January 15, 2020 (after the CCPA effective date). This clarification is essential so that businesses can properly prepare.

In addition, we request that the AG establish an enforcement date that is no earlier than July 1, 2020, even if the six-month anniversary of final regulations is an earlier date. Based on the understanding that final regulations will be issued during the fall of 2019, many businesses will need time to review the regulations and implement the rules. In the fall of 2019, many businesses will still be implementing changes needed based on the statutory language, apart from final regulations.

We request that the AG indicate that it will not enforce the CCPA until July 1, 2020. That date is appropriate so that consumers, businesses, and the AG are aligned on expectations, and businesses have sufficient time to review and implement direction from the regulations, which may require changes to implementation plans that were based in good faith on the statutory language, prior to regulations being adopted.

Thank you for the opportunity to provide commentary in advance of the formal rulemaking that will take place later this year. We welcome any questions you may have regarding our letter.

Sincerely,

California Bankers Association
California Credit Union League
California Mortgage Bankers Association

Message

From: Isberg, Pete (CORP) [REDACTED]
Sent: 2/6/2019 6:55:30 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: California Consumer Privacy Act Rulemaking
Attachments: NPRC-APA CCPA Testimony Feb 5 2019.pdf
Flag: Follow up

Thank you for the opportunity yesterday to offer input to the rulemaking related to the California Consumer Privacy Act (CCPA). Attached are written comments of the National Payroll Reporting Consortium (NPRC) and the American Payroll Association (APA). NPRC is a non-profit trade association whose member organizations provide payroll processing services to nearly two million U.S. employers, representing over 36% of the private sector workforce. The American Payroll Association (APA) is a nonprofit professional association representing more than 20,000 payroll professionals across the United States.

Privacy and protection of personal data have always been of paramount concern to payroll administrators and payroll service providers, and we applaud the objective of the legislation to establish appropriate and balanced legislation that effectively protects consumers.

We appreciate the initiative of the Attorney General's office in seeking public input. Our comments are intended to highlight ambiguous and/or overly broad definitions and terms in the law; to point out a number of practical implications and to seek clarity in related regulations. We would welcome the opportunity to discuss this further.

Pete Isberg

Vice President, Government Relations

ADP, LLC

[REDACTED]

President

National Payroll Reporting Consortium, Inc.

[REDACTED]

This message and any attachments are intended only for the use of the addressee and may contain information that is privileged and confidential. If the reader of the message is not the intended recipient or an authorized representative of the intended recipient, you are hereby notified that any dissemination of this communication is strictly prohibited. If you have received this communication in error, notify the sender immediately by return email and delete the message and any attachments from your system.



National Payroll Reporting Consortium

**AMERICAN
PAYROLL
ASSOCIATION**

**California Consumer Privacy Act Public Forum
February 5, 2019**

**Testimony of
The National Payroll Reporting Consortium¹ and
The American Payroll Association**

Privacy and protection of personal data are and always have been of paramount concern to payroll administrators and payroll service providers. We applaud the objective of the legislation and the efforts of policymakers to establish appropriate and balanced legislation that effectively protects consumers without unduly impeding the critical functioning of appropriately protected business activity.

We appreciate the initiative of the Attorney General's office in seeking public input to inform the rulemaking related to the California Consumer Privacy Act (CCPA), and the opportunity to offer comments today. Our comments are intended to highlight ambiguous and/or overly broad definitions and terms in the law; to point out a number of practical implications and to seek clarity in related regulations.

The Attorney General's website summarizes the Act as granting consumers:

"...new rights with respect to the collection of their personal information: a consumer can request that a business disclose what information it collects about the consumer, where it collected the information from, and with whom it has shared the information. Consumers may also request that their personal information be deleted and can opt-out of the sale of their personal information."

Thus, the CCPA creates new rights for California residents to access their personal information collected and maintained by a business; to have such information deleted and to opt out of the sale of their personal information.

¹ The National Payroll Reporting Consortium ("NPRC") is a non-profit trade association whose member organizations provide payroll processing and related services to nearly two million U.S. employers, representing over 36% of the private sector workforce.

The American Payroll Association (APA) is a nonprofit professional association representing more than 20,000 payroll professionals across the United States. APA's primary mission is to educate payroll professionals on the best practices associated with paying workers while complying with applicable laws and regulations. APA works with government to find ways to help employers with compliance, while minimizing the administrative burden on government, employers, and individual workers.

Our overarching concern is that the broad and ambiguous definitions of “sale,” “personal information,” and “consumer” may result in an inconsistent implementation of the law, which in turn could *decrease* privacy protections for individuals such as employees. For example, even a cursory internet search shows that there is widespread confusion and inconsistent analyses over whether employment-related records are regulated by the CCPA, with some commentators arguing that the law does not apply to employment-related records or that the law is superfluous due to conflicts with existing legal obligations, which may result in inconsistent application of privacy protections.

The Act does not apply where it would prevent compliance with federal or state law, and directs the Attorney General’s office to adopt regulations, including “establishing any exceptions necessary to comply with state or federal law.” We recommend that any regulations clarify the definitions noted above, and establish any exceptions necessary to eliminate ambiguity.

Right to opt-out of the sale of personal information

The right to opt out of any “sale” (i.e., transfer) could prevent the normal functioning of routine business operations, including employer payroll operations. The CCPA defines “sale” to include any *data transfer* “for monetary or other valuable consideration.”

The right to “opt out” under the CCPA is triggered by a broad definition of “sale” that does not only apply to contemporaneous exchanges of data or money, but includes any data transfer “for monetary or other valuable consideration.” The definition of “sale” is ambiguous. It is not clear whether the monetary consideration must be received for the actual purchase of personal data, as opposed to another business arrangement where the data is not the subject of the exchange. Without additional clarity, the term may include many types of routine data sharing for businesses; for example, business arrangements where personal information is not the subject of the exchange, transfers to third parties to prevent fraud or other criminal activity to preserve the effectiveness of anti-fraud, sanctions, and money-laundering screening and identity verification functions and services; and benchmarking activities that provides invaluable analysis to businesses, including employers.

The breadth of these definitions appear to confer a right for an employee to opt out of a transfer of critical business-related information, which could be problematic and prevent the normal functioning of routine employer payroll operations.

Right to Access

While not in conflict with the Act, access to personal information in the employment context is already established in California law, which provides that employees have the right to access their personnel files and records, including payroll records².

The definition of “personal information” is ambiguous in that it does not have to identify a “consumer”, but could relate to, or be capable of being linked to, a particular consumer *or household*. The inclusion of “household” could, for example, be read to allow a spouse to gain access to employee records, even when that person is not entitled to do so under current law. Even the definition of “consumer” is very broad by not applying only to actual “consumers” who have purchased or

² Labor Code Sections 1198.5, 226(b)

received services directly from a covered business.

Right to request that personal information be deleted

The right to have personal employment records deleted would conflict with many federal and state laws. For example, the California Labor Code requires employers to maintain detailed records reflecting virtually all activity with respect to employment, from hiring, enrollment in employee benefits such as health insurance and retirement savings plans; documentation of hours worked, wages earned, deductions from pay, and many other related matters. It would be very problematic if any employer was led to actually delete personal, wage and/or tax records under the CCPA.

Similarly, federal and state tax laws require employers to maintain detailed records of every wage payment, amounts withheld, and periodic summary reports of earnings, such as new hire reports and quarterly wage reports filed with the Employment Development Department; Forms W-2 filed with the Social Security Administration; IRS Forms 941, which report aggregate employment tax liabilities, and so on. Employers must be able to substantiate all such activity, and therefore any request for deletion of employment records would be substantially limited to records not required by law.

These data processing activities are all necessary for payroll and employment services administration, and any changes, such as employees having rights to opt out of fraud prevention services or delete employment-related records, may conflict with employer responsibilities to comply with the applicable laws and to protect their workforce. For example, assuming that the current form of the CCPA does encompass employee related data, an employee determined to have engaged in sexual harassment could request the opt-out from effective screening mechanisms or the deletion of critical employment records. Actual findings of harassment should be preserved in performance records.

The Attorney General is given broad authority to write regulations to further the purposes of the CCPA. We believe that broad and ambiguous definitions may result in an inconsistent implementation of the law, which in turn could defeat its purpose. We urge the Attorney General's office to clarify these points during rulemaking.

Again, we support California's commitment to protecting the privacy and security of personal data, and we appreciate the opportunity to offer comments today.

Contact information:

Pete Isberg
President, National Payroll Reporting Consortium

www.nprc-inc.org

Alice P. Jacobsohn, Esq.
Senior Manager, Government Relations
American Payroll Association

www.americanpayroll.org

Message

From: James Harrison [REDACTED]
Sent: 1/9/2019 3:20:27 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: California Consumer Privacy Act
Attachments: CCPA Proposed Regulations (Verifiable Request) 1.9.19 (00368819xAEBO3).pdf; CCPA Proposed Regulations (Opt-Out) 1.9.19 (00368821xAEBO3).pdf; CCPA Proposed Regulations (Use of Personal Information) 1.9.19 (00368822xAEBO3).pdf

Dear Privacy Regulations Coordinator,

On behalf of Californians for Consumer Privacy, attached please find proposed regulations to implement the CCPA. The proposed regulations address three topics: (1) verifiable consumer request; (2) consumers' right to opt-out of the sale of their personal information; and (3) the use of personal information for business purposes.

Thank you for your consideration.

James

James C. Harrison

Remcho, Johansen & Purcell, LLP

1901 Harrison Street, Suite 1550

Oakland, CA 94612



CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.

PROPOSED REGULATIONS TO IMPLEMENT VERIFIABLE CONSUMER REQUEST

BACKGROUND

What does a verifiable consumer request apply to?

A consumer must submit a “verifiable consumer request” in order to exercise the consumer’s rights to obtain information about a business’s collection and use of a consumer’s personal information and to request deletion of a consumer’s personal information, as follows:

Sec. 1798.100: Right to request disclosure of: (1) categories of personal information collected and (2) specific pieces of information collected. *(Note that this overlaps with the right in section 1798.110 to request the disclosure of categories of personal information collected and specific pieces of personal information, but section 1798.100 has its own compliance provisions while compliance with section 1798.110 is governed by Section 1798.130. See the note in “What obligations do businesses have with respect to verifiable consumer requests?”, below, for a recommendation about how to address this.)*

Sec. 1798.105: Right to request that a business that has collected personal information from a consumer delete that personal information, unless an exception applies.

Sec. 1798.110: Right to request disclosure of: (1) categories of personal information collected, (2) categories of sources from which personal information is collected, (3) the business purpose or commercial purpose for collecting or selling the consumer’s personal information, (4) the categories of 3rd parties with whom the consumer’s personal information is shared, and (5) specific pieces of personal information.

(Note that section 1798.110(b) requires disclosure pursuant to 1798.130(a)(3), which only addresses disclosure of categories of personal information collected; however, because section 1798.110(a) and (b) establish the right to request such information and the obligation to disclose the information, the Attorney General’s regulation should address all of the information specified in subdivision (a) of section 1798.110.)

Sec. 1798.115: Right to request that a business that sells a consumer’s personal information, or that discloses it for a business purpose, disclose the categories of personal information collected, the categories of personal information sold, the categories of 3rd parties to whom the personal information is sold, the categories of personal information disclosed for a business purpose, and the categories of 3rd parties to whom the personal information is disclosed for a business purpose.

(Note that section 1798.115(a) does not require disclosure of the categories of 3rd parties to whom the personal information is disclosed for a business purpose, but subdivision (b) of section 1798.115 requires compliance with section 1798.130(a)(4), which requires a business to disclose the categories of 3rd

parties to whom the personal information is disclosed for a business purpose, in addition to the categories of 3rd parties to whom the information is sold. The Attorney General's regulations should therefore include disclosure of the categories of 3rd parties to whom the consumer's personal information is disclosed for a business purpose, in addition to the categories of third parties to whom the information is sold.)

What is the definition of a verifiable consumer request?

Sec. 1798.140(y) defines a “verifiable consumer request” as “a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer’s behalf.”

(Note that this definition does not cross-reference section 1798.100, but because that section uses the same term, the Attorney General's regulations should apply equally to requests made pursuant to section 1798.100.)

What obligations do businesses have with respect to verifiable consumer requests?

Section 1798.100, which allows a consumer to request disclosure of the categories of personal information and specific pieces of personal information collected about the consumer by a business, requires a business to “promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable [format] and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.”

(Note that, unlike section 1798.130, which requires that the information be provided within 45 days [with an additional 45 day extension if reasonably necessary], section 1798.100(d) does not impose an express time limit. In addition, it does not address a business's obligation to verify a request. Given the overlap between sections 1798.100 and 1798.110, however, the Attorney General's regulations should apply equally to the submission of verifiable consumer requests under both sections.)

Section 1798.130(a)(1) requires a business to make two or more “designated methods for submitting requests” available to consumers to submit a verifiable consumer request for information pursuant to sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.

(Note that this section does not cross-reference section 1798.100, but as discussed above, the regulations should apply equally to both sections in light of the overlap.)

Section 1798.140(i) defines “designated methods for submitting requests” to mean “a mailing address, email address, Internet Web page, Internet Web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.”

Section 1798.130(a)(2) requires a business, upon receipt of a request from a consumer, to promptly take steps to determine whether the request is a verifiable consumer request. The determination of whether a request is verified does not extend the business’s duty to disclose and deliver the information within 45 days of receipt of the consumer’s request, unless the business reasonably determines that it needs additional time and provides notice of the extension to the consumer within the first 45-day period, in which case the deadline to respond may be extended once by an additional 45 days. “The disclosure shall cover the 12-month period preceding the business’s receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer’s account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer’s option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business shall not require the consumer to create an account with the business in order to make a verifiable consumer request.”

What are the Attorney General’s responsibilities with respect to adopting a regulation to implement the provisions of law relating to a verifiable consumer request?

Section 1798.185(a)(7) requires the Attorney General to “[e]stablish[] rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer’s or the consumer’s authorized agent’s ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business’s determination that a request for information received by a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the

business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter."

PROPOSED REGULATIONS¹

Definition of "verifiable consumer request"

A "verifiable consumer request" means a request submitted by a consumer, by a consumer on behalf of the consumer's minor child aged 13 or less, or by the consumer's authorized agent, pursuant to sections 1798.100, 1798.105, 1798.110, or 1798.115, as to which the business that receives the request authenticates that the consumer who submitted the request, or on whose behalf the request is submitted, is the consumer about whom the request is made.

Definition of "authenticate"

"Authenticate" means to use reasonable measures to verify that a consumer who submits a verifiable consumer request, or on whose behalf a verifiable consumer request is submitted, for the disclosure of information pursuant to sections 1798.100, 1798.110, and 1798.115, or who requests deletion of personal information pursuant to section 1798.105, is the consumer to whom the request pertains, including but not limited to, through the use of a user name and password by a consumer who maintains an account with the business while the consumer is logged into the account, two-factor authentication, knowledge-based challenge-response authentication, or a similar method that offers the consumer an opportunity to verify the consumer's identity to the business, provided that the method is not unduly burdensome to the consumer.

Definition of "two-factor authentication"

"Two-factor authentication" means a security process in which the consumer provides two different pieces of evidence to verify themselves, such as evidence establishing something they know, something they have, or something they are.

Definition of "knowledge-based challenge response"

"Knowledge-based challenge-response" means a security process in which the business asks the consumer a question based on non-public information known to the consumer and the business to which the consumer must provide a correct response.

¹ To the extent that the proposed regulations use terms defined by the CCPA (e.g., consumer, person, etc.), the definitions set forth therein shall apply to the regulations.

Definition of “self-authenticate”

“Self-authenticate” means a process whereby a consumer verifies the consumer’s identity to the business, provided that the method is not unduly burdensome to the consumer, including but not limited to, by providing the consumer’s user name and password to the business while logged into the consumer’s account, providing two different pieces of evidence to the business to verify themselves, responding correctly to a question asked by the business based on some private information known to the consumer, or using a similar method to verify the consumer’s identity directly to the business.

Definition of “authorized agent”

“Authorized agent” means a natural person, or a person registered with the Secretary of State authorized by the consumer, or by a consumer on behalf of the consumer’s minor child aged 13 or less, to act on the consumer’s behalf.

Use of Authorized Agent

A consumer may use an authorized agent to submit a verifiable consumer request to a business on the consumer’s behalf, provided that either: (1) the authorized agent facilitates the submission of the consumer’s verifiable consumer request, and if applicable, the reception of data on the consumer’s behalf, and the consumer is required to self-authenticate; or (2) the consumer provides the agent with the consumer’s power of attorney to submit the request on the consumer’s behalf to the business pursuant to section 4401 of the Probate Code. The power of attorney must be notarized and signed in the presence of two witnesses.

Inclusion of Identifiers in verifiable consumer request

Businesses shall allow consumers who submit a verifiable consumer request to provide the business with the consumer’s verifiable identifiers for the purpose of associating those verifiable identifiers with any personal information previously collected about the consumer by the business. A business that receives or collects personal information from a consumer in connection with the consumer’s submission of a request or the business’s verification of the request shall use that information solely for the purposes of verification and responding to the consumer’s request.

Definition of verifiable identifier

“Verifiable identifier” means an identifier, including but not limited to a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers, provided that the business authenticates that the identifier belongs uniquely to the consumer.

Requirement to respond within 45 days

(a) A business that receives a verifiable consumer request pursuant to sections 1798.100, 1798.110, or 1798.115, shall disclose and deliver the required information to the consumer within 45 days of receipt of the verifiable consumer request. The business may extend this deadline by 45 days, provided that the business determines that it is reasonably necessary and provides notice of the 45-day extension to the consumer. This deadline shall not be extended as a result of the time spent by the business to determine that the request is a verifiable consumer request.

(b) A business that receives a verifiable consumer request pursuant to section 1798.105 shall delete the required information and notify the consumer of its action within 45 days of receipt of the verifiable consumer request. The business may extend this deadline by 45 days, provided that the business determines that it is reasonably necessary and provides notice of the 45-day extension to the consumer. This deadline shall not be extended as a result of the time spent by the business to determine that the request is a verifiable consumer request.

PROPOSED REGULATIONS TO IMPLEMENT RIGHT TO OPT-OUT

BACKGROUND

Right to opt-out

Section 1789.120 authorizes a consumer to opt-out of the sale of the consumer's personal information. A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information, has not received consent to sell the minor consumer's personal information, is prohibited from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.

Right of Consumer to Use Authorized Agent

Section 1798.135(c) authorizes a consumer to authorize another person to opt-out of the sale of the consumer's personal information on the consumer's behalf.

Obligation of businesses to comply with right to opt-out

Section 1798.135 requires businesses to notify consumers of the right to opt-out of the sale of the consumer's personal information and to refrain from selling the personal information of consumers who have opted-out. It also requires businesses to respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information, and it prohibits businesses from using any personal information collected from the consumer in connection with the submission of the consumer's opt-out request for any purpose other than complying with the opt-out request.

Section 1798.135(c) requires a business to comply with an opt-out request received from "a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General."

Attorney General's obligations with respect to right to opt-out

Section 1798.185(a)(4) requires the Attorney General to adopt rules and regulations to: (1) facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information; (2) govern businesses' compliance with a consumer's opt-out request; and (3) develop a recognizable and uniform opt-out logo or button for use by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

PROPOSED REGULATIONS¹

Use of Opt-Out Agent

A consumer aged 16 or more may authorize another person to opt-out of the sale of the consumer's personal information on the consumer's behalf. A business shall comply with an opt-out request submitted by a person on behalf of the consumer provided that the person certifies that the consumer has authorized the person to opt-out of the sale of the consumer's personal information on the consumer's behalf.

Opt-Out Notice

(a) Businesses shall maintain an opt-out button or logo that reflects the opt-out status of the consumer. Businesses shall not ask a consumer whom the business can identify, or probabilistically identify, and who has opted-out of the sale of their information, to consent to the sale of their information for twelve months following the date the consumer most recently opted-out of the sale of the consumer's personal information.

(b) If the consumer has opted-out of the sale of the consumer's personal information, the button or logo shall notify the consumer that the business is not selling the consumer's personal information, through a method of display that is clear and obvious to the consumer as to the opt-out status of that consumer, including but not limited to by making the button inactive and displaying a message that the consumer has already opted-out of the sale of their information.

(c) If the consumer has not opted-out of the sale of the consumer's personal information, or if the business is unable to identify the consumer, the opt-out button or logo shall be active so that the consumer may elect to opt-out of the sale of the consumer's personal information.

¹ To the extent that the proposed regulations use terms defined by the CCPA (e.g., consumer, person, etc.), the definitions set forth therein shall apply to the regulations.

PROPOSED REGULATIONS TO IMPLEMENT BUSINESS PURPOSES EXCEPTION

BACKGROUND

Definition of Business Purpose

Section 1798.140(d) defines “business purpose” to mean “the use of personal information for the business’s or a service provider’s operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected.

Business purposes are:

- (1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.
- (2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.
- (3) Debugging to identify and repair errors that impair existing intended functionality.
- (4) Short-term, transient use, provided that the personal information is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer’s experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.
- (5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.
- (6) Undertaking internal research for technological development and demonstration.
- (7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

Definition of Service Provider and Written Contract Requirement

Section 1798.140(v) defines “service provider” to mean “a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.”

Definition of Commercial Purpose

Section 1798.140() defines “commercial purpose” to mean “to advance a person’s commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. ‘Commercial purposes’ do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.”

The definition of “service provider” makes clear that a service provider may only use a consumer’s personal information for the commercial purpose of providing the services specified in the contract with the business.

Service Provider Exception

Section 1798.140(t) defines “sell” to exclude the use or sharing of a consumer’s personal information with a service provider “that is necessary to perform a business purpose” if two requirements are met: (1) The business has provided notice that consumers’ personal information is being used or shared in its terms and conditions consistent with Section 1798.135; and (2) the service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

(Note that the definition of service provider also prevents the service provider from “retaining” or “disclosing” the personal information, other than to provide the services specified in the contract.)

Third Party Definition

Section 1798.140(w)(2)(A) defines “third party” to exclude a “person to whom the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract” prohibits the person from selling, retaining, using, or disclosing the personal information other than for the business purpose specified in the contract and includes a certification by the person that it will comply with these restrictions.

As a result of this exception, the transfer of information by a business to a person (which is defined broadly in section 1798.140(n) to include individuals, corporations, associations, etc.) for a business purpose pursuant to a contract that satisfies these terms is not considered a sale of personal information.

PROPOSED REGULATIONS¹

Definition of Contractor

“Contractor” means a person to whom the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the person from selling, retaining, using, or disclosing the consumer’s personal information other than for the business purpose specified in the contract and includes a certification by the person that the person will comply with these restrictions.

Use of Personal Information by Service Provider or Contractor

(a) A service provider or contractor shall only use a consumer’s personal information for the purposes of providing services specified in the written contract to the business. A service provider or contractor shall not further collect, sell, disclose, use, or retain the personal information of the consumer, including but not limited to, for the purpose of enhancing the services it provides to another person.

(b) In order to comply with subdivision (a), a service provider or contractor shall separately maintain or “silo” personal information it receives from a business about a consumer from: (1) personal information it receives about the same consumer from another person and (2) personal information it receives about the same consumer from that consumer’s interaction with the service provider or contractor.

¹ To the extent that the proposed regulations use terms defined by the CCPA (e.g., consumer, person, etc.), the definitions set forth therein shall apply to the regulations.

(c) A service provider or contractor shall be prohibited from using or accessing personal information received from a business or from the consumer's interaction with the service provider or contractor for the purpose of providing services to another person.

(d) A service provider or contractor shall be prohibited from aggregating the personal information it receives about a consumer from a business with the personal information it receives from another person about the same consumer, or with the personal information it receives from the same consumer's interaction with the service provider or contractor.

Retention of Personal Information for Advertising

A person that obtains access to a consumer's personal information for the purpose of preparing a bid for the use of that information for advertising or marketing services shall be required to delete the consumer's personal information to which it had access as part of the bid process if the bid is not successful.

Definition of "advertising or marketing services"

"Advertising or marketing services" means the transmission or receipt of personal information by, or on behalf of, a business for the purposes of inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.

Message

From: Benjamin Trice [REDACTED]
Sent: 1/8/2019 2:44:54 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA (1798.185) - Public Feedback

Beyond following standard best practices on logo / iconography development, here are some additional thoughts on the logo / button as it relates to the California Consumer Privacy Act:

- Logo / ability to request consumer data should be linked at the bottom of email communications so it can be treated similar to how it is for an Unsubscribe link.
- Links for Data Requests should also link directly to a CA Gov website that provides information on consumer rights under the law and what can be specified. This should be presented in a form that is easy to understand for the most average of consumers.
- Companies required to comply should have a page that can be searched and found using basic search terms that are standard (i.e. privacy, ccpa, consumer privacy).
- To assist with smaller businesses, CA Gov should have a website that can be linked to provide all of the latest information as it complies with the act. This way it is a simple direct link for the smaller businesses to comply with.

Benjamin Trice

mail: [REDACTED]

Google #: [REDACTED]

Message

From: Eva Gutierrez [REDACTED]
Sent: 3/7/2019 3:21:56 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA - Comment Submission from Sift Science, Inc.
Attachments: Sift Comment to AG re CCPA Antifraud Exception 190307.pdf

Privacy Regulations Coordinator,

Please find attached a written comment on behalf of Sift Science, Inc. to the California Consumer Privacy Act of 2018.

Respectfully,
Eva Gutierrez

--



Eva Gutierrez
Senior Director, Legal and Compliance





123 Mission Street, Suite 2000
San Francisco, CA 94105
www.sift.com

March 7, 2019

Via Email

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

Re: *Comment on California Consumer Privacy Act: Protection of Anti-Fraud Technologies*

Dear Attorney General Becerra:

Sift Science, Inc. ("Sift") submits these comments for your consideration as part of the Attorney General's preliminary rulemaking activities under the California Consumer Privacy Act ("CCPA"). We appreciate the opportunity to submit our views on these important consumer issues. As described in greater detail below, in the interest of consumer safety, Sift urges the Attorney General to use its rulemaking authority to clarify and support the anti-fraud exception to the CCPA.

1. Background on Sift's Services

Sift provides its customers with a suite of digital trust and safety products designed to prevent fraudulent activity in real time. Sift uses machine learning in a proprietary and algorithmic way to identify patterns in customer data that it receives across its customers – in other words, through crowd-sourced data inputs. The data it derives in real time from its customers is crucial to accurately detecting potential fraud patterns. Sift's services include:

- **Payment Protection:** We help ecommerce businesses to prevent fraudulent payment transactions/orders on their websites.
- **Account Defense:** We help businesses prevent fake account creation and malicious takeovers of legitimate accounts.
- **Content Integrity:** We help publishers and community-based businesses prevent and/or block malicious content, such as fake listings and fake reviews.

To provide these services, Sift collects a number of data points that are "personal information" under the CCPA. For example, we typically collect email address, IP address, cookie and user agent (for browsers), and app installation ID (for apps) - we correlate those data points to create fraud indicators. Based on this data, we assign a relative fraud score of 1-99 when a customer's end user logs into the service (or performs a particular activity after logging in) to represent the likelihood that the activity is fraudulent.

The effectiveness of our services depends on our ability to correlate data across customers. To provide a very basic illustration: when multiple data points have been repeatedly correlated together in the same way over time (say, an email address that for several years has been correlated with the same or the same series of IP address), Sift's algorithms may produce a low fraud score for that email address relative to the customer, in which case the customer may elect to "whitelist" that user for account creation rather than performing additional fraud checks. Conversely, Sift's solutions may generate a higher fraud score for a device or IP address attempting to create a new account on a customer's website because of prior activity identified as fraudulent by other Sift customers.

2. The Importance of Crowd-Sourced Fraud Solutions

In order for our fraud solutions (and those of our competitors) to be effective, they must pool data collected from many sources. Customer A may receive a score that is partially-derived from and therefore relates to various "personal information" collected from Customer B, Customer C, and Customer D (and many other customers).

In fact, such pooling of data is the essence of an effective anti-fraud solution – using data from a wide range of sources and sharing conclusions with others to prevent harm to potential victims. Absent that information sharing, anti-fraud solutions would be little more than guesswork – and at best would make broad assumptions about website visitors based on more rudimentary factors.

As described below, while we believe the California legislature surely intended the CCPA to permit such services, certain language within the CCPA is confusing and, we believe, calls for clarification by the Office of the Attorney General.

3. Relevant CCPA Provisions

Certain CCPA provisions suggest that no "sale" of personal information occurs when businesses and service providers use and disclose personal information for anti-fraud purposes. (We have assumed that a fraud score that is associated with an individual, device or browser is "personal information," given the broad definitions in section 1798.140(o).)

For instance, the term "business purpose" includes "detecting security incidents, [and] protecting against malicious, deceptive, fraudulent or illegal activity." Section 1798.140(d)(2). This suggests to us that the CCPA recognizes at least as a general matter the need to protect uses of personal information for anti-fraud purposes.

Additionally, under Section 1798.140(d), a service provider's use of a business's personal information for the service provider's own "operational" purposes is itself a "business purpose." In other words, a service provider may generally crowd-source personal information that it receives from a business for its own operational purposes without rendering the initial disclosure of information from the business to the service provider a "sale" of the personal information by the business. This too suggests that crowd-sourced fraud solutions are a business purpose rather than a sale of information.

On the other hand, section 1798.140(t)(2)(C) adds confusion to this issue. Under that provision, a business is not deemed to sell personal information when it “uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose” so long as “the service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.” As applied to crowd-sourced fraud solutions: these anti-fraud services unquestionably use the personal information of each to perform a business purpose – a collectivized anti-fraud business purpose. But it may not be “the business purpose” for which it was submitted by a given customer if read narrowly. For instance, Customer A may have submitted personal information as part of its payments fraud subscription, and that personal information also will be used for Customer B’s payments fraud subscription and its anti-spam fraud subscription. We believe this is a distinction without a difference that should not be read to limit sharing of derived personal information for fraud solutions – and we ask the Attorney General to confirm that is the case.

It is critical for anti-fraud services to not only collect personal information from multiple customers, but also to disclose derivatives based on that personal information to multiple customers. Whatever crowd-sourced score, flag, or other signal is developed by an anti-fraud service must (in most cases) be shared with the customer to be effective. But if the disclosure to a customer of a score that is derived from the personal information of multiple customers is deemed a “sale” of personal information, fraudsters could simply opt-out of the “sale” of their personal information under section 1798.120(a). For obvious reasons, permitting this would undermine the effectiveness of anti-fraud solutions.

4. Clarification We Are Requesting

We think that the CCPA cannot (and must not) logically be read to cede control of crowd-sourced, distributed fraud solutions to the fraudsters themselves. Assuming we are correct, then the onward commercial transfer of fraud scores (or similar signals) by anti-fraud providers like Sift cannot and ought not be deemed a “sale.”

Given the statutory tension we have described above, we request that the Attorney General clarify that crowd-sourced fraud solutions as described above do not involve the “sale” of personal information. One way to accomplish this would be for the Attorney General to confirm that the definition of “business purpose in” Section 1798.140(d)(2) as including “detecting security incidents, [and] protecting against malicious, deceptive, fraudulent or illegal activity” overrides the “further sale or use” provision in 1798.140(t)(2)(C)(ii). An alternative way to accomplish this would be clarify that the phrase “except as necessary to perform the business purpose” in section 1798.140(t)(2)(C) is to be read liberally –in this case, to mean, effectively, “in order to perform any security-related, anti-malware or anti-fraud purpose.”

Sift would be pleased to meet with your staff or provide any further information or insight that might be useful. Thank you for considering this important matter.

Respectfully submitted,

Eva Gutierrez
Senior Director, Legal and Compliance
Sift Science, Inc.

Message

From: Pulliam, Eva [REDACTED]
Sent: 3/8/2019 6:49:51 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: [REDACTED]
Subject: CCPA - Preliminary Comment - Request for Clarification

Attorney General Becerra,

Our firm represents clients across a wide spectrum of industries who will need to comply with the California Consumer Privacy Act. Accordingly, we seek clarification regarding the definition of "personal information." Currently, the CCPA defines "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Is the term "household" intended to include information pertaining to casual workers (e.g., babysitters, gardeners, etc.), pets, and others who may be seen as members of a household?

Regards,

Eva J. Pulliam

Associate

Arent Fox LLP | Attorneys at Law

55 2nd Street, 21st Floor
San Francisco, CA 94105

[REDACTED]

[REDACTED] www.arentfox.com

CONFIDENTIALITY NOTICE: This e-mail and any attachments are for the exclusive and confidential use of the intended recipient. If you received this in error, please do not read, distribute, or take action in reliance upon this message. Instead, please notify us immediately by return e-mail and promptly delete this message and its attachments from your computer system. We do not waive attorney-client or work product privilege by the transmission of this message.

CCPA00000182

Message

From: Gibbons, Jennifer [REDACTED]
Sent: 3/8/2019 4:42:14 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Desmond, Edward [REDACTED]; Pasierb, Stephen [REDACTED]; Sheila Millar, Esq. [REDACTED]; Leigh Moyers [REDACTED]
Subject: CCPA -- Toy Association Comments March 2019
Attachments: Toy Association Comments on CCPA 030819.pdf; 2019-03-08 CCPA Comment Attachment.pdf

Hello,

Attached, please find comments from the Toy Association, on behalf of its members, regarding the California Consumer Privacy Act (CCPA). Additionally, we have included a chart to summarize our issues and recommendations for consideration. The Toy Association appreciates the Attorney General's effort to solicit input from stakeholders on the CCPA in advance of its rulemaking initiative.

By way of background, The Toy Association represents more than 1,100 businesses – toy manufacturers, importers and retailers, as well as toy inventors, designers and testing labs – all involved in bringing safe, fun and educational toys and games for children to market. The Toy Association and its members work with government officials, consumer groups, and industry leaders on ongoing programs to ensure safe play, both online and offline.

The toy industry is deeply committed to privacy, security and product safety, and supports strong and effective standards to protect consumers. We support principles of transparency, notice, consumer choice, access, correction and deletion rights for consumers, and reasonable security, all part of the objectives of the CCPA.

Please feel free to contact us with any questions, or if additional information regarding our comments is needed.

Best,
Jennifer

Jennifer Gibbons
Vice President, State Government Affairs

1375 Broadway, Suite 1001 • New York, NY 10018



www.toyassociation.org

March 8, 2019

Via Electronic Submission: privacyregulations@doj.ca.gov

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

Re: Comments on the CCPA

The Toy Association, Inc., on behalf of its members, appreciates the Attorney General's effort to solicit input from stakeholders on the California Consumer Privacy Act (CCPA) (Cal. Civ. Code §§ 1798.100–1798.199) in advance of its rulemaking initiative. By way of background, The Toy Association represents more than 1,100 businesses – toy manufacturers, importers and retailers, as well as toy inventors, designers and testing labs – all involved in bringing safe, fun and educational toys and games for children to market. The U.S. toy industry contributes an annual positive economic impact of \$109.2 billion to the U.S. economy. The Toy Association and its members work with government officials, consumer groups, and industry leaders on ongoing programs to ensure safe play, both online and offline. The toy industry is deeply committed to privacy, security and product safety, and supports strong and effective standards to protect consumers. We support principles of transparency, notice, consumer choice, access, correction and deletion rights for consumers, and reasonable security, all part of the objectives of the CCPA.

Our members not only create toys that are physically safe for children to play with, but also engage with children, as well as parents, online. Protecting children and maintaining the trust of parents are the most vital concerns for the toy industry. Toy industry members are heavily regulated by an extensive set of preemptive laws, including the Children's Online Privacy Protection Act of 1998 (COPPA) (15 U.S.C. §§ 6501–6506), and a variety of product safety laws, such as the Consumer Product Safety Act (CPSA) (codified at 15 U.S.C. §§ 2051–2089) and Federal Hazardous Substances Act (FHSA) (15 U.S.C. §§ 1261–1278), as modified by the Consumer Product Safety Improvement Act (CPSIA). Thus, the toy industry is uniquely qualified to comment on consumer privacy and data security issues raised by this new California law and potential conflicts with federal law in light of CCPA §1798.196 with a view to promoting more clarity.

Our comments focus on six key issues:

- Preemption language of COPPA and the CCPA, and key inconsistencies between the CCPA and the COPPA statute and rule.
- Key definitions, including “personal information” and “selling.”
- Operational burdens of the CCPA, including the mandatory “Do Not Sell My Personal Information” button and mandatory options for submitting access requests.
- Covered businesses will include many very small companies operating in California.

- Implications of a private right of action for security breaches.
- Recognizing safe harbor programs.

The above does not represent a comprehensive list of all potential issues affecting our members.

Attachment A provides a matrix with an overview of our comments for convenient reference.

CCPA Recognizes the Preemptive Effect of COPPA

Section 1798.196 of the CCPA contains a general preemption section, stating:

This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the California Constitution.

Congress expressly created a national preemptive regime governing children’s privacy when it enacted COPPA in 1998, stating:

No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section.

See 15 U.S.C. §6502(d). Thus, although the CCPA does not expressly mention COPPA in the list of federal laws that preempt the CCPA at §1798.145, the CCPA recognizes the preemptive effect of COPPA.

While many Toy Association members deal exclusively with parents and adult purchasers, a significant number of our members offer digital experiences directed, primarily or secondarily, to children under 13. While our members are affected by the CCPA in all their operations, definitional inconsistencies between the CCPA and COPPA and new CCPA obligations are in conflict with COPPA and create confusion. The COPPA approach, which balances privacy harms with burdens to consumers and businesses, provide some useful guidance to consider in implementing the CCPA.

Key CCPA Definitions Conflict with COPPA

When Congress enacted COPPA, it established a national legal framework for children’s privacy that reflects a common-sense harms-based approach. In other words, COPPA seeks to balance privacy risks to children under 13 for certain types of data collection, use and sharing with a recognition of business needs and consumer convenience through its definitions, exceptions, and “sliding scale” approach to parental consent. The CCPA’s broad definitions of “personal information” and “sale” risk undermining privacy-safe practices authorized under COPPA. The apparent requirement that a business obtain parental consent any time a business engages in the “sale” of “personal information,” for example, conflicts with COPPA due to the overbroad definition of both terms. Likewise, imposing an opt-in consent process on businesses who “sell” information concerning individuals 13 – 16 would impose unnecessary limits on necessary and useful business operations that COPPA recognizes do not require parental consent when the data involves children under 13. Concepts from the approach in COPPA might be usefully applied to advance the CCPA objectives in protecting the privacy of teens 13 – 16.

We highlight below three key major inconsistencies between provisions of the CCPA and COPPA: the reference age of a “child,” the definition of “personal information,” and the definition of a “sale.” We

also provide examples of how COPPA’s risk-based approach allows for privacy-safe interactions without burdening parents, children or businesses with consent obligations.

Who Is a Child

The CCPA and COPPA define “children” very differently. COPPA defines a “child” to include children “under 13” (*see* 15 U.S.C. §6501(1)). Congress established this age cut-off deliberately, recognizing that teens have their own sphere of privacy and parental consent models will never work effectively with the teen population. This reference age aligns with the definition of a child under the Consumer Product Safety Improvement Act, which refers to products designed and intended primarily for children 12 and younger. Thus, for both informational safety and physical product safety purposes – key issues for toy industry members – federal law recognizes that the at-risk population should be defined as under 13. The CCPA, in contrast, does not define “children” in the definitions section at §1798.140. Instead, §1798.120(d) prohibits a business with *actual knowledge* that a consumer is under 16, from “selling” (defined to include sharing) personal information of such individual absent consent of a parent or guardian for those under 13, or the individual’s opt-in consent, for those 13 – 16.

While the CCPA imposes a parental consent obligation on all information collected and “sold” when a business has “actual knowledge” that an individual is under 13, COPPA creates a framework under which online services primarily directed to children are obligated to *assume* that they are dealing with a child under 13. Businesses with actual knowledge that they are dealing with a child under 13 are also subject to COPPA.

We briefly discuss below how the CCPA’s approach to managing data from children and teens under §1798.120(d) conflicts with COPPA, and would impose unworkable and unnecessary operational restrictions on businesses without advancing privacy. From this standpoint, the CCPA’s overbroad definitions of “personal information” and “selling” must be reviewed together to understand those inconsistencies and the public policy and business implications as a result.

“Personal Information” and “Selling” Under the CCPA

COPPA, last amended by the Federal Trade Commission (FTC) in 2013 (78 Fed. Reg. 3,971 (Jan. 17, 2013)), has been in force for more than 20 years since enactment, and has been revised several times to reflect changes in the online landscape. The COPPA Rule, consistent with the harms-based approach established by Congress, excludes certain data collection and uses from the obligation to obtain parental mandating consent because risks to children versus burdens on parents and businesses do not warrant it. *See* 16 C.F.R. §312.5(c). The CCPA’s blanket obligation that businesses obtain parental consent before “selling” any type of personal information of children, as broadly defined in the CCPA, is at odds with COPPA.

The CCPA defines “personal information” at §1798.140(o)(1) to include a broad variety of data generally, including data traditionally considered to be anonymous, such as an alias, or an Internet Protocol (IP) address, as well as browsing history. Section 1798.140(o)(2) excludes from the broad definition of “personal information” only “publicly available” information. Yet COPPA permits the collection of certain information – including limited personal contact information, like an e-mail address – without parental consent in a number of circumstances. For example, operators can collect a child’s email address for certain purposes, and can ask a child to furnish a parent’s email address to contact a parent and obtain consent. COPPA recognizes that absent a vehicle to request some type of contact information about a parent from a child, there would be no way to provide notice to parents and start any

necessary consent process. These COPPA-permitted types of data collection, use and sharing are not reflected in the CCPA.

Consistent with COPPA, an operator can also collect a user name (potentially an “alias” under the CCPA) and a password from a child under 13, and link it to a device identifier such as an IP address, to recognize a returning child visitor. This allows for some personalization with limited risk to a child’s privacy, without the need to collect any personal contact information or to obtain parental consent. The COPPA Rule recognizes that this type of limited data collection will allow businesses to enhance a child’s online experience by, for example, allowing a child to save game scores in an online game, and that this involves no risk to children that would require parental consent. Characterizing an “alias” as *per se* personal information thus is in conflict with COPPA. Likewise, an operator under COPPA can collect an IP address or other persistent identifiers used over time *and* across websites solely to support an online service’s internal operations without either obtaining parental consent or providing notice. 16 C.F.R. §312.5(c)(7). The FTC rejected the notion that parents should have to consent to the collection of this type of anonymous information to support its operations, as doing so would have forced companies to block child visitors and obtain parental consent before any type of interaction, preventing them from serving children in a privacy-safe way. It goes without saying that such collection and use fall outside parental access and deletion obligations. Notably, this exception does not cover data collected for online behavioral advertising purposes, which is strictly prohibited under COPPA absent parental consent.

Under the COPPA Rule, IP addresses and other information can be collected and shared to support the internal operations of a website or online service so long as the information collected for such purposes is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose. 16 C.F.R. §312.2. Support for internal operations means those activities necessary to:

- (a) maintain or analyze the functioning of the website or online service;
- (b) perform network communications;
- (c) authenticate users of, or personalize the content on, the website or online service;
- (d) serve contextual advertising on the website or online service or cap the frequency of advertising;
- (e) protect the security or integrity of the user, website, or online service;
- (f) ensure legal or regulatory compliance; or
- (g) fulfill a request of a child as permitted by these guidelines.

The FTC also specified when it updated the COPPA Rule in 2013 that support for internal operations also includes activities such as intellectual property protection, payment and delivery functions, spam protection, optimization, statistical reporting, or de-bugging. *See* 78 Fed. Reg. at 3,981.

Collection and sharing of this type of information is essential to provide services and manage business operations, and COPPA recognizes that imposing a parental consent obligation for such uses would burden businesses and parents without advancing children’s privacy. Consistency in approaches is therefore vital.

Conflicts between COPPA and the CCPA are exacerbated by the CCPA’s definition of “sale.” The CCPA establishes that a business does not “sell” personal information under certain circumstances, but those circumstances are confusingly described at §1798.140(t)(2)(C):

- (C) The business uses or shares with a service provider information of a consumer that is necessary to perform a business purposes [sic] if two conditions are met: services that the

service provider performs on the business' behalf, provided that the service provider also does not sell the personal information.

(i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.

(ii) The service provider does not further collect, sell or use the personal information of the consumer except as necessary to perform the business purpose.

The inartful wording in the CCPA definition creates confusion and potential conflicts with COPPA. The language also appears inconsistent with the exemption from the obligation to delete personal information upon a consumer's request in §1798.150(d).

Most online services – whether or not they are directed to children - cannot function without collecting and sharing a variety of data that helps support internal operations. The COPPA Rule exceptions thus recognize that for businesses to function, they must be allowed to collect and share certain types of data without parental consent. This allows businesses that offer child-directed online services to offer those services to children in a privacy-safe manner that gives businesses the flexibility to responsibly manage online operations.

Requiring that businesses must obtain the opt-in consent from teens 13 – 16 before a California business can share any type of “personal information” used to support operations and functionality fails the risk balancing test that undergirds the COPPA “support for internal operations” exception. Imposing such an obligation risks undermining customer service and consumer convenience without materially enhancing teen privacy. The common-sense approach of the COPPA Rule thus can usefully be applied not only to children's data, but to collection and sharing of all similar data from teens subject to the CCPA. However, this requires addressing the confusing and inconsistent statutory language.

The CCPA's Operational Burdens

Definitional Inconsistencies Add to Burdens

Operational compliance burdens imposed by the CCPA are exacerbated by inconsistencies in the Act's definitions and obligations. For example, §1798.140(o) excludes from the definition of “personal information” only “publicly available” information. However, a business does not “sell” personal information under circumstances that are confusingly described in §1798.140(t)(2)(C), as noted above, and is not obligated to delete personal information under §1798.104(d) under circumstances that seem to reflect, at least in part, activities that would constitute “support for internal operations” under COPPA. It appears that the drafters may have intended to cover activities that qualify for the COPPA exemption for “support for internal operations,” but the inartful wording creates confusion and potential conflict. Likewise, defining a “service provider” in §1798.140(v) to only include an entity that operates under a written contract fails to recognize the widespread use of online agreements or other arrangements through which information might be shared to support internal operations.

Section 1798.125 of the CCPA prohibits discrimination against a consumer who exercises any of the rights set forth in the Act, including “denying goods or services to the consumer.” However, COPPA acknowledges that there are circumstances where a firm may terminate a child's access to services if a parent refuses or withdraws consent. 16 C.F.R. §312.6(c). In fact, if a parent withdraws consent for an activity that requires verifiable consent, the business could not allow the child to continue to participate. This is not discrimination, but represents another conflict between the CCPA and COPPA.

Home Page Button Is Burdensome

Another example of a significant burden is the requirement for a “Do Not Sell My Personal Information” button at the home page of a website. Notably, child-directed online services are strictly limited from “selling” a child’s personal information to third parties for behavioral advertising or other purposes absent parental consent. Thus, this California-specific requirement is not applicable to child-directed online services and represents another inconsistency with COPPA. More generally, our members are concerned that requiring yet another California-specific link at a company’s home page (on top of obligations to provide a link to California privacy rights and California Transparency in Supply Chains Act disclosures) is burdensome. Those burdens will become even greater if other states adopt similar state-specific requirements.

Mandating Two Modes for Consumers to Submit Access and Deletion Requests is Burdensome

Toy industry members are subject to specific obligations under COPPA to verify that an individual requesting access to a child’s personal information is a parent. 16 C.F.R. §312.6. The CCPA does not clearly limit requests to access the data of children under 13 to a parent. COPPA does not specify the specific mode or method for a parent to exercise this right, which is left to the business, thus reflecting another area where the CCPA conflicts with COPPA. The CCPA requires covered businesses to offer both a toll-free number and a web option. This will be burdensome for businesses and conflicts with the approach under COPPA.

Impact on Small Businesses

The majority of The Toy Association’s 1100 members are small businesses. While over 600 of our members have offices in California, virtually all of our members will be affected by the CCPA due to its broad scope. Section 1798.140(c) establishes that any business that meets any one of several criteria is subject to the Act. It is unclear if §1798.140(c)(1)(A), which refers to businesses with revenues of \$25 million or more, is intended to apply to businesses with that level of revenues from California operations or to total revenues. More significantly, the CCPA covers businesses that “sell,” alone or in combination, the personal information of 50,000 or more consumers, households, or devices. *See* §1798.140(c)(1)(B). Because device identifiers are defined as personal information, and “selling” includes sharing, including for ill-defined activities that fit COPPA’s definition of support for internal business operations, even if the drafters intended this threshold to apply only to California consumers, very small businesses are likely to be covered. For example, assuming that an average two-person household has a minimum of 6 devices (a computer, phone and tablet) – which, with the growth of connected devices is likely an underestimate – businesses reaching just 8,334 California households are likely to be covered by the requirements. Thus, the law will affect very small businesses indeed.

Additionally, the definition of “consumers” simply as California residents at §1798.140(g) could affect business operations that involve employees acting purely in an employee capacity. This could include employees principally handling machine to machine communications. For example, if an employee has to log into a machine to manage manufacturing operations (which would be necessary for company security and related reasons), the employee log-in appears to trigger CCPA requirements. Employee activities should be excluded from the CCPA.

Private Right of Action

Neither the preemptive COPPA framework nor the framework of preemptive federal laws governing the physical safety of toys allows for a private right of action. The CCPA creates a novel private right of action for security breaches. Moreover, the CCPA does not establish a statute of limitations for bringing such actions. The toy industry opposes a private right of action. While the right is currently limited to breaches of unencrypted sensitive information, and thus applies only to specific types of “sensitive” information defined elsewhere in California state law, we urge elimination of a private right of action.

Safe Harbors

COPPA imposes a general obligation that businesses “[e]stablish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children.” 16 C.F.R. § 312.3(e). The FTC has provided a variety of general business guides on security measures generally, and the National Institute for Standards and Technology (NIST) has issued a management framework for security that provides a flexible approach. Congress provided a framework to provide incentives for self-regulation when it enacted COPPA. 16 U.S.C. §6503. COPPA allows for establishment of safe harbor organizations. Complaints involving members of safe harbor organizations recognized by the FTC are referred to the safe harbor organization. This, rather than a private right of action, would be a better alternative to promote compliance. We urge the Attorney General to consider a process to recognize such programs. At a minimum, the Attorney General should provide examples of “reasonable security” of the covered sensitive data that would insulate companies from unnecessary litigation, recognizing that security continues to evolve and that a measure of flexibility is essential.

Other Issues

Other areas of concern exist as well.

For example, the CCPA may prevent marketers from offering loyalty programs, which is a key way in which brands build consumer relationships and affinity and offer discounts to consumers. As currently written, CCPA’s non-discrimination provision at §1798.125 appears to prohibit tiered pricing, discounts or coupons, which are commonly used to reward loyalty customers.

As noted above, in addition to concerns about the practical implications that exist with extending obligations to “households,” these definitions would appear to require a business to allow any member of a household to access information about everyone in the household. This may create a new series of privacy concerns about how to protect the rights of children, teens and adults from violations of privacy or abuse of information from other household members.

Finally, from a resource burden perspective clarity is needed around whether businesses must create individualized privacy policies for each consumer to disclose the “specific pieces of personal information the business has collected about that consumer” per §1798.110(a)(5).

Conclusion

The toy industry is second to none in its support for strong national consumer privacy and safety frameworks. We hope this submittal will assist the Attorney General as it studies the potential impact and implications of the CCPA on consumers and businesses. Please contact Ed Desmond at [REDACTED] or Jennifer Gibbons at [REDACTED] if you would like additional information on our industry's perspective.

Sincerely,

A handwritten signature in black ink, appearing to read "Steve Pasierb". The signature is fluid and cursive, with the first letter "S" being particularly large and stylized.

Steve Pasierb
President & CEO

Enclosure

ATTACHMENT A

Summary of Toy Association Comments on the California Consumer Privacy Act

CCPA Provision	Issue	Comments and Recommendations
Federal Preemption 1798.196	<p>CCPA §1798.196 states: “This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the California Constitution.”</p> <p>COPPA preempts inconsistent state law per 15 U.S.C §6502(d): “No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter [online collection of data from children under 13] that is inconsistent with the treatment of those activities or actions under this section.”</p>	<p>Some elements of the CCPA are inconsistent with COPPA, including COPPA’s definition of children as those under 13 (<i>see</i> 15 U.S.C. §6501(1)), and other definitions in the Act and rule (16 C.F.R. Part 312). Failure to align with COPPA not only creates a preemption issue, but also imposes burdens that fail to advance privacy interests. COPPA’s risk-based framework provides useful guidance on how to balance privacy risks with burdens to consumers and businesses.</p>
Sell 1798.140 (t)	<p>The “sale” of personal information is defined broadly to include selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating to another business for monetary “or other valuable consideration.” 1798.140(t)(1)</p> <p>“Selling” does not include:</p> <ul style="list-style-type: none"> • Consumer requests that the business intentionally disclose to 3d party (subject to other restrictions); • Sharing to communicate consumer opt-out; • Sharing with a service provider information necessary to perform a business purpose if service provider does not sell the personal information and, 1) business has provided notice that information is being used or shared, and 2) service provider does not further collect, sell or use personal information except as necessary to perform the business purpose; • Transfer of information as an asset that is part of a merger, acquisition, bankruptcy or other transaction, subject to conditions on third party, including bar on making material retroactive privacy policy changes. 1798.140(t)(2)(C). 	<p>While the CCPA exceptions to the definition of “sale” are useful, §1798.140(t)(2)(C) does not fully align with the exceptions from honoring deletion requests in 1798.105(d). Clarification is needed to establish that a business does not “sell” personal information when the personal information is necessary for a business, service provider, law enforcement or other authorized party to engage in activities described in 1798.105(d).</p>
Right to Request Information on Collection 1798.110	<p>Consumers have right to request that a business disclose, and a business must disclose:</p> <ul style="list-style-type: none"> • Categories of PI collected about the consumer; • Categories of sources from which the PI is collected; • Business or commercial purpose for collecting or selling PI; • Categories of third parties with whom the business shares PI; 	<p>It is important to clarify that these obligations do not require development of individual privacy policies or burdensome paperwork obligations.</p>

ATTACHMENT A

CCPA Provision	Issue	Comments and Recommendations
Right to Request Information on Sale 1798.115	<ul style="list-style-type: none"> Specific pieces of PI collected about that consumer. <p>Consumers have the right to request that a business that sells or discloses consumer PI disclose, and business must disclose:</p> <ul style="list-style-type: none"> Categories of PI that the business collected about the consumer; Categories of PI that the business sold and categories of third parties to whom PI was sold, by category and third party; Categories of PI about the consumer disclosed for a business purpose. 1798.115 (a). <p>A third party may not sell PI about a consumer that has been sold to the third party unless the consumer has received explicit notice and been given the right to opt out. 1798.115 (d).</p>	<p>“Sales” to agents and service providers should be excluded from this obligation.</p>
Right to Opt Out 1798.135	<p>Business must put link on its homepage with the words “Do Not Sell My Personal Information”:</p> <ul style="list-style-type: none"> Link must also enable a consumer to opt out of “sale” of their personal information (the Right to Opt Out) (a) (2) Consumer can instruct business not to sell their personal information to third parties at any time. (a) (4) 	<p>COPPA requires that in addition to the direct notice to the parent, an operator must post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its Web site or online service, <i>and</i>, at each area of the Web site or online service where personal information is collected from children. The link must be in close proximity to the requests for information in each such area. §312.4 (d). Operators of online services subject to COPPA – particularly those primarily directed to children – cannot “sell” information to third parties absent parental consent; they can, however, share information with service providers to support internal operations.</p> <p>The requirement for the “Do not sell ...” link at the home page is burdensome and conflicts with COPPA, which has a defined mechanism for parents to request an opportunity to access, correct or delete children’s data.</p>
Right to Deletion 1798.105	<p>Consumers can request deletion of “any personal information” the business has collected. 1798.105 (a)</p> <ul style="list-style-type: none"> Businesses must delete the requested information and direct any service providers to do the same. 1798.105 (c) Businesses do not need to delete PI if necessary to: complete a transaction; detect security incidents; protect against illegal activity. fraud, etc.; exercise free speech; comply with the CA Electronic Communications Privacy Act; engage in research in the public interest; comply with legal obligation; “enable solely 	<p>While the CCPA does not require businesses to delete PI necessary to support internal operations (as enumerated, and those should be expanded), businesses must provide information on collection and “sale” per 1798.110 and 1798.115; offer adult consumers a right to opt-out of the sale of PI per 1798.120(a), give parents of children <13 the opportunity to opt-in to the sale of PI and minors 13 – 16 the right to opt-in per 1798.120(c), subject to definitional exception of a “sale” in 1798.140(t)(2). As</p>

ATTACHMENT A

CCPA Provision	Issue	Comments and Recommendations
	internal uses that are reasonably aligned with the expectations of the consumer based on the consumer’s relationship with the business”; “otherwise use the consumer’s personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.” 1798.105 (d)	noted, definitions should align with COPPA and avoid burdening businesses with obligations to share names of agents and service providers, which are often confidential business information.
Mechanisms to honor requests 1798.130	Consumers can request a copy of all PI a business has collected. <ul style="list-style-type: none"> Business must provide at least two means for consumers to submit requests for disclosure including a toll-free telephone number and website. Businesses must provide the requested PI free of charge within 45 days of receipt of request. (a) (1), (2) 	Requiring businesses to offer both a toll-free number and a website is burdensome, especially for small businesses. Either a toll-free number or a website should suffice.
Consent; Children/Minors 1798.120 (c), (d)	Business can’t sell personal information if business knows consumer is under 16 without first obtaining affirmative consent. <ul style="list-style-type: none"> Parent or guardian must consent where consumer is under 13 years. Consumers between 13-16 must give affirmative consent. 	COPPA requires verifiable parental consent prior to collecting, using, or disclosing personal information from children, subject to a number of exceptions, including collection of persistent identifiers to support internal operations (excluding use for interest-based advertising). The CCPA’s broad definition of “personal information” and “sale” appear to require parental consent for data collection, use and sharing exempt under COPPA. Further, requiring consumers age 13 – 16 to “consent” to uses excepted from parental notice and consent obligations under COPPA where children under 13 are concerned will burden businesses without advancing privacy.
Data Breaches 1798.150	Businesses are liable if they fail to take “reasonable security measures” in relation to data covered in CA Civ. Code 17987.80 (CA sensitive data) and data breach occurs. <ul style="list-style-type: none"> Business must notify consumers, regulators of unauthorized access to unencrypted sensitive data “in the most expedient time possible and without unreasonable delay” under separate CA data breach notification law (CA Civ. Code 1798.80 <i>et seq</i>). 	COPPA requires reasonable security, and SB 327 requires security of connected products.
Enforcement and Penalties 1798.150	Consumers can bring private actions for data breaches involving nonencrypted/nonredacted PI as defined in data breach law at CA Civ. Code 1798.81.5 (generally sensitive data), and permits recovery of actual or statutory damages. Recently a proposal to amend the CCPA was introduced to expand the private right of action to any violation of the CCPA.	COPPA bars any private right of action and the Toy Association opposes a scheme of statutory damages and a private right of action. Enforcement of COPPA is the province of the FTC, and state Attorneys General have delegated authority to enforce COPPA. CCPA enforcement should be left exclusively to the Attorney General (or delegated to local District Attorneys with notice to the AG).

ATTACHMENT A

CCPA Provision	Issue	Comments and Recommendations
		Guidance should establish that businesses should have no liability for “selling” personal information (as defined in the Act) to a third party that fails to adhere to the requirements of 1798.140(t)(2).
Covered Entities 1798.140	<p>“Business”: 1798.140 (c)</p> <ul style="list-style-type: none"> • Sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit; • Annual gross revenues over \$25,000,000; • derives 50 percent or more of its annual revenues from selling consumers’ personal information; • Sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices. <p>Applies to entities that share common branding controlled by a qualifying business.</p>	Broad definitions of “personal information” and “selling” (including sharing for ill-defined activities that fit COPPA’s definition of support for internal business operations), coupled with the relatively small number of households or devices affected, very small businesses are likely to be covered. For example, assuming that an average two-person household has a minimum of 6 devices (a computer, phone and tablet) – which, with the growth of connected devices is likely an underestimate - businesses reaching just 8,334 California households are likely to be covered by the requirements.
Protected Individuals 1798.140	“Consumer”: a natural person who is a California resident. 1798.140 (g)	This broad definition, coupled with the broad definition of personal information, risks affecting machine-to-machine communications where employees must log in to operate the equipment. The requirements should be limited to consumer settings only.
Safe Harbors	The CCPA does not create a role for safe harbors.	COPPA establishes a mechanism for safe harbor organizations to be recognized. Complaints involving members of safe harbor organizations recognized by the FTC are referred to the safe harbor organization. This, rather than a private right of action, would be a better alternative to promote compliance with the CCPA. We urge the Attorney General to consider a process to recognize such programs. At a minimum, the Attorney General should provide examples of “reasonable security” of the covered sensitive data that would insulate companies from unnecessary litigation, recognizing that security continues to evolve and that a measure of flexibility is essential.

Message

From: Charisse Castagnoli [REDACTED]
Sent: 2/19/2019 4:03:11 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA
Flag: Follow up

I'm very interested in the thoughts regarding

- "the establishment of rules and procedures related to the verification of consumer requests."

One of the challenges many online companies face is that the identity is often represented by only an email address. Given the vulnerabilities in email systems, it would be not un-thinkable for unscrupulous individuals to attempt to gain access to PI by email compromise.

GDPR provides no good guidance on this issue, except that the validation requests can not be "overly burdensome".

Further any validation process may in and of itself add to the accumulation of PI. So for example if you request a copy of a DL over a secure HTTP connection, even if only used for the purposes of validation – you have now increased the amount of PI you need to manage and audit.

Finally, if all you have to connect a consumer to potential PI is an email address, it may not be possible to truly disambiguate the user. What if the email address is [REDACTED] – how would you really go about identity proofing such an email address.

Next – it would be useful to clarify the obligations of a service provider that does not have the original relationship with the consumer.

Under GDPR if you are a data processor or sub processor and you receive a subject access request – you contact the controller and ask how they want you to handle it. There should be a process for service providers – especially those who may be unable to reasonably validate identity – to pass the request back to the original data controller.

Thank you for your kind attention

Charisse Castagnoli
JD IAPP-EU, US certified

CA Bar 181478

-- Charisse Castagnoli

General Manager



Message

From: Stockburger, Peter Z. [REDACTED]
Sent: 3/8/2019 2:16:18 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Karlstad, Heather [REDACTED]
Subject: CCPA Comment - First American Title Insurance Company
Attachments: CCPA Comment - First American Title Insurance Company (3-8-19).pdf

Good afternoon,

Attached please find a comment letter on behalf of First American Title Insurance Company in relation to the California Consumer Privacy Act of 2018 and the Attorney General's Office pre-rulemaking solicitation of public participation.

Thank you,

 Peter Z. Stockburger

[REDACTED] | US Internal 38018

[Bio](#) | [Website](#)

Dentons US LLP

Hamilton Harrison & Mathews > Mardemootoo Balgobin > HPRP > Zain & Co. > Delany Law > Dinner Martin > Maclay Murray & Spens > Gallo Barrios Pickmann > Muñoz > Cardenas & Cardenas > Lopez Velarde > Rodyk > Boekel > OPF Partners > 大成

Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. This email may be confidential and protected by legal privilege. If you are not the intended recipient, disclosure, copying, distribution and use are prohibited; please notify us immediately and delete this copy from your system. Please see dentons.com for Legal Notices.

March 8, 2019

BY E-MAIL (privacyregulations@doj.ca.gov) AND U.S. MAIL

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

**Re: California Consumer Privacy Act of 2018
Pre-Rulemaking Comments / First American Title Insurance Company**

Dear Sir or Madam:

This firm represents First American Title Insurance Company ("First American"), one of the country's leading title insurance and settlement service providers. First American specializes in helping homebuyers, sellers, real estate agents, and other professionals close real estate transactions by facilitating and streamlining the process and providing comprehensive title insurance protection.

First American submits this letter to provide the California Attorney General's Office ("AGO") with insight and context as to how the California Consumer Privacy Act of 2018, as amended (Civ. Code §§ 1798.100, *et seq.*) ("CCPA"), will adversely impact title insurance companies like First American. Specifically, the CCPA, as amended, fails to adequately take into account the complexities of the title insurance business or provide companies like First American the flexibility needed to prevent and protect against fraudulent and / or criminal activity. Accordingly, and as explained in greater detail below, First American urges the AGO to adopt regulations that **interpret Civil Code § 1798.145(a)(4)** to include the right of a business to prevent and protect against fraudulent and / or criminal activity. First American submits this letter as part of the AGO's pre-rulemaking process of soliciting "broad public participation" as it works to adopt final regulations that further the purpose of the CCPA.¹

1. The AGO Has Broad Discretion To Issue Regulations Addressing First American's Concerns

The CCPA grants the AGO broad authority to adopt regulations to further the purposes of the CCPA. The AGO is specifically directed to adopt regulations that would, among other things:

- Create exceptions necessary to comply with state or federal law;
- Create "rules and procedures" for furthering a consumer's right to obtain personal information from a business, "taking into account" among other things "the burden on the business[.]"and
- Otherwise "further the purpose" of the CCPA "as necessary[.]"²

¹ Civ. Code § 1798.185(a).

² Civ. Code § 1798.185(a)(3), (7), (b).

2. The AGO Should Adopt Regulations Interpreting Civil Code § 1798.145(a)(4) To Include The Right Of A Business To Prevent And Protect Against Fraudulent And / Or Criminal Activity

The CCPA grants California residents the right to inquire about what personal information has been collected about them, with whom it has been shared, and to demand the deletion and opt-out of the sale of the same. The CCPA also imposes obligations on how businesses collect, store, sell, and process the personal information of California residents. That said, Civil Code § 1798.145(a)(4) makes clear that a business's obligations under the CCPA do not restrict its ability to, among other things, "[e]xercise or defend legal claims."

Although this exception is helpful, it does not adequately capture the entirety of legitimate business purposes for which title insurance companies like First American collect, process, and use personal information. Nor does it adequately take into account the unique nature of the title insurance business, which requires vigorous oversight and the prevention and protection against fraudulent and /or criminal activity.

For most California residents, purchasing a home is the single biggest financial investment of their lives. Ensuring clear title for those residents is therefore a matter of significant public importance. Clear title is a necessary element for any successful real estate transaction because it allows for the owner of the property to be known, the transaction to be secured, and the claims against the property to be understood and resolved. Clear title also prevents fraud by avoiding false instruments and deeds entered into the public record, which are often used to illegally encumber, convey, or sell property.

To ensure clear title in a real estate transaction, companies like First American conduct a search on titles to check for claims, liens, or other issues relating to the property. During this process, personal information, as that phrase is broadly defined under the CCPA to include insurance policy numbers and loan information, may be collected, processed, and / or shared. The current exception at Civil Code § 1798.145(a)(4) does not contemplate this function, and inadvertently imposes an undue burden on companies like First American whose services are critical to ensuring that California residents achieve their goals of home ownership without complication. Strictly read, the CCPA would significantly hamper First American from researching and completing a title search in a timely manner, thereby jeopardizing California real estate transactions for California residents.³ In short, the CCPA, as amended, does not provide companies like First American the flexibility they need to collect, retain, or use personal information to prevent acts of fraud or to protect against unlawful activity.⁴

The AGO should therefore interpret Civil Code § 1798.145(a)(4) to include the right of a business to prevent and protect against fraudulent and / or criminal activity. This interpretation directly aligns with the AGO's statutory mandate, which charges the AGO with adopting regulations that will address exceptions necessary to comply with state or federal law and that will create "rules and procedures" that further a consumer's right to obtain personal information from a business, taking into account "the burden on the business[.]"⁵ Interpreting Civil Code § 1798.145(a)(4) to include the right of a business to prevent and

³ First American completed more than 202,671 transactions on California property in 2018.

⁴ Similar comments were raised by Craig Page on behalf of the California Land Title Association at the AGO's February 5, 2019 CCPA forum held in Sacramento, California. See Feb. 5, 2019 Transcript at 61:11-64:23, available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-sac-020519.pdf>. Mr. Page noted that a fraud prevention exception is particularly necessary because title insurance companies often discover child support and tax liens, and the people who are trying to avoid paying these liens may try to obfuscate those records by exercising their rights under the CCPA. Mr. Page also noted the title insurance industry "plays a very important role" in thwarting fraud "all the time" by working with financial and federal agencies to help identify money laundering efforts, and by working closely with federal and state prosecutors on fraud cases.

⁵ Civ. Code § 1798.185(a)(1), (3), (7).

protect against fraudulent and / or criminal activity would align with these statutory goals because the prevention of and protection against fraudulent and / or criminal activity are legal obligations imposed on title insurance companies like First American,⁶ and such an interpretation would take into account the burden on title insurance companies when fielding consumer requests for disclosure, deletion, or the opt-out of a sale.

Interpreting Civil Code § 1798.145(a)(4) to include the right of a business to prevent and protect against fraudulent and / or criminal activity would also align Civil Code § 1798.145(a)(4) with the AGO's authority to "adopt additional regulations as necessary to further the purposes"⁷ of the CCPA.⁸ Specifically, such an interpretation would bring the provision in line with other provisions of the CCPA that address the right of a business to prevent and protect against fraudulent and / or criminal activity. Consumers, for example, are granted the right to request the deletion of personal information collected about the consumer by a business.⁹ Businesses may decline such a request if the personal information slated for deletion is "necessary for the business" to, among other things, "[d]etect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity."¹⁰ The phrase "business purpose" is also defined under the CCPA to include detecting "security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity."¹¹ Interpreting Civil Code § 1798.145(a)(4) to include the right of a business to prevent and protect against fraudulent and / or criminal activity would therefore align Civil Code § 1798.145(a)(4) with other provisions of the CCPA, and further the statute's purpose.

3. Conclusion

Because title insurance companies such as First American play a critical role in preventing and protecting against fraudulent and / or criminal activity, First American requests that the AGO adopt regulations that further accommodate the unique nature of the title insurance business and allow for reasonable flexibility for companies to take important measures against fraudulent and / or criminal activity in line with the existing obligations under the CCPA. Accordingly, First American requests that the AGO issue regulations that interpret Civil Code § 1798.145(a)(4) to include the right of a business to prevent and protect against fraudulent and / or criminal activity.

Sincerely,



Peter Z. Stockburger

110448903IV-2

⁶ For example, the U.S. Department of the Treasury's Financial Crimes Enforcement Network has issued Geographic Targeting Orders that require First American to collect and report information about the persons involved in certain residential real estate transactions and that impose recordkeeping requirements on First American.

⁷ Civ. Code § 1798.185(b).

⁸ Such an interpretation would also align the CCPA with other California privacy regimes, such as the Insurance Information and Privacy Protection Act (Cal. Ins. Code § 791, *et seq.*), which allows disclosure of personal information to a third party if that third party will assist in detecting and protecting against fraudulent or criminal activity. Cal. Ins. Code § 791.13(b)(2)(B).

⁹ Civ. Code § 1798.105(a).

¹⁰ *Id.* at (d)(2).

¹¹ Civ. Code § 1798.140(d)(2).

Message

From: Matt Akin [REDACTED]
Sent: 3/8/2019 12:23:42 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: John Shirikian [REDACTED]; Brad Wenger [REDACTED]; John W. Mangan [REDACTED]
[REDACTED] Patricia Thompson [REDACTED]
[REDACTED] Michael Gugig [REDACTED]
[REDACTED] Michael B. Hickey [REDACTED]
Subject: CCPA Comment Letter
Attachments: DRAFT ACLHIC-ACLI CA AG Comment Letter Final Revisions (2).pdf

Dear Attorney General Becerra:

Thank you for the opportunity to provide comments on the promulgation of regulations in furtherance of the California Consumer Privacy Act of 2018.

Attached please find joint comments from the American Council of Life Insurers (ACLI) and the Association of California Life and Health Insurance Companies (ACLHIC).

Our organizations look forward to working with you and your staff.

Should you have any questions, please do not hesitate to contact the ACLHIC office at the number listed below.

Sincerely,

Matt Akin

Legislative and Communications Associate
ACLHIC
1201 K Street, Suite 1820
Sacramento, CA 95814
[REDACTED]

FX: [REDACTED]
Website: www.aclhic.com



The Honorable Xavier Becerra
Attorney General
California Department of Justice
300 S. Spring St.
Los Angeles, California 90013
ATTN: Privacy Regulations Coordinator

Re: California Consumer Privacy Act of 2018

Dear Attorney General Becerra:

Thank you for the opportunity to provide comments on the promulgation of regulations in furtherance of the California Consumer Privacy Act of 2018 ("CCPA"). The Association of California Life & Health Insurance Companies ("ACLHIC") and the American Council of Life Insurers ("ACLI") look forward to discussing the fundamental importance of privacy and security to our industry and our customers.

Life insurers provide important services to Californians, helping to protect their financial security through life insurance and annuity products. In addition, life insurers make major contributions to the California economy and the financial confidence of Californians. There are 417 life insurers licensed to do business in California and they generate more than 225,000 direct and indirect jobs in the state. California residents have \$3.7 trillion in total life insurance coverage. California residents own 10 million individual life insurance policies, with coverage averaging \$244,000 per policyholder. In 2016, \$38 billion was paid to California residents in the form of death benefits, matured endowments, policy dividends, surrender values, and other payments, with \$8 billion in annuity benefits paid in the state in the same year.

In the wake of the highly publicized data privacy scandals in the technology sector, it made sense for public policymakers to adopt the CCPA. The new law is designed to regulate the collection and use of consumer's private personal information. It is important to note that life insurers have remained strongly committed to properly using and protecting the personal information of our consumers for over two centuries.

Life Insurer Obligations to Protect Privacy and Security of Consumer Information

Life insurers have long been the diligent stewards of consumers highly sensitive medical and financial personal information and life insurers take seriously the obligation to maintain the security, confidentiality and integrity of the information entrusted to them.

Life insurers collect and use personal information to perform essential life insurance business functions. For example, to underwrite applications for life, annuity contracts, disability income, and long-term care insurance policies; and to pay claims and administer benefits submitted under these policies.

At the same time, our industry is required to implement and maintain compliance with various federal and state laws and regulations that provide an established, increasingly complex, broad and

rigorous regulatory framework that require life insurers to protect both the privacy and the security of consumers' personal information.

Promulgation of CCPA Regulations

There are four specific areas we believe you should consider in development of the regulations: 1) timing of notification; 2) exclusion of employee/agent information; 3) the parameters of a verifiable request; and, 4) implementation dates.

Timing of Notification

Operationalizing the requirement to provide notice "at or before the time of collection" is not practically feasible (Section 1798.100[b]). A primary concern is with providing 'at or before notice' to future prospects and other non-applicants, which include a wide range of individuals. Companies currently provide notice to applicants and policyholders because they have contact information enabling them to interact. This is in compliance with current California insurance law. In this instance, applicants provide the majority of personal information directly to the company and, therefore, companies are able to provide the notice when first contact is initiated. For future prospects and non-applicants, companies do not have the same interaction points and interaction capabilities. Therefore, we recommend applying a flexible, risk-based approach to the manner in which notice is provided to individuals. For example, depending on the circumstances and the nature of the personal information collected, providing notice on a website may be a sufficient means of providing notice "at or before the time of collection". Adopting a flexible approach to notice will avoid burdening consumers with multiple formal notices that are not useful and avoid an unnecessary and costly burden to organizations.

Exclusion of Employee/Agent/Vendor Information from the Scope

Clarification should be included in any regulations promulgated to clarify that employee information, including prospective employees, should not be included as personal information. The CCPA can be read to reasonably conclude that personal information of certain "non-consumer(s)" such as employees, vendors, and agents (both current and potential), are ordinarily not considered consumers. Therefore, employee data, distribution channels, and vendor information should not be included under the strictures of the promulgated regulations.

Verifiable Consumer Request

The phrase "verifiable consumer request" in §1798.130(a)(3) is ambiguous and causes significant confusion. In order to establish clarity around the disclosure of information, we would respectfully suggest that the Attorney General adopt the guidance already in place in CA Ins. §791.08 which requires an individual to provide proper identification when submitting a request for recorded personal information.

Implementation Dates

And, finally, we believe that the law should be applied on a prospective basis. The obligation to disclose for the prior 12 months should be interpreted to apply to July 1, 2020; and should be limited to mean that the capability must exist on that date, such that compliant disclosures will not include a full 12 months history until July 1, 2021.

Need for Careful and Thoughtful Consideration

We believe that California's current insurance laws are comprehensive and effective at protecting the privacy and security of the personal information of insurance consumers. Yet we are sensitive to the concern that new and evolving technology are creating new privacy and security challenges. We must give thoughtful consideration to how any new privacy or security law will affect consumer access to the financial security products that life insurers offer.

Need for Harmony between CCPA and Existing California & Federal Insurance Privacy Requirements

A framework of differing, duplicative or conflicting new rules could jeopardize life insurers' ability to effectively and efficiently protect the privacy and security of their customers' personal information. Life insurers' privacy protocols and security systems generally are the same throughout their company operations across the country.

Any new privacy and security rules intended to be applicable to life insurers must be harmonized with existing California insurance privacy requirements. This will ensure level consumer protection and will avoid subjecting life insurance companies and other insurance licensees to administrative burdens and costs associated with implementing and maintaining differing degrees of compliance programs and mechanisms to comply with the various laws which may work counter to the best privacy and security protection for consumers.

Without uniformity and consistency with existing laws for certain regulated sectors, the CCPA not only will conflict with existing law, but may also fail to reflect the critical balance and policy objectives achieved by current privacy and security laws applicable to and strongly supported by life insurers.

Key California Laws Applicable to Life Insurers

California consumers are protected by a host of privacy and security laws and regulations in California in their engagement with Life Insurers:

- the Insurance Information and Privacy Protection Act (CA Ins. Sec. 791);
- the Confidentiality of Medical Information Regulation (CA Civ. Code Sec. 56);
- the California Financial Information Privacy Protection Act (CA Fin. Code Sec. 4050); and,
- the Privacy and Standards for Safeguarding Nonpublic Personal Information (CA Admin. Code tit. 10 Sec. 2689).

These existing regulations currently applicable to insurers' use of consumer personal information which reflect a critically important balance between consumers' legitimate privacy concerns and life insurers' need to appropriately use personal information to serve their existing and prospective customers expectations.

The proliferation of new technologies has heightened awareness surrounding the collection, use and disclosure of personal data in some sectors. However, the insurance industry has been subject to a robust regimen for protecting the privacy and security of consumer and customer personal information. Many of the consumer protections in the CCPA and other recent privacy proposals are common insurance industry practices, but the concern is that inconsistency of terms and lack of uniformity may create inefficiencies, negatively impact innovation, create overly burdensome compliance operational efforts, with no apparent additional benefit to consumers.

Key Federal Privacy Laws Applicable to Life Insurers

In addition to the privacy requirements under California's insurance privacy laws and regulations, there are several significant federal laws that govern insurers' information practices, most notably: (i) the Gramm-Leach-Bliley Act, (ii) the federal Fair Credit Reporting Act, and (iii) the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

This combination of federal and state privacy laws and associated regulations provides the basis for a regulatory framework that imposes comprehensive requirements on life insurers to protect the confidentiality and security of their customers' personal information.

At the same time, these laws reflect federal and state lawmakers' recognition that life insurers must use and sometimes responsibly share personal information to perform fundamental and legitimate

insurance business functions and to serve their customers in the most efficient, cost-effective manner possible.

California Financial Information Privacy Protection Act & the Insurance Information and Privacy Protection Act

California's current statutory and regulatory framework set standards for the privacy of consumer personal information by ensuring that Californians can control the disclosure of their personal information and intentionally goes beyond federal law (i.e., the GLBA). Both our organizations actively participated in the development of this law.

Thus, we are hopeful that as your office considers the promulgation of these important and complex regulations, you continue to keep in mind:

- life insurers' unique need to use consumers' personal information to perform fundamental insurance business functions;
- the complexity of the privacy/security framework to which life insurers are subject; and
- the need for harmony across California's regulatory platforms so that life insurers' can continue to effectively and efficiently protect the privacy and security of their customers' personal information.

Again, thank you for the opportunity to comment on this important rule making process. We are glad to answer any questions.



Brad Wenger
President and CEO
ACLHIC



John Mangan
Regional Vice President, State Relations
ACLI

cc: Honorable Ricardo Lara, California Insurance Commissioner

Message

From: Aaron Brown [REDACTED]
Sent: 3/7/2019 8:02:39 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA comment

The state of Washington recently introduced proposed privacy legislation. The act in Washington state specically excludes independent contractors and employees.

We would like to see a similar carve-out under a CCPA amendment.

Consider the gap in coverage that has been created... A small company need not observe CCPA protections/obligations as it relates to its employees. However, larger organizations must adhere to the requirements. The question is why protect one set of employees and not the other?

Employee and independent contractors have the opportunity to negotiate terms with an employer or company in a manner that Consumer cannot. The protections provided by CCPA are very important but should be narrowly applied to those not in a position to protect their own information from companies who operate in the dark.

Message

From: edward murphree [REDACTED]
Sent: 3/8/2019 11:47:27 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA Comments
Attachments: CCPA AG Commentary 2019.pdf

Sir or Madam

Please see our comments attached for your reference and consideration.

Respectfully

Edward Murphree

John Paul Tomaszewski &
Edward Murphree (jointly)



CA Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Sprint St.
Los Angeles, CA 90013

RE: Commentary and Recommendations regarding the California Consumer Privacy Act of 2018

Sir or Madam:

We are writing in response to your invitation for public participation in the rule making process mandated through the passage of the California Consumer Privacy Act of 2018. Our commentary and recommendations below are in response to what we feel are the most important items to address for your review and consideration.

1. We recommend the following approach to successfully balance advancement of consumer privacy and protection innovation:

- a. Promulgate Rules and Regulations which are:
 - i. Technology Neutral
 - ii. Risk and context sensitive
 - iii. Outcome-oriented
 - iv. Interoperable with other systems
 - v. Effective in reducing administrative burdens for organizational compliance
- b. Adherence to subsection 'a' will support the outcomes necessary to achieve this balance:
 - i. Enhancing trust in the information ecosystem

- ii. Scalability
- iii. Supporting innovation

Establishing and maintaining trust between CA Consumers and the impacted Business community is the end state goal of the Act. The exercise of consumer rights to privacy and business responsibilities are the mechanisms with which to achieve that goal. Implementing effective regulations, rules and procedures are critical to achieving this goal.

2. **Foreword .** The California Consumer Privacy Act authorizes the Attorney General to adopt additional regulations *as necessary to further the purposes of this title*. There are no express limitations on this statement, providing the Attorney General wide latitude to set the tenor and scope of the Act’s regulatory effect. We urge the Attorney General to set the bar high, but no so high as to fail its primary objective of establishing the baseline of trust. A high bar means establishment of clear regulations, rules and procedures with which parties may rely. These regulations must be fair and reasonable, recognizing that personal data has become integral part of business process. Balance must be made between competing interests and consideration given to the various parties’ perspectives, issues and concerns, and importantly, written in such a way that interested parties will comply with it - in particular businesses. Additionally, the more thoughtful and detailed the regulation, the easier it will be for your office to enforce it.

3. **Specific Recommendations.**

- a. **Consumer** - the Act defines this as “a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, *however identified*, including by any unique identifier.

- i. **Issues:**

‘Consumer’ is broadly defined and can include employees.

Consumer is commonly defined as “Individual who purchases, uses, maintains, and disposes of products and services.” Note that under this common definition, the individual must *perform actions* in relation to products and services. The Act, by contrast, defines Consumer in relation to ‘residence’ - itself, linked to a threshold obligation to pay taxes in California. A ‘resident’ of California is a Consumer under the Act.

The problem: ‘Consumer’ is sufficiently broad enough to include employees. Employees don’t stop being consumers when they are working and will have the rights to their personal data in an employment or human resources context.

To solve this problem, we recommend that the Office of the Attorney General clarify that the Act establishes a general foundational privacy regulation for Consumers in relation to their personal information outside an employment purpose, but is inapplicable to personal information in an employment or post-

employment setting. This clarification will require an impacted business to identify the purpose of the personal information.

The law itself somewhat reflects this in the way it defines “business”. The definition of business seems to recognize that employees are not exactly within the scope of the law. Additionally, we further recommend the Office of the Attorney General provide explanation and examples for the public. This wouldn’t necessarily be a heavy lift as a broad definition of what constitutes non-employment information with examples may suffice.

- b. **Personal Information** - the Act defines Personal Information very broadly - and includes a list of descriptors that will identify, or are capable of being associated with, or could reasonably be linked, with a consumer or household. So, confirming identification of, or association or reasonable linkage to a consumer as well as a household is sufficient to constitute Personal Information.

- i. **Issues**

- 1. The expansive definition is daunting from a business compliance perspective. In particular, the inclusion of information that is capable of association with and reasonably could be linked to a consumer, itself now including household and device, make compliance challenging. The burden on business should be reasonable and not overly burdensome. We recommend, first, to trigger the Act, personal information must be reasonably linked to a particular consumer, and personal information linked to a household only include personal information reasonably linked to that consumer. Without restricting what may be accessed, an access request could be used to infringe privacy as opposed to protecting it, say, for example where it is used to acquire information from the household, but not regarding the consumer requesting it.

- c. **Business** - the Act applies to businesses processing consumer personal information. Business is defined very broadly.

- i. **Issues**

- 1. The Act applies to a for-profit legal entity that collects information (or on behalf of which information is collected), determines the purpose and means of processing of a consumer’s personal information, that does business in California AND satisfies one of three thresholds.
 - 2. ‘*Doing business.*’ One important area to clarify is the extent to which an organization would be considered to be *doing business* in the State of California. Under Section 1798.175 of the Act, it can be inferred that a business would not necessarily have to be physically located in California for the Act to apply. Application

includes information collected electronically or over the internet. Given the nature of the internet as being borderless, regulation over it triggers US Constitutional issues - in particular, the dormant Commerce Clause. Existing language in the Act attempts to address the constitutional issues of regulation of interstate commerce. We also note that there is a severability clause included in the Act. A law is presumed to be Constitutional; however, there is a significant enough risk to recommend preparing for such a challenge.

3. *'Thresholds.'*

- a. One of these definitional thresholds is 'has annual gross revenues in excess of \$25 million.' Will gross revenues of the entire business be included even if they did not result from business in CA? Here, clarification is necessary because even if only one CA Consumer's personal information is processed, this threshold could be met if gross revenues are included outside CA, thereby bringing that organization under the Act's expansive definition of business. **To solve this problem**, we recommend that the CA AG clarify that the revenues in question mean gross revenues generated from 'doing business' in CA rather than en total. This means establishing a means with which revenue can be identified as arising out of CA - such as with tax.
- b. Another definitional threshold states 'Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.' We understand the intent behind this was to address the myriad instances in which personal data can be collected and/or further processed. However, this threshold number can be met quite easily with the allowable aggregation of personal information through expanded actions. Further, one organization may receive duplicative personal information from myriad devices. Will all the personal information an organization receives count from myriad devices count? Further, household is included in the count, but is not defined under the Act. This has the effect of expanding the definition of consumer from one sole 'resident,' to potentially many people who are part of that household. Further, a consumer could conceivably request access of the consumer's personal information it has collected and receive information that impacts the privacy of other people making up the household. There is a potential for abuse here, especially in a legal proceeding. Without clear

guidance as to when and how this threshold applies, it could apply to many organizations that, but for this provision, would not have to comply and add an additional burden to the CA Attorney General's office in enforcement. **To solve this problem**, we recommend that the CA AG 1) define household narrowly so consumer personal information from the household, to be counted, must be clearly linked to that consumer themselves - . 2) clarify that duplicate records from multiple devices do not count.

d. Opt-Out involving the Sale of Personal Information.

- i. **Issue** This provision requires an impacted business to notify the Consumer of a sale of their personal information to a 3rd party and obliges that business to acquiesce to the Consumer's right to opt-out of that sale. For businesses offering free use of services to the user (but generating revenues off that user's personal information via online behavioral or interest based advertising), this could significantly impact their source of revenue if the use of that personal information constitutes a sale. As currently written, *Sale* includes the exchange of *valuable consideration*.
To solve this problem, we recommend that the CA AG clarify that this does not constitute a sale.
- ii. **Issue.** The Act disallows discrimination in relation to the exercise of a Consumer's rights, but allows an exception in the form of a different price, rate, level or quality of service to a Consumer who has exercised the opt-out provided that such difference is directly related to the value of the Consumer's data. Such financial incentive must **not** be unjust, unreasonable, coercive, or usurious. These broad statements do not provide explanation or examples of reasonable financial incentives for a business to follow. Under the Act, the AG must establish rules to govern business compliance with the Consumer's opt-out request. **To solve this problem**, we recommend that the CA AG establish guidance that reasonable financial incentives means one of three things: 1) the business charges a lower price and provides the same quality of goods or services; 2) a business charges a lower price and a higher quality of goods or services; or 3) charges the same price and provides a higher quality of goods or services.
- e. **Verifiable Consumer Request.** Under the Act, the Attorney General is required to assist in furthering the purposes of Sections 1798.110 and 1798.115 and to facilitate the consumer's ability to obtain information and reduce the overall burden on the business to comply with these requests by establishing rules and procedures pertaining to a business's ability to reasonably verify the consumer's identity.

- i. **Issue:** In order to verify the identity of a Consumer in furtherance of their exercise of privacy rights under this Act, companies would have to collect identifying data in order to authenticate the user. **As a starting point to solving this issue**, we recommend that the AG review the consumer identification procedures listed in the Fair Credit Reporting Act. See <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act>.
- ii. **Issue:** A business is required to respond to a request with *specific pieces of information*, an undefined term within the Act. Without guidance as to what is meant, businesses will have to define for themselves what this covers and disclose within the required time period. A procedure supported by the Attorney General to assist in the identification of consumers is strongly recommended.
- iii. **Issue.** The Act applies to both paper and digital personal information. The Act heavily emphasizes Attorney General and impacted business requirements in regards to digital personal information to the detriment of non-digital personal information. **To solve this problem**, Attorney General obligations under Section 1798.185 must include establishment of rules, procedures and exceptions necessary to ensure that notices and information that businesses are required to provide address paper personal information - including procedures dedicated to the exercise of consumer rights outside the internet.
- f. **Security.** The Act provides a narrow private cause of action for the breach of the duty to implement and maintain reasonable security procedures and practices. Yet, the Act as well as the CA data breach regulations under the CA Civil Code do not address what constitutes reasonable security procedures and practices. **To solve this problem**, we strongly recommend that the Office of the Attorney General establishes a minimum cybersecurity standard an organization must comply with to be in compliance. Our recommendation is that the NIST cybersecurity framework be adopted as that minimum standard. See <https://www.nist.gov/industry-impacts/cybersecurity> for more information.

2. Text of the Act Requiring Correction.

- a. **Business Duty to Disclose.** Business duty to disclose and deliver is 45 days from receipt of the verifiable consumer request. Time taken to verify does not extend the 45 day period. This period may be extended an additional 45 days when reasonably necessary if consumer provided notice within the 1st 45 days. Disclosure is for the prior 12 month period delivered in writing.
 - i. **Issue:** The above text contradicts Section 1798.145(g)(1) which extends a business's response time by up to 90 additional days (as opposed to 45 days) where necessary, taking into consideration the complexity and number of requests as well as mandating reasons for the delay. Further,

Section 1798.145 provides procedures should the business not take action or determine the request is manifestly unfounded or excessive which are **not** found in Section 1798.130. **To solve this problem**, this will require correction, likely through Amendment. In the interim, we recommend that Section 1798.145(g)(1), as the more specific provision, be followed through rule of statutory construction that specific controls over general text until such a correction can be made.

b. Section 1798.130 Business Obligations

- i. **Notice.** Business is required to provide notice of business practice by placing the following information in (1) its online privacy policy(ies) if they exist, (if they don't exist, then on its Internet Web site AND in (2) CA-specific description of consumers' privacy rights by posting the following information (and updating it at least once every 12 months):
 1. A description of Consumer's rights pursuant to Sections 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.
 2. Lists of categories of PI the business has collected, sold or disclosed about a consumer for a business purpose as specifically detailed in the Act.
- ii. **Issue:** Section 1798.105(b) details the business's duty to disclose *pursuant to 1798.130*, the Consumer's rights to request deletion of Consumer's PI. Section 1798.130(a) requires the business to designate 2 or more methods for submitting requests. This will require clarification or harmonization with subsection 1 above, which only requires 1 designated method.

Message

From: PJ Hoffman [REDACTED]
Sent: 1/23/2019 6:19:14 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA Comments - Electronic Transactions Association
Attachments: ETA Comments - Privacy - AG Open Forum Comments.pdf

Dear Attorney General Becerra:

On behalf of the Electronic Transactions Association ("ETA"), we appreciate the opportunity to comment on the California Consumer Privacy Act of 2018 ("CCPA"). The payments industry makes dedicated efforts to use innovation to fight fraud and ensure that consumers have access to safe, convenient, and affordable payment services. ETA and its members strongly support privacy laws that allow companies to implement innovative tools to protect consumer privacy and data while fighting fraud. **ETA requests that policymakers consider strengthening the fraud prevention components of the CCPA and provide for an express exception for use of data for purposes of fraud prevention.**

ETA is the leading trade association for the payments industry, representing over 500 payments and financial technology ("FinTech") companies that offer electronic transaction processing products and services and commercial loans, primarily to small businesses. During 2018 in North America alone, ETA members processed over \$7 trillion in consumer purchases. ETA members include financial institutions, payment processors, FinTech companies, and all other parts of the payments ecosystem. ETA has offices in San Francisco, CA and Washington, DC.

Thank you for the opportunity to participate in the discussion on this important issue. If you have any additional questions, you can contact me or ETA Senior Vice President, Scott Talbott at [REDACTED]

PJ Hoffman

Director of Regulatory Affairs

Electronic Transactions Association

[REDACTED] Direct



January 23, 2019

Attorney General Xavier Becerra
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013.

**RE: Strengthening Fraud Prevention Under the California Consumer Privacy Act
of 2018 (“CCPA”)**

Dear Attorney General Becerra:

On behalf of the Electronic Transactions Association (“ETA”), we appreciate the opportunity to comment on the California Consumer Privacy Act of 2018 (“CCPA”). The payments industry makes dedicated efforts to use innovation to fight fraud and ensure that consumers have access to safe, convenient, and affordable payment services. ETA and its members strongly support privacy laws that allow companies to implement innovative tools to protect consumer privacy and data while fighting fraud. ETA requests that policymakers consider strengthening the fraud prevention components of the CCPA and provide for an express exception for use of data for purposes of fraud prevention.

ETA is the leading trade association for the payments industry, representing over 500 payments and financial technology (“FinTech”) companies that offer electronic transaction processing products and services and commercial loans, primarily to small businesses. During 2018 in North America alone, ETA members processed over \$7 trillion in consumer purchases. ETA members include financial institutions, payment processors, FinTech companies, and all other parts of the payments ecosystem.

Executive Summary

ETA and its members support U.S. and international efforts to strengthen privacy laws to not only help industry combat fraud and but also disclose to consumers how their data is being used. As lawmakers and regulators explore additional ways to protect consumers, it is critical that government coordinate with the payments industry so that companies can continue to combat fraud and cybercrime and ensure consumers have access to safe, convenient, and affordable payment options and other financial services.

There are numerous existing consumer protection laws in the U.S. and around the globe that address data security and privacy, and which align with the payments industry’s fraud fighting efforts. In the U.S., for example, financial information data is governed by federal laws, including the Gramm-Leach-Bliley Act and related Federal Trade Commission’s Safeguards Rule and Consumer Financial Protection Bureau’s Privacy Rule, as well as robust self-regulatory programs like the Payment Card Industry Data Security Standard, which sets forth requirements designed to

ensure companies that process, store, or transmit credit card information maintain a secure environment for such data. All of these laws and self-regulatory efforts recognize the critical role played by industry in combatting fraud, and they include provisions that allow for the targeted use and sharing of information by financial institutions and payments companies to protect consumers and to prevent fraud from occurring in the first instance.

Moving forward, ETA encourages policymakers to consider ways that law enforcement and industry stakeholders can continue to work together to develop new ways to combat rapidly evolving and increasingly sophisticated fraud and cybercrime. Working together, lawmakers, regulators, and the payments industry have kept the rate of fraud on payment systems at remarkably low levels. By continuing to collaborate, government and industry can provide consumers with access to safe and reliable payment services. Additionally, as different states and the federal government consider this important issue, it is important for policymakers to work together across state-lines to provide a consistent privacy framework without creating a patchwork of conflicting regulations.

The Role of the Payments Industry in Fighting Fraud

The payments industry is committed to providing consumers and merchants with a safe, reliable, and modern payments system. Indeed, consumers continue to choose electronic payments over cash and checks because of the protections afforded by electronic payments. These protections include, for example, zero liability for fraudulent charges, making electronic payments the safest and most reliable way to pay.

When it comes to credit cards, for example, a consumer can submit a chargeback request to his or her card issuing bank disputing a particular transaction. This process protects consumers and ensures that the financial institution bears ultimate responsibility for fraudulent transactions, demonstrating the industry's strong interest in making sure fraudulent actors do not gain access to payment systems.

In addition, the payments industry has a long history of fighting fraud through robust underwriting and monitoring policies and procedures, and the use of advanced authentication technologies. With the benefit of decades of expertise, ETA members have developed effective due diligence programs to prevent fraudulent actors from accessing payment systems, monitor the use of those systems, and terminate access for network participants that engage in fraud. Working with its members and industry and government stakeholders, ETA has published various guidelines that provide underwriting and diligence best practices for merchant and risk underwriting, including the "Guidelines on Merchant and ISO Underwriting and Risk Monitoring" and "Payment Facilitator Guidelines," which provide information on anti-fraud tools, security, and related issues.

When it comes to card data protection, the payments industry took the lead in developing the Payment Card Industry Data Security Standard ("PCI-DSS") to ensure the safety of cardholder data. The PCI-DSS sets forth requirements designed to ensure companies that process, store, or transmit credit card information maintain a secure environment for such data. In addition, the PCI-

DSS establishes a framework for implementation of those data security standards, such as assessment and scanning qualifications for covered entities, self-assessment questionnaires, training and education, and product certification programs.

ETA members are constantly developing and deploying new technology and tools to detect, deter, and eliminate fraud. Just a few examples of these efforts include the following:

- **Data Encryption.** The payments industry has introduced point-to-point encryption (P2PE) and the tokenization of data to minimize or eliminate the exposure of unencrypted data in connection with a purchase.
- **Improved Authentication.** The use of new authentication methods to verify and authenticate transactions helps minimize potentially fraudulent transactions. These new tools include the use of the following types of advanced tools:
 - biometric authentication, including the use of thumbprints, facial, and voice recognition
 - geolocation that compares the merchant's location with the location of the consumers phone
 - behavioral biometrics (e.g., monitoring keystrokes)
- **Fraud Scoring / Suspicious Activity Monitoring.** The payments industry continues to refine tools for monitoring and analyzing payment data for suspicious activity. With improvements in machine learning and artificial intelligence, the payments industry gains additional tools for identifying suspicious patterns in transaction data.
- **Chip Cards and EMV.** The payments industry has worked to replace magnetic stripes for credit and debit cards with a computer chip card, also called EMV. Chip cards make our payments system stronger by protecting against theft, counterfeit cards, and unauthorized use of cards in stores.

These are just some of the tools that the payments industry has developed in recent years to fight fraud, protect consumers, and ensure the integrity of the payments ecosystem. These efforts have been remarkably successful in reducing fraud while ensuring that consumers have access to fast, reliable, and safe payment options.

ETA Supports a Regulatory Framework that Recognizes the Efforts of Industry to Fight Fraud and Protect Privacy

ETA and its members support U.S and international regulatory efforts that encourage and respect industry efforts to combat fraud and disclose to consumers how their personal information is being used. Working together, lawmakers, regulators, and the payments industry have had remarkable success in protecting consumers and providing them with access to safe and convenient payment systems. This is achievable because the existing legal framework for protecting consumer privacy recognizes the important role of industry efforts in preventing and fighting fraud.

In the U.S., for example, laws have been passed to protect health information (HIPAA) and financial information (Gramm-Leach-Bliley Act and Fair Credit Reporting Act), and marketing activities are regulated through federal and state competition laws, as well as industry and activity specific laws, such as the Telephone Consumer Protection Act, Telemarketing Sales Rule, and CAN-SPAM regulations. These laws recognize the important role that industry plays in combatting fraud and provide provisions that allow for the targeted use and sharing of data to protect consumers and to prevent actual or potential fraud from occurring in the first instance.

Just a few of these U.S. laws include:

Consumer Protection Laws and Provisions Related to Industry Fighting Fraud
Gramm Leach Bliley Act ("GLBA"): The GLBA requires financial institutions to explain their information-sharing practices to customers and safeguard sensitive data. The GLBA has an exception to its information-sharing restrictions for information disclosed to "protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability." ¹
Bank Secrecy Act ("BSA"): The BSA establishes various requirements for covered financial institutions to assist the government in identifying and combatting money laundering and terrorist finance. The BSA includes numerous provisions governing the sharing of information between covered financial institutions and law enforcement, as well as sharing of information between financial institutions in order to identify and report activities that may involve terrorist activity or money laundering.
Health Insurance Portability and Accountability Act of 1996 ("HIPAA"): This law provides data privacy and security provisions for safeguarding medical information. Under the HIPAA Privacy Rule, a covered entity can disclose protected health information to detect fraud, abuse, or compliance violations.
California Financial Information Privacy Act ("CFIPA"): The CFIPA governs financial institutions in California handling nonpublic personal information of the State's residents, including provisions related to consumer notice and the sharing of this personal information. The CFIPA creates an exception to its restrictions to allow sharing of consumer information with nonaffiliated third parties "to protect against or prevent actual or potential fraud, identity theft, unauthorized transactions, claims, or other liability." ²
Federal Trade Commission ("FTC") Act: Section 5 of the FTC Act prohibits unfair or deceptive business acts or practices, including those relating to privacy and data security. The FTC has recognized the need for industry to share information in order to fight fraud. In a 2012 privacy report, the FTC identified "fraud prevention" as a category "of data practices that

¹ 12 C.F.R. § 1016.15(a).

² Cal. Fin. Code § 4056. While the CCPA does not contain an express fraud prevention exception from the substantive rights and protections in the law, for purposes of the opt-out requirement for the sale of a consumer's personal information, there is an argument that a business's disclosure of personal information to prevent fraud affecting the consumer would not amount to the "sale" of such information because the information is not being disclosed "for monetary or other valuable consideration." As discussed further in this letter, such language should indeed be clarified in the CCPA to preserve this vital consumer protection.

Consumer Protection Laws and Provisions Related to Industry Fighting Fraud

companies can engage in without offering consumer choice" because they are "sufficiently accepted or necessary for public policy reasons."³

The Fair Credit Reporting Act ("FCRA"): The FCRA establishes a framework for the use and sharing of consumer reports and requires covered entities to develop and implement an identity theft prevention program. While not an explicit exemption, it has traditionally been understood that consumer information disclosed for the purposes of fraud prevention is not "consumer report information" subject to the restrictions of the FCRA.⁴

Telephone Consumer Protection Act ("TCPA"): The TCPA was designed to safeguard consumer privacy by regulating telemarketing using voice calls, text messaging, and faxes. In 2015, the Federal Communications Commission exempted from the TCPA calls from financial institutions intended to prevent fraudulent transactions, identity theft, or data breaches.⁵

Likewise, the legal frameworks in Europe and Canada respect the need for industry to share personal information in order to protect consumers from fraud. In Europe, the recently enacted General Data Protection Regulation (GDPR) recognizes the important role that industry plays in fighting fraud and expressly permits (a) "processing of personal data strictly necessary for the purposes of preventing fraud,"⁶ and (b) decision-making based on profiling that is used for fraud monitoring and prevention consistent with law. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) allows for the sharing of personal information without consent if it is "made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud. . . ."⁷

As lawmakers and regulators continue to explore new ways to protect consumers, ETA and its members encourage them to collaborate with industry to ensure that new laws and regulations are appropriately tailored to address specific needs – this ensures a balance between protecting consumers and allowing industry room to innovate and develop new and beneficial security practices and fraud detection and mitigation tools.

³FTC, Protecting Consumer Privacy in an Era of Rapid Change, available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> at 36 (2012); see also id. at 39 (reaffirming this preliminary conclusion following review of public comments).

⁴ This view was supported by the court's decision in *Kidd v. Thomson Reuters Corp.*, 299 F. Supp. 3d 400 (S.D.N.Y. 2017), which concluded that Thomson Reuters was not a "consumer reporting agency" by virtue of a service that disclosed information to customers for fraud prevention purposes.

⁵ See *In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 et al.* <<https://www.fcc.gov/document/tcpa-omnibus-declaratory-ruling-and-order>>., CG Docket No. 02-278, July 10, 2015 at ¶ 129.

⁶ European Union, GDPR, Recital 47.

⁷ PIPEDA, Available at <https://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/118084/sc-2000-c-5.html>.

Conclusion

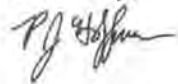
The payments industry never rests. We work tirelessly to fight fraud and protect consumers, including by developing new tools and solutions to prevent, identify and fight fraud by analyzing data. Privacy laws, such as the CCPA, should recognize these goals and the important role the payments industry plays in combatting fraud. By working together, lawmakers, regulators, and industry can protect consumers while providing them with access to the safest and most convenient payments system in the world.

* * *

Thank you for the opportunity to participate in the discussion on this important issue. If you have any additional questions, you can contact me or ETA Senior Vice President, Scott Talbott at



Sincerely,



PJ Hoffman
Director of Regulatory Affairs
Electronic Transactions Association



Message

From: Jennifer R [REDACTED]
Sent: 3/8/2019 5:09:40 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA comments

Dear Attorney General Becerra;

I am a technologist experienced in data retention, cybersecurity and regulatory compliance. One of my former employers banned social media use, even on our own time or devices. I never asked why, but now I understand the impetus. All of this scraping is not just a threat to consumers. Consumers are a conduit for state sponsored hacking and B2B intelligence gathering. Our economy and national security are at risk.

I want to express gratitude for undertaking this monumental effort. While a regulation of this scope needs to remain flexible enough to address various industry sectors, my comments should pertain to all.

For ease in navigation, the subject matter I address includes:

- a. [Data Residency](#)
- b. [Data Dictionary](#)
- c. [Record Owner](#)
- d. [Snapping Data](#)
- e. [Retention Schedule](#)
- f. [Storage Limitations](#)
- g. [Forensics](#)
- h. [Contractors](#)
- i. [Certification](#)
- j. [Document Properties](#)
- k. [Unencrypted Messages](#)
- l. [CCPA Portals](#)
- m. [Disclosure](#)
- n. [Breach Definition](#)
- o. [Universal Consent](#)
- p. [Data Protection Officer](#)
- q. [Cookies and Tracking Technology](#)
- r. [Surveillance is Stalking](#)
- s. [Employees](#)

1. **DATA RESIDENCY:** Data privacy regulations rely upon discovery and enforcement. Therefore, CCPA needs to emulate the EU and their data residency and sovereignty laws. At the very least US consumers and business should always have a choice before our data is sent abroad where the US legal system has no jurisdiction. If CCPA passes without this, then personal data may be intentionally offshored to avoid oversight. None of the

data breaches that occur offshore are ever solved due to this reason. Many of the countries where our data resides have no data protection laws. In December, 2018 the UK announced that they will review Privacy Shield and may enforce their data residency laws after Brexit.

2. **DATA DICTIONARY:** Enforcement also hinges upon the data definition being unambiguous. When systems lack a common data dictionary this impedes interoperability and electronic data transfer. Electronic health records shortfall is that it lacks semantic interoperability. US consumers cannot electronically transfer our medical records to new providers. Whereas, the financial services industry has a global data dictionary that provides interoperability. <https://www.iso20022.org/>. Semantic interoperability will provide transferability, audits, forensics and also enable technology vendors to create products for protection, such as automated encryption.
3. **RECORD OWNER:** Data breach forensics will benefit from a data owner identifier being included in personally identifiable data record taxonomy. Lots of hacked data appearing on the dark web is of unknown origin. But if the data owner is identified in the record then the identity of the source of the breach will be automatically evident. Perhaps the Federal or State EIN should be used. If a company knows their EIN could be leaked during a breach they will make better efforts to protect the data.
4. **DATA MINIMIZATION:** Information should only be retained if a business has a valid reason to do so. Snapping or not retaining data is technically different than deletion. Germany instructed Facebook to stop retaining certain data. **Instead of deleting data, consumers should be pre-approving the collection and retention of our data.**
5. **RETENTION SCHEDULE:** Data retention terms should be set by CCPA for all categories of data. Then there won't be any ambiguity concerning data minimization or expired data. Companies would be forced to delete data that has no business use or purpose. Corporations should be required to publish data retention schedules apart from their privacy policies. Data retention schedule display should be standardized by the Attorney General to include, but not limited to:
 - a. Data Type
 - b. Anonymized (Y/N)
 - c. Retention Period
 - d. Paper and Electronic Destruction Method
 - e. Locations Stored
6. **FORENSICS:** When there's a breach, the data controller should pay for the cost of forensics and be required to release a third-party report containing root cause. The data controller should be defined as the party that creates or originally receives the personal data. This way the controller will be more careful in choosing who to share data with if they are forever liable for ensuring its protection. Most breaches occur due to lack of investment in security and staff. CCPA should reinforce California's existing Whistleblowing laws providing a method for employees to report unaddressed cybersecurity risks without fear of retaliation.
7. **CONTRACTORS:** Contractors are often used to deflect liability, but there shouldn't be any indemnification allowed for CCPA. This alone will ensure that companies hire high caliber employees to data governance and cybersecurity roles, provide them with continuous education, pay for their certifications and conduct enhanced background checks. The Congressional Cybersecurity Act of 2010 (§ 209.1) originally required that these private sector cybersecurity employees go through security clearance and that NIST stipulate standards. Congress recognized how sensitive these roles were then.
8. **CERTIFICATION:** The leading bank lobbies are all pushing for the NIST Cybersecurity Framework to be made the global standard for cybersecurity and privacy. NIST is based upon ISO. ISO 27001 is a cybersecurity certification recognized globally. Whereas SOC 2 is an attestation only recognized in the US. Since the US are laggards to regulated data protection, we should look to Europe's best practice, which is ISO 27001. GDPR's Article 42

acknowledges that regulators won't be able to hire enough staff to conduct cyber audits so they will eventually recognize a cybersecurity certification as a GDPR standard. Perhaps CCPA should include proviso mirroring GDPR Article 42 so that corporations adhere to NIST and seek ISO certification.

9. **UNENCRYPTED MESSAGES:** Unencrypted email or text should be disallowed from containing any personal or financial data. Some service providers and financial institutions send email with personal financial data in it. It is as if they recognize this data is being scraped by data brokers and are encouraging it. But this also puts the recipient at risk for attack. I know of one bank that never sends PII by email. Instead they notify customers by email to access their accounts to see messages. This is how it should be done. **I think most consumers will choose to do business with companies that take their data protection seriously.**
10. **BREACH DEFINITION:** Should include cloud or datastore misconfiguration. This is akin to leaving your door open or unlocked. It is increasingly common due to the popularity of the cloud. But if you leave your door open, you cannot necessarily tell who came in, what they saw or whether they took anything. Including cloud misconfiguration as a breach would ensure that this is prevented and reported. **This is not the cloud vendors fault.** Their services default to a protected state. The onus is on their customers to hire the right employees, train them and implement ample security controls and monitoring technology.
11. **CCPA PORTALS:** The Equifax hack occurred on their consumer data discovery and correction portal. A [Congressional investigation](#) (page 96) determined that attaching a web query tool with read/write access onto an insecure legacy environment is very unwise. CCPA rules should prevent corporations from repeating this mistake with consumer opt-in portals. Companies should not increase consumer risk in their CCPA compliance efforts.
12. **DISCLOSURE:** Since consumers don't know which companies are maintaining, sharing or processing their data, any corporation handling personal data should be required to register themselves in an online database established by your office.
13. **UNIVERSAL CONSENT:** CCPA disallows universal consent by requiring presentment of the actual data capture. European companies are using cookie banners to disclose cookie use. But these cookie banners do not disclose the actual data capture, how it is being used or who it is being shared with. To prevent these cookie opt-in banners appearing in the US, CCPA should stipulate that universal consent is disallowed.
14. **DATA PROTECTION OFFICER:** GDPR's Article 37-39 requires the appointment of a Data Protection Officer. CCPA should stipulate a Data Protection Officer ("DPO") with the same terms. Otherwise corporations may assign people to privacy governance that have no technological experience. In order to prevent this the DPO should be registered in public records and be deposed in legal matters. Data Protection Officers and Whistleblowers should be required to prove they made all best efforts to rectify any CCPA violations internally before reporting to the AG's office. Covered corporations should be required to publish their internal CCPA compliance reporting and escalation procedures so that adherence is auditable and irrefutable. DPO's should also be required to provide annual cybersecurity and data privacy attestations same as required by New York's 23 NYCRR 500 so that they are accountable.
15. **COOKIES and TRACKING TECHNOLOGY:** There are four types of cookies:
 - a. Security and Privacy – perform authentication. None of the data mining or web content marketing companies have this technology.
 - b. Performance – anonymous
 - c. Profiling – presently not anonymous - harmful
 - d. Targeting – presently not anonymous - harmful

Email also has web beacons and link tracking that would have to be disclosed under CCPA unless they are used for regulated security. A lot of worthless data is being retained or compiled by cookies and tracking technologies because companies are erroneously assuming that it might have value in the future. Online behavior needs refinement because the internet is relatively new. To say that consumers should sacrifice their privacy for convenience makes no sense when it subjects them to damage. Companies need to focus on protecting data, instead of compiling it. Lots of very smart people thought that subprime mortgages were a good idea too. Data mining is no different. It is destructive to our economy and national security. The more data that is surreptitiously compiled on a person, the more likely it will be inaccurate and disseminated to nefarious persons. Data mining's underlying motivation is to set people up for failure and that is inherently harmful to society.

16. **SURVEILLANCE IS STALKING:** Corporations need to be regulated to respect privacy and make better decisions. "Voyeuristic disorder" is a psychiatric illness. When I've uncovered instances where I am being surveilled or electronically stalked, it makes me feel as vulnerable and injured as a physical violation. As with stalking, there's quantifiable material damages too. Voyeurism is classified as a psychosexual disorder. It was recently identified that apps have been surveilling teenagers and women's bodily functions. Do women and children deserve protection from victimization? The National Institute of Justice conducted a national stalking victimization study in 2009. Of 3,416,460 victims, 36.6% of stalker motivation were "retaliation, anger or spite", 32.9% were "control" and 23.4% were "mental illness or emotional instability". Doesn't this apply to those who stalk people with data mining or social media? Wouldn't these same motivations exist for corporations that compile perverse personal data on consumers or employees? Electronic voyeurs, like stalkers also attempt to rationalize, minimize and excuse their behavior. It has taken many States too long to address stalking and now wrongdoers have an electronic arsenal to aid them. The justice system acknowledges that stalkers are criminals who have an underlying mental disorder. It is time that electronic voyeurism be legally defined as criminal stalking.
17. **INCLUDE EMPLOYEES:** I read through the CCPA community testimony and most anti-privacy comments were requesting that CCPA exclude coverage for employees. Yet most of the data scraping is performed to screen potential or current employees. There's no acknowledgment that if you are spying on your employee, then someone else is too. And companies are increasing their own vulnerability by doing so. Everyone is spying on their employees but they cannot tell if anyone's spying on their own networks. The focus is on scraping employee activity while they neglect their own cyber defenses.

I am submitting this anonymously for the public record. But your office is very welcome to contact me for clarification or assistance.

Thanks again.

Message

From: George Usi [REDACTED]
Sent: 3/5/2019 2:40:46 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: John Riley [REDACTED]
Subject: CCPA Hearing Stanford - Omnistruct
Flag: Follow up

Thank you for your time at Stanford today. My statement is incorporated into the body of this email.

-----start statement-----

My name is George Usi with Omnistruct Inc, a cyber risk management consultancy and service business helping businesses who strive to adopt and enforce cyber security and privacy regulations so they can protect privacy data under their stewardship.

We commend the introduction and adoption of CCPA as well as the prospect of the privacy protection outcomes resulting from your effort.

I am internetworking and cyber security scientist by origin having designed networks for some of the first internet service and content providers in the 1990s when we were still trying to explain to businessmen and lawmakers how the fundamentals of the the Internet Works. I am also a recipient of the global IPv6 Internet Pioneer award for my contributions to Metronet6, Northcom wireless interoperability publications, and internet security standards in next generation wired and wireless internet technologies including collaborative advocacy of IPv6 & Delay Tolerant Networks with Scott Hogg, Edward Horley, Tom Coffeen, Dr Vint Cerf, Dr Larry Roberts, and Jim Bound.

I have also dedicated my life to setting standards in technology, privacy governance, and cyber security. My path emerged after I lost my wife, Sherie Usi, to breast cancer where I was grieving with other widowers who had had their deceased wives privacy data stolen while they were settling their estates. Thus, I take the complications and technical matters related to any law with data collection or monitoring to heart.

I would like to highlight the classification of data elements for privacy identification based on IP and geolocation identifiers within the legislation that could present a masking, false positive, or obfuscation, problem for consumers, businesses, service providers, and organizations in general required to monitor and prove enforcement or defense of the privacy data position.

First, Public IP addressing can be masked or changed easily using tunnels, dynamic dns services, and other virtual private network methods that could present enforcement challenges for a consumer pursuing their privacy rights or for a business defending their privacy protection position. We suggest that IP addressing as a unique identifier be enhanced, or replaced, with a different IP or infrastructure attribute that can be tracked more accurately as well as additional attributes uniformly shared by both IPv4 and IPv6 addressing.

Secondly, we want to note that with regards to geolocation and the introduction of new internet technology addressing schemes in use by the largest content and service providers, who are likely to handle the most amount of consumer privacy data, that the noting of a technical monitoring complication within IPv6 to IPv4 dual stack or tunneled geolocation issues coupled with the inherent risk of inaccuracy for IPv6 geolocation, will severely impact the geolocation accuracy of monitored data making artifact collection untenable. We do suggest a multi-facted enhancement to the geolocation identifier or eliminating the provision.

Consequently, these are both complicated technical challenges that may require new protocols, architectures, and designs that make current CCPA enforcement deadlines untenable for the scientific, business, and public sector communities.

I, The American Registry for Internet Numbers, California IPv6 Task Force, and the Internet Corporation for Assigned Names & Numbers can provide technical guidance in this capacity and due to the technical nature of my feedback, comments will be published to the email address you have provided.

-----end statement-----

Thank you,

George Usi, CEO

Omnistruct Inc

mobile: [REDACTED]

desk: [REDACTED]

m: [REDACTED]

www.omnistruct.com (stealth mode site. new site coming soon - visit www.sactech.com for services today)

Omnistruct Inc & Security Assurance & Compliance Technologies (SACTECH) helps your organization plan, on-board, and enforce Cyber Security Frameworks through a fully maintained NIST-based information security program so you can reduce the financial risk of cyber security incidents while protecting privacy, and other data.

EMAIL US NOW TO LEARN MORE ABOUT OUR OMINSTRUCT PLATFORM & CARESM

CONFIDENTIALITY: This communication may contain confidential information. If you are not the intended recipient, or believe that you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use the information. Also, please indicate to the sender that you have received this email in error, and delete the copy you received.

LEGAL DISCLAIMER: Informational statements regarding laws, insurance coverage, cyber insurance coverage, or umbrella coverage are for general description purposes only. These statements do not amend, modify or supplement any insurance policy and Omnistruct & SACTECH is NOT an insurance broker or attorney and offers no insurances or insurance guarantees based on consulting recommendations in regulatory compliance or insurances of any kind. Consult your attorney and the actual policy or your agent for details regarding terms, conditions, coverage, exclusions, products, regulatory compliance, services and programs which may be applicable to you or your business. Your eligibility for particular products and services is subject to the final determination of underwriting qualifications and acceptance by the insurance underwriting company providing such products or services.

View our Privacy Statement at <http://www.sactech.com/privacy-policy2/>

Message

From: Thomas Considine [REDACTED]
Sent: 1/11/2019 4:01:53 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA Input

Good day to you,

Although my signature block below shows I'm currently in Arizona, I own property in California and my daughter is attending college there. My point being, I and my family have a vested interest in the CCPA regulations also.

I'm sure you are swamped with input on the CCPA, so I will get to the point.

As a Privacy Professional in private practice, one of the most appalling issues I have dealt with for my clients had been Payment Card data breaches. I'm not referring to large corporate breaches such as Marriott Hotels, or Target data breaches, I'm referring to unreported data breaches occurring at small to mid-sized organizations. These smaller data breaches do not get reported to State Attorney Generals offices under current data breach regulations. Yet, contractually the Payment Card Industry (PCI) and merchant banks can levy extreme fines and penalties against these smaller organizations, oftentimes forcing them to close their doors, lay off employees, and eventually file for bankruptcy protection.

In October 16, 2012 Visa Blog post stated; *"In fact, small businesses represent more than 90 percent of all the merchant data breach compromises reported to Visa."* You can read the blog post in it's entirety ["HERE."](#)

While all who process payment card transactions are contractually mandated to comply with PCI's Data Security Standards (PCI-DSS), the fines and penalties levied against the merchant account holder go unchecked and unreported to government officials, including the data breach itself and who the merchant(s) involved were. The Payment Card Industry and merchant banks earn many millions of dollars each year from these fines and penalties without the knowledge of State regulators, while ignoring data breach reporting requirements.

I worked with the late Nevada Senator Debbie Smith on crafting Nevada NRS-603A Protection of Personally Identifiable Information & Data Breach notification requirements. NRS-603A mandated compliance with PCI-DSS and a safe-harbor clause for merchants who suffered a breach. We never imagined PCI companies and banks would fail to report breaches to the the Nevada Attorney Generals Office for breaches involving payment cards and Nevada residents.

In closing I would like to say the Payment Card Industry and Merchant Banks should not be allowed to levy fines and penalties against merchants "UNLESS" the data breach is reported to State officials as required by most State Data Breach notification requirements. There should be some form of State oversight in place to assist merchants from these unregulated practices.

If you have any questions regarding this matter I would be happy to assist in anyway possible.

Respectfully,

Thomas J. Considine, CIPP/G, CIPP/US

Sr. Information Security Engineer

Enterprise Security, Privacy, Risk & AZRamp Vendor Compliance

ADOA - Arizona Strategic Enterprise Technology (ASET) Office | State of Arizona

Desk phone: [REDACTED]

Cell phone: [REDACTED]

<http://aset.azdoa.gov>

CONFIDENTIALITY NOTICE: The information contained in this e-mail and all attachments may contain privileged or confidential information. If you are not the intended recipient please notify the sender and delete the message and all attachments from your system without copying or disclosing it.

{"email-

policy":{"state":"closed","expirationUnit":"days","disableCopyPaste":false,"disablePrint":false,"disableForwarding":false,"enableNoauth":false,"expires":false,"isManaged":false},"attachments":{},"compose-id":"6","compose-window":{"secure":false}}

Message

From: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Sent: 3/14/2019 10:55:12 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA ltr.pdf
Attachments: CCPA ltr.pdf



From: Enhanced Recovery Company

Address: 8014 Bayberry Rd Jacksonville, FL 32217.

ATTN: Privacy Regulations Coordinator, 300 S. Spring St., Los Angeles, CA 90013.

To whom this may concern,

ERC is a debt collection agency that meets the threshold requirements of a company subjected to the California Consumer Privacy Act (CCPA) going into effect January 2020. Because it is clear the CCPA was not designed or written with our industry in mind, ERC has a list of concerns regarding provisions of the CCPA and its effect on the Debt Collection industry.

We first seek clarification on the definition of a 'consumer'. The CCPA's definition of consumer is broader than the traditional definition of consumer, that existing laws in California use as applied to persons who a business serves. The already existing California Rosenthal Fair Debt Collection Practices Act as well as the Fair Debt Collections Practices Act (FDCPA) which governs the debt collection industry defines consumer as any natural person obligated or allegedly obligated to pay any debt. The CCPA, on the other hand, defines consumer as a natural person who is a resident of California.

The definition of consumer provided by the CCPA seemingly refers to a data subject. Clarification on whether the CCPA's definition of consumer is actually any person whose personal data is being collected, held, or processed would assist industries like ours in becoming compliant as it would clarify whether the definition would include employees of a business as well.

Communications are a large portion of lawsuits that affect the debt collection industry. The CCPA provides that a consumer may request access to personal information a business has collected about them and a business must disclose the requested information free of charge within 45 days of the receipt of a consumer's request. Standardizing communications by providing businesses subjected to CCPA compliance with safe harbor language will allow a safe way to notify consumers, per disclosure requirements, without communications being found as "false, deceptive, or misleading" per industry and Federal Debt Collection Practices Act ("FDCPA") standards.

Privacy and confidentiality are a business's top priority in the financial service industry. Specifically, in the debt collection industry, the FDCPA provides that a collector must not disclose the existence of a debt to a third party. The California Rosenthal Fair Debt Collection's Protections Practices Act is even more restrictive providing that an agency must obtain written consent before speaking with a third- party. Fulfilling CCPA requests will put businesses at a high risk of third-party disclosure. There are currently no provisions regarding requests received from agents of the consumer and verification of a principal agency relationship whether it be parent guardian, attorney client, or spouse just as examples.

The debt collection industry would also benefit from clarification regarding verifications. The CCPA allots for letters or email verifications. Requiring businesses to disclose the requested information free of charge, may come at a significant cost to businesses depending on the number of requests received. Although, industry executives seek to ideally reduce postage expenses, and have the option to provide verifications via email, there are third party disclosure concerns specifically regarding emails used in consumer communication. Debt collection agencies have a duty to protect consumers against inadvertently sharing their information with a third party. Providing verifications per consumer request through emails creates the risk that a consumer may provide a work email or shared email address which would give rise to third-party disclosures.

When providing any sort of deletion in compliance with a request, ERC seeks clarification on a business's ability to retain records that show they have responded to a request for deletion, along with a record retention period.

The CCPA private right of action is amended under SB-1121 to clarify a consumer may bring action only for a business's alleged failure to "implement and maintain reasonable security procedures and practices" that result in a data breach (CCPA § 1798.150 (c)). Additionally, § 1798.155(b) allows the AG to impose up to \$2,500 for unintentional violations, and up to \$7,500 for intentional violations. How does a business prove it implemented "reasonable" security practices and procedures? Moreover, what defines intentional versus unintentional? This broad definition opens a very large platform for interpretation and leaves businesses without guidance.

SB-1121 amends CCPA § 1798.150(k) which stated a business must disclose on its website or in its privacy policy a consumer's right to request deletion of his or her personal information, to now require businesses to make this disclosure "in a form that is reasonably accessible to consumers". The debt collection industry communicates with consumers through mail and telephone. ERC, like most debt collectors in our industry, also uses its website to facilitate communications and account maintenance. Our industry seeks clarification on what is to be considered a form that is reasonably accessible to consumers.

Lastly, we suggest California provide a platform for businesses to ensure a structured and efficient means for CCPA compliance, in the form of an official CCPA certification. Certification can serve as marketing tools to encourage CCPA Compliance. CCPA certification will also assist businesses in onboarding third party service providers to ensure businesses are dealing with a trusted third party.

Thank you for allowing a forum where businesses can provide feedback. It is our hope that the concerns of the debt collection industry are given serious consideration when executing any future comments or amendments to the CCPA.

Kind Regards,

Michelle Gensmer
Senior Vice President of Legal and Compliance



Message

From: Olivia Samad [REDACTED]
Sent: 3/8/2019 12:35:32 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: (G [REDACTED])
Subject: CCPA Pre-rulemaking comments re Privacy Rules for CPUC-Regulated Energy Utilities
Attachments: Letter to OAG 3 8 2019 re CCPA.PDF

Attached, please find a joint letter from Southern California Edison Company, Southern California Gas Company and San Diego Gas & Electric Company for your consideration in the CCPA rulemaking regarding privacy rules for CPUC-regulated energy utilities.

March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street, Los Angeles, CA 90013
Via email: PrivacyRegulations@doj.ca.gov

Re: Regarding Privacy Framework for CPUC-Regulated
Energy Utilities

Dear Privacy Regulations Coordinator,

This is a follow up to a meeting we had in San Francisco on Wednesday, November 14, 2018 regarding the California Consumer Privacy Act (CCPA) with Eli Blume, Niklas Ackers, Stacey Schesser, and Anthony Lew. At that meeting, we mentioned general background on privacy laws that affect investor-owned energy utilities (IOUs). This letter provides more background on the existing privacy framework that governs IOUs under state law and under the rules of the Cal. Public Utilities Commission (CPUC).

While other businesses may share customer data for commercial gain, our reasons are often to further State policy goals (clean energy, GHG reduction, public purpose research, enabling competition) that do not neatly fit the privacy concerns that the CCPA focuses on, or raise the specter of profiting from a data subject's data. In addition, CPUC regulation has tailored privacy rules that further protect consumers and allow for competition, access, sharing.

I. State Laws that Govern Electric and Gas Utilities Selling and Sharing of Consumer Data

One key concern that the CCPA seeks to address is the sale of customer data. IOUs are already prohibited from selling customer data under state law,¹ and also restricted in how that data is shared. Although CCPA does not apply to municipalities, the same statutory prohibitions that apply to IOUs also apply to municipalities.²

CCPA creates obligations on IOUs (though not on municipal utilities) to track and disclose sharing of customer data. IOUs may share data without customer consent to fulfill primary purposes. Pub. Util. Code § 8380(e)(2) states: "Nothing in this section shall preclude an electrical corporation or gas corporation from disclosing a customer's electrical or gas consumption data to a third party for system, grid, or operational needs, or the implementation of demand response, energy management,

¹ Public Utilities Code Section 8380(b)(2) prohibits us from selling customer data or PII. It also prevents us from sharing the data except for limited exceptions. See 8380(b)(1) and (e).

² Pub. Util. Code § 8381. In contrast, CCPA only applies to for profit businesses.

or energy efficiency programs, provided that, for contracts entered into after January 1, 2011, the utility has required by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure, and prohibits the use of the data for a secondary commercial purpose not related to the primary purpose of the contract without the customer's consent."

This is called the "primary purpose" exception, which concerns the utility's use and sharing of customer data without the need for customer consent. This is both statutory and CPUC-decisional. The CPUC expanded on the statutory definition as follows:³

(c) Primary Purposes. The "primary purposes" for the collection, storage, use or disclosure of covered information are to:

- 1) provide or bill for electrical power or gas,
- 2) provide for system, grid, or operational needs,
- 3) provide services as required by state or federal law or as specifically authorized by an order of the Commission, or
- 4) plan, implement, or evaluate demand response, energy management, or energy efficiency programs under contract with an electrical corporation, under contract with the Commission, or as part of a Commission authorized program conducted by a governmental entity under the supervision of the Commission.

The definition the CPUC arrived at was subject to years of stakeholder workshops and briefing. Non-utility use is a secondary purpose unless it falls within the meaning of primary purpose.⁴

II. CPUC Privacy Rules

In addition to the fact that IOUs are not allowed under Public Utilities Code Section 8380 to sell customer data, or to share it except under narrow exceptions (with parallel restrictions on municipal energy utilities), many other rules specifically protect the privacy of customers of CPUC-regulated energy IOUs.⁵

Smart Grid Data privacy rules,⁶ based on Public Util. Code § 8380 et seq., provide transparency and

³ See D.11-07-056 at p. 50; *see also* Attachment D to D.11-07-056, p. 7. CPUC decisions since 2000 are available at <http://docs.cpuc.ca.gov/DecisionsSearchForm.aspx>.

⁴ See D.11-07-056 at p.50. Attachment D to the decision is what governs the IOUs. See D.11-07-056 at p. 117.

⁵ There are of course general privacy laws that govern IOUs, but this letter is intended to provide industry-specific background to assist understanding the operating rules we already have.

⁶ These rules were established in Rulemaking 08-12-009. All decisions can be found by clicking on the link to the Docket Card and then entering R0812009 in the proceeding. See <http://www.cpuc.ca.gov/proceedings/>.

numerous protections for utility customers.

The first Smart Grid decision, D.11-07-056,⁷ allows customers to authorize third parties to automatically access their Smart Meter hourly usage data, directly from the utility data servers. The decision also provides the following:

- Adopts privacy rules that apply to customer energy data collected from Smart Meters (“Privacy Rules”). Provides for collection of “covered information” for “primary purposes” only. “Secondary purposes” require customer consent.
- Ordering Paragraph (OP) 3 of the Decision requires that the IOUs submit annual privacy reports to the Executive Director of the CPUC containing the information required to be reported annually by Rule 8(b) and Rule 9(c) of the Privacy Rules.
- OP 4 of the Decision ordered the IOUs to conduct independent audits of their data privacy and security practices, as required by Rule 9(d) of the Privacy Rules, and the IOUs have reported the audit findings as part of each General Rate Case (GRC) application filed after 2012.
- Attachment B to D.11-07-056 includes additional CPUC privacy rules and decisions that pre-date D.11-07-056.
- Attachment D to D.11-07-056 includes the energy privacy rules that were later described in conforming tariffs.

Then, D.12-08-045⁸ established privacy protections concerning customer usage data for customers of gas utilities, community choice aggregators (CCAs), and electric service providers (ESPs) similar to those established in D.11-07-056 for electric utility customer data.

Based on the Smart Grid privacy decisions, IOUs have CPUC-approved tariffs that codify the Privacy Rules that govern our customer relationships. For example, for SCE, most of the relevant privacy rules are codified in tariff Rules 24, 25, and 26.⁹

In addition to the Smart Grid Privacy rules, these are a sample of additional CPUC rules that govern customer data from oldest to newest:

- D.91-05-007, OP 3 states, “SDG&E, PG&E, and Edison shall not permit any person who is not charged with monitoring power producer operating efficiencies to gain access to power producers’ operating data. SDG&E, PG&E and Edison shall not permit any employee of any utility affiliate to gain access to power producers’ operating data.”
- D.97-10-031 was issued in the Direct Access Proceeding, which created rules for allowing competition. It also requires that any aggregated information provided by an IOUs must be

⁷ Decision and appendices A-E *available at* <http://docs.cpuc.ca.gov/SearchRes.aspx?DocFormat=ALL&DocID=457514>.

⁸ Decision available at <http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M026/K531/26531585.PDF>.

⁹ SCE’s tariffs are available at <https://www.sce.com/regulatory/tariff-books/rules>.

made up of at least 15 customers and a single customer's load must be less than 15% of an assigned category (the 15/15 rule).

- D.01-07-032 denied California Narcotics Officers Association access to utility customer information without a subpoena and customer notice. When utility customer data is provided to law enforcement agencies without legal process, the customers' privacy rights under Article I, §13 of the California.
- D.06-06-066 (modified by D.07-05-032) adopted a process for determination of whether information is entitled to confidential treatment as "market sensitive" for purposes of § 454.5(g); includes a matrix of market sensitive procurement data and rules for providing access to it; D.08-04-023, D.06-12-030, D.11-07-028 include rules for accessing procurement data, including form model protective order and non-disclosure agreement Constitution are violated.

III. Sharing Data for Approved or Public Purposes

In the most recent Smart Grid privacy decision, D.14-05-016,¹⁰ the CPUC adopted exceptions to the Smart Grid privacy rules and a process for oversight of third parties who access customer data by participating in the program. This is the decision that requires IOUs to provide customer-specific data to academic researchers that meet certain exceptions. If the utility responds to the requestor that it cannot grant access to the data sought and the requestor does not agree to other options or modifications to the request such that its request could be granted, the requestor may bring the dispute for informal discussion before the Energy Data Access Committee (EDAC).¹¹ EDAC meets quarterly and is composed of the investor-owned energy utilities (Pacific Gas and Electric Company, Southern California Edison Company, Southern California Gas Company, San Diego Gas & Electric Company), Commission staff, the Office of Ratepayer Advocates, qualifying academic researchers, representatives of customer and privacy advocacy groups, and other interested parties.¹² The requestor may also escalate further by petitioning the Commission about its denied request.¹³ The decision also created a website list of third parties ineligible due to past abuses. It requires IOUs to post aggregated customer usage data by zip code and customer class (i.e., residential, commercial, industrial, agriculture).

The same decision created an exception for utilities to share customer data with state and federal agencies for specific purposes that align with their statutory purpose, and specified forms of aggregate customer data to local governments. It also adopted aggregation methods for customer energy usage data by customer class against the background of the general 15/15 rule and other Smart Grid privacy rules.

¹⁰ Decision available at <http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M090/K845/90845985.PDF>.

¹¹ See D.14-05-016, Attachment A, "Data Request and Release Process," at pp. 1-2, paragraph 5.

¹² See D.14-05-016 at p. 159, OP 10, OP 11.

¹³ See D.14-05-016, Attachment A, "Data Request and Release Process," at pp. 3-4, paragraph 10.

IV. Other Data Access Rights IOUs Provide

CCPA introduces concepts like access to specific pieces of information and portability. However, for IOUs, CPUC rules already allow for energy utility competition, portability and data access for third parties.¹⁴ The aforementioned privacy rights are balanced by the CPUC in policy decisions to allow access to third parties in some instances.¹⁵


V. Conclusion

We hope this high level overview of industry-specific privacy rules and concerns that govern IOUs proves helpful as you consider what you need to implement by way of regulations and enforcement under the CCPA. If you have additional questions, please let us know how we can help.

Sincerely,


/s/ R. Olivia Samad

R. Olivia Samad
Privacy Counsel, Senior Attorney
On behalf of
Southern California Edison Company
2244 Walnut Grove Avenue
Rosemead, CA 91770



/s/ Gary Perlmutter

Gary Perlmutter, Sempra Energy
Chief Counsel, Technology & Business
Services
On behalf of its subsidiaries, Southern
California Gas Company and San Diego Gas &
Electric Company



¹⁴ See e.g. D.12-11-025 (ordering the implementation of rules to allow third party Demand Response Providers (DRPs) access to retail customer's data for purposes of registering and using the customers loads in the CAISO market) *available at* <http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M037/K494/37494080.PDF>.

¹⁵ Third parties often seek less stringent standards for data access or protection. See e.g. Comments of Center for Energy Efficiency and Renewable Technologies, at p. 5 (seeking less stringent control over customer information in their comments to a proposed decision) *available at* <http://docs.cpuc.ca.gov/PublishedDocs/EFILE/CM/136529.PDF>.

Message

From: Allison Cohen [REDACTED]
Sent: 3/8/2019 11:48:11 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulator]
CC: James Taylor [REDACTED]; Jessica Lee [REDACTED]; Melanie Howard [REDACTED]; Susan Israel [REDACTED]; Jeff Hamburg [REDACTED]; Robyn Mohr [REDACTED]; John Monterubio [REDACTED]
Subject: CCPA Preliminary Comments from Loeb and Loeb
Attachments: CCPA Preliminary Comments from Loeb and Loeb.pdf

Attached please find our CCPA Preliminary Comments for your review and consideration.

Thank you.

Allison Cohen
Of Counsel



10100 Santa Monica Blvd., Suite 2200 | Los Angeles, CA 90067

[REDACTED] Fax: 310.919.3814 [REDACTED]

Los Angeles | New York | Chicago | Nashville | Washington, DC | San Francisco | Beijing | Hong Kong | www.loeb.com

CONFIDENTIALITY NOTICE: This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is STRICTLY PROHIBITED. If you have received this transmission in error, please immediately notify the sender. Please destroy the original transmission and its attachments without reading or saving in any manner. Thank you, Loeb & Loeb LLP,



10100 Santa Monica Blvd.
Suite 2200
Los Angeles, CA 90067

Main 310.282.2000

Via E-mail: PrivacyRegulations@doj.ca.gov

March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Re: California Consumer Privacy Act Rulemaking

Dear Attorney General Xavier Becerra:

At Loeb & Loeb, we represent mid to large size companies that interact with California consumers. The brands we represent care very much about respecting the privacy rights of consumers and are currently working diligently to understand and implement the California Consumer Privacy Act ("CCPA"). Your written regulatory guidance is crucial in helping businesses across the country comply with the CCPA.

In an effort to assist you in the development of such regulations, we have outlined three distinct issues that merit written regulations to clarify the intent and scope of the CCPA. Below you will find the rationale and proposed regulatory language for each of the three issues.

The Attorney General is granted authority to adopt these regulations pursuant to Section 1798.185.

I. CLARIFY THE APPLICABILITY OF THE CCPA TO EMPLOYER/EMPLOYEE RELATIONSHIPS.

Rationale: Employees and contractors, acting in that capacity, should not be considered "consumers" and the personal information collected in the context of an employer-employee relationship should be exempt from the CCPA's definition of a consumer. Cal. Civ. Code § 1798.140(g). As the CCPA is currently drafted, a California employee could fall under the definition of "consumer."

The CCPA is a consumer protection law, protecting against unfair, deceptive or fraudulent business practices, promoting fair trade and competition, or preventing consumer injury due to damaged, faulty or dangerous goods and services.

California law already provides employees and job applicants with various rights of access to employee personnel information. These laws are specifically tailored to the employer-employee relationship and more accurately address access to personal information in the employment context than any of the provisions in the CCPA. Cal. Lab. Code §1198.5 and § 432.

Because an employer/employee relationship is fundamentally different from that of a business/consumer, the CCPA is likely to adversely affect an employer's routine business operations, and, in some instances, it may be administratively impossible for an employer to determine which records may be subject to such CCPA requirements and which are excluded under 1798.105(d)(8) and 1798.145(a)(1), raising obstacles to implementation and privacy concerns.

Please find below our recommended language for a regulation that would exempt information collected during the course of the employer-employee relationship from the requirements for consumer personal information.

Attorney General Authority to Adopt Regulation:

The Attorney General is granted authority to adopt this regulation pursuant to Section 1798.185 (a)(1).

Proposed Language:

Personal Information Collected Pursuant to an Employer-Employee Relationship. To the extent personal information is collected from an employee (as defined by the Cal. Lab. Code §§ 3351 and 3357) in the context of an employer-employee relationship (as defined by Cal. Bus. & Prof. Code § 7580.10), it shall not be treated as the personal information of a consumer under the California Consumer Privacy Act (Cal. Civ. Code § 1798.140(g)).

II. CLARIFY THAT INDIVIDUAL PERSONAL INFORMATION IS NOT SUBJECT TO HOUSEHOLD PERSONAL INFORMATION ACCESS REQUESTS

Rationale: The definition of "Personal Information" in §1798.140(o)(1) includes information about "a particular consumer or household." In making rules for the exercise of consumer rights set forth in Section 1798.130, the Attorney General should clarify that no individual consumer has the right to request access to, or deletion of, the personal information of any other individual consumer, even if the other consumer is a member of the same "household." Only aggregate "household information," such as "household income" or "household utility use," should be provided to an individual consumer in response to such a request.

Attorney General Authority to Adopt Regulation:

The Attorney General is granted authority to adopt this regulation pursuant to Section 1798.185(a)(7)

Proposed Language:

No individual consumer shall be entitled, under Section 1798.130, to access or delete personal information of any other individual consumer even if such individuals are members of the same household. The only household personal information that may be subject to an individual request for access or deletion is aggregate household information. The prohibition against one individual consumer receiving access to or deleting the personal information of another individual consumer does not apply when a consumer is acting as the duly authorized representative of another consumer.

III. CLARIFY THAT THE TRANSFER OF PERSONAL INFORMATION IN CONNECTION WITH CERTAIN FINANCIAL TRANSACTIONS IS NOT A "SALE"

Rationale: Financial institutions need to transfer personal information in connection with certain financial transactions such as the sale of a loan or loan portfolio, the sale of a credit card account or portfolio of accounts, securitizations, and the servicing of any of the foregoing. Such transfer of personal information should be an exception to the definition of a "sale", in keeping with the intent of the carve-out for Graham-Leach-Bliley Act in Section 1798.145(e). To effectuate this, Section 1798.140(t)(2)(D) bears further elaboration to make clear that: (1) selling loan portfolios to a third party constitutes a transfer of "all or part of" a business; and (2) personal information is inextricably linked to such portfolios and is attendant to servicing the underlying loans. Please find our recommended language for a regulations here.

Attorney General Authority to Adopt Regulation:

The Attorney General is granted authority to adopt this regulation pursuant to Section 1798.185(b).

Proposed Language:

(a) **Transfers via Merger, Acquisition, Bankruptcy, or Other Transaction.** All exemptions for transfers of personal information pursuant to a "merger," "acquisition," "bankruptcy," or "other transaction," which meet the definition set forth at California Consumer Privacy Act Section 1798.140(t)(2)(D), shall apply to the following financial transactions: the transfer or sale of personal information attendant to the sale of loan accounts or portfolios, credit card accounts or portfolios, securitizations and the



servicing of any of the foregoing. For purposes of Section 1798.140(t)(2)(D), servicing includes sending monthly payment statements and collecting monthly payments, maintaining records of payments and balances, collecting and paying taxes and insurance, managing escrow and impound funds, remitting funds to the note holder, and following up on delinquencies.

(b) **Nonpublic Personal Information Transfers.** To the extent that a transfer described in (a) consists of any categories of nonpublic personal information as defined and interpreted under federal regulations published by the Board of Governors of the Federal Reserve System ("Board"), the Federal Deposit Insurance Corporation ("FDIC"), the National Credit Union Administration ("NCUA"), the Office of the Comptroller of the Currency ("OCC"), and the Consumer Financial Protection Bureau ("CFPB"), California Consumer Privacy Act Section 1798.145(e) shall apply to such information.

We appreciate the opportunity to submit these comments, and we look forward to working with the Attorney General in your efforts to develop regulations to interpret the CCPA.

Respectfully submitted,

James Taylor, Partner

Jessica Lee, Partner

Melanie Howard, Partner

Allison Cohen, Of Counsel

Susan Israel, Of Counsel

Jeff Hamburg, Attorney At Law

Robyn Mohr, Attorney At Law

John Monterubio, Attorney At Law

Message

From: Jennifer Peters [REDACTED]
Sent: 3/8/2019 2:39:28 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA Preliminary Comments
Attachments: AG Rulemaking - CSM Guidance (1).pdf

Good Afternoon,

Please see Common Sense's comments regarding the California Consumer Privacy Act.

If you have any questions or concerns, please feel free to contact us directly.

Best,

--

Jen Peters
Advocacy Coordinator | [Common Sense Kids Action](#)
e: [REDACTED]
p: [REDACTED]

SUBMISSION RE CCPA REGULATIONS - RIGHT TO OPT-IN

To: Office of the Attorney General, California

From: Common Sense Media

Date: March 8, 2019

This submission offers proposed guidance regarding the right to opt-in. Rulemaking is required under Section 1798.185(a)(4) for the right to opt-out; as the right to opt-in is a similar right, Common Sense believes guidance would be helpful to give businesses, teens, and families more clarity and certainty.¹

CCPA Section 1798.120(c): Under CCPA, a business may not sell the personal information of a child under 13 years of age unless a parent or guardian has affirmatively authorized such sale (the “right to opt-in”). For minors ages 13, 14, and 15, the minor him or herself must affirmatively authorize the sale of their personal information. Businesses must refrain from selling the personal information of consumers they know are under 16 years of age. Businesses cannot willfully disregard a consumer’s age.

Proposed regulatory language:

Children under 13: A parent or guardian may affirmatively authorize the sale of a child under 13’s personal information (the “right to opt-in”). Such authorization must be both (i) affirmative and (ii) reasonably calculated, in light of available technology, to ensure that the person providing consent is the child’s parent or guardian. Affirmative authorization requires a verifiable consumer request,² made specifically by the parent or guardian of the child, in response to a clear and conspicuous disclosure detailing the business’s sale of personal information. Methods that are reasonably calculated to ensure that the person providing consent is the child’s parent or guardian include:

- (i) Providing a consent form to be signed by the parent or guardian and returned to the business in person, by postal mail, facsimile, or electronically;
- (ii) Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;
- (iii) Having a parent or guardian call a toll-free telephone number staffed by trained personnel;
- (iv) Having a parent or guardian connect with trained personnel via video-conference;
- (v) Having a parent or guardian communicate in person with trained personnel;
- (vi) Verifying a parent or guardian’s identity by checking a form of government-issued identification against databases of such information, where the parent’s identification is deleted by the business from its records promptly after such verification is complete.

¹ In addition, if legislation is passed that expands the right to opt-in--to older teens and adults, and/or to activities beyond sale (see Privacy For All, AB1761, Wicks), rulemaking will be needed regarding opt-in.

² Please note this submission is not intended to define what constitutes a “verifiable consumer request”.

To the extent a business is also seeking verifiable parental consent under federal law to comply with the Children's Online Privacy Protection Act and Rule, 16 CFR 312, it must obtain separate affirmative authorization to sell a child's information under CCPA.³

Youth ages 13, 14, and 15: A child aged 13, 14, or 15 may affirmatively authorize the sale of his or her personal information (the "right to opt-in"). Affirmative authorization includes a verifiable consumer request, made by the teen, in response to a clear and conspicuous disclosure detailing the business's sale of personal information. The disclosure must be appropriate to the teen's age and level of understanding.

Additional considerations:

Children visiting sites, services, and businesses should not have the misimpression that companies are selling their information, when the default is companies are not allowed to sell their information. One way to achieve this would be to require that businesses do not have any "Do Not Sell" link, button, or logo in such situations; or that they have a link, button, or logo indicating the business is not at present selling the child's information. See the first paragraph below for suggested language.

In addition, when children have opted-in to the sale of their information, they should be able to opt-out at any time in just as simple a manner as an adult can. Businesses should assume as much from the statutory language. However, to the extent additional guidance is helpful, the second paragraph below offers suggested language.

Additional potential regulatory language:

Websites, services, and businesses who have identified, or probabilistically identified, consumers under 16, or whose sites, services, and businesses are directed to consumers under 16, shall, to the extent technically feasible, display a button, link, or logo that indicates businesses are not presently selling the consumer's personal information, in a manner that is clear and obvious to the consumer and appropriate to the consumer's age and level of understanding.

If a consumer under 16's opt-in rights are exercised, a business shall provide the Do Not Sell opt-out button, link, or logo. A consumer, or the consumer's parent or guardian, shall be able to subsequently opt-out by following the standard opt-out procedures. A consumer, or the consumer's parent or guardian, as applicable, shall be able to opt-out at anytime.

³ This is consistent with federal requirements which state that "An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties." 16 CFR 312.5(a)(2).

Message

From: Engel, Jason [REDACTED]
Sent: 3/8/2019 3:15:17 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA Privacy Regulations
Attachments: Experian Comments to the California Attorney General_CCPA_Final.pdf

Please see the attached submission on behalf of Experian with respect to the regulations to implement the California Consumer Privacy Act.

Jason Engel
SVP & General Counsel

Experian North America



475 Anton Boulevard
Costa Mesa, CA 92626
[REDACTED]

The information transmitted in this message (including any attachments) is intended only for the person or persons to whom it is addressed, and may contain material that is confidential or protected by the attorney-client privilege. Any review, retransmission, dissemination or other use of the information contained herein by persons or entities other than the intended recipient(s) is prohibited. If you have received this message in error, please notify the sender immediately and delete the message.



March 8, 2019

Via electronic filing

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

Re: The California Consumer Privacy Act Rulemaking

Attorney General Becerra:

I am pleased to offer the enclosed comments on behalf of Experian for your consideration as you develop regulations to implement the California Consumer Privacy Act of 2018 ("CCPA").

Experian is comprised of a family of companies that are tied together by two simple objectives: (1) helping organizations protect, manage, and understand their data; and (2) helping consumers make informed choices and live smarter lives. Among the many products and services we offer, we facilitate consumers' access to credit, protect families from identity theft, provide consumers expert education on credit management, and provide numerous anti-fraud tools to businesses.

The success of our business relies strongly on consumer trust and being good stewards of information. Consumer privacy is central to Experian's corporate values, and we applaud the California legislature's goal of increasing consumer privacy and transparency with the passage of the CCPA. However, we believe that certain provisions within the law need to be clarified by the Attorney General to further the objectives of the CCPA and to ensure that the law does not result in harmful, unintended consequences to consumers. With this background, our comments bring attention to these key points:

1. *Clarify that the CCPA Exempts Data Processing for Anti-Fraud Purposes and Protects the Ability to Create Legitimate Fraud Prevention Tools.*

The CCPA's exemptions do not fully exempt data processing for anti-fraud purposes. First, although the fraud exemption in the CCPA's data deletion requirement clearly covers users of fraud tools (who "maintain the consumer's personal information in order to...protect against...fraudulent...activity"),¹ arguably, the exemption does not cover Experian's data

¹ Cal. Civ. Code § 1798.105(d)(2).

suppliers that provide information necessary to create those fraud tools because those data suppliers do not necessarily maintain the information in order to protect against fraudulent activity. The exemption also may not enable Experian's use of data to create and enhance anti-fraud tools because Experian does not just use these tools to protect Experian from fraud, but sells these tools in the marketplace for gain to enable businesses to protect themselves from fraud. Second, even though the CCPA clearly exempts data processing for anti-fraud purposes from the scope of the deletion right, the law is far less clear regarding an analogous exemption to the opt-out right for such anti-fraud data processing. As a result of the imprecise drafting in the CCPA, the law could inadvertently restrict the ability to gather the information needed to create, provide, enhance, or deliver anti-fraud tools and services, impacting the government and private sector actors that rely on these tools.

Since the CCPA provides consumers the right to request deletion of their personal information and/or opt-out from having a business share their personal information, consumer personal information that would otherwise be included in these fraud prevention tools may be deleted or prevented from being shared and used for anti-fraud activities that the CCPA endeavors to protect. Without the data needed to create, enhance, and update anti-fraud tools, users of these tools may not be able prevent fraud. As an example of the many uses of these tools, the State of California uses Experian's fraud prevention tools to verify the age of lottery participants for the California Lottery and to review the California DMV's list of individuals owning a disabled person parking placard to ensure deceased individuals are removed from the program. Similarly, California hospitals and health providers use Experian's anti-fraud tools to perform identity checks on persons who use online patient portals to interact with California healthcare providers. These tools also underpin important federal programs; the Internal Revenue Service, for instance, uses Experian's tools to prevent fraud in its disbursement of tax refunds. Lenders and online merchants across the country also use the tools to reduce financial and marketplace fraud, including identity theft. If data about a particular consumer is not available to allow an entity to validate the identity of that consumer, this may impede the consumer's access to those services or benefits.

We request that the Attorney General clarify through rulemaking (1) the scope of the fraud exemption to the deletion right, and (2) that such an exemption also exists for the opt-out right in the CCPA. The Attorney General may issue such regulations using his authority to adopt rules to "further the purposes of [the CCPA]."² In particular, we request that the Attorney General clarify that the CCPA fraud exemption to the consumer deletion right covers the collection, use, and sharing of personal information to create and distribute fraud prevention and detection tools. We also ask the Attorney General to clarify that a parallel exemption exists for the opt-out right so consumers may not opt out of a business's sharing of personal information for fraud prevention purposes. We submit that these clarifications would further the purpose of the CCPA, as the CCPA already recognizes the importance of fraud prevention, the clarifications would ensure this policy outcome is achieved, and they would create a consistent policy position on anti-fraud data processing and tools throughout the CCPA.

² Cal. Civ. Code § 1798.185(a), (b).

2. *The CCPA's Broad Coverage Jeopardizes the Reliability, Accuracy, and Availability of Data in Commercial Credit Reports Even Though These Reports Have No Bearing on Consumer Privacy.*

The CCPA's definition of "personal information," which helps set the boundaries for the scope of the law, includes the undefined concept of "professional or employment-related information."³ This language presumably reflects the judgment that sometimes an individual's profession or job helps define that person when marketers, retailers, or others offering consumer products or services are seeking to segment the consumer market. For example, certain generalizations made about blue-collar workers versus white-collar workers may hold true and be helpful for marketing purposes. However, as a result of imprecise drafting, this phrase in the CCPA could be construed to include any business or employment-related data regardless of whether or not the individual to whom the data is linked is acting in a consumer capacity. Such an interpretation would mean that all business-related information about an individual, and any associated information about the business (including financial information, business records, and other non-consumer information) potentially could be deleted or prevented from being shared under the CCPA.

There is a difference between the professional and consumer lives of individuals. The professional activities of Sally Smith, a hypothetical senior executive at Experian, need no privacy protection. Nor do the business activities of her spouse, Anthony Acosta, the sole proprietor of the Main Street Bike Shop. On the other hand, the CCPA reflects a consensus that the consumer activities of both Sally Smith and Anthony Acosta deserve privacy protection. Yet, commercial credit reports that Experian and other companies have provided to the market for decades include business and employment-related information and, therefore, may have inadvertently been swept into the law.⁴ If commercial credit reports are covered by the CCPA, all data within those reports would be jeopardized because individuals and businesses may be able to use rights afforded by the CCPA to delete information in or prevent the sharing of information contained in them.⁵

The following are just a few of the many examples of the unintended consequences of interpreting the CCPA to cover the business-related information in commercial credit reports: (1)

³ "Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household [including]... [p]rofessional or employment-related information...." Cal. Civ. Code § 1798.140(o)(1)(I).

⁴ This information includes data elements such as an individual's name, address, birthdate, and tax ID number, as well as any judgments instituted against the individual, d/b/a information, and information from various Secretaries of State on commercial licenses the individual may hold, among other data points.

⁵ Although personal information contained in *consumer* credit reports is expressly exempted from the ambit of the CCPA, no such exception is made for data in *commercial* credit reports. Cal. Civ. Code § 1798.145(d).

federal and state government agencies that use commercial credit reports (and their service providers) will not be able to conduct proper due diligence on their private sector contractors; (2) private sector efforts to fight fraud and money laundering through knowledge of banking customers gleaned through commercial credit reports will be hindered; (3) bank regulators that use commercial credit reports to understand banking relationships will not be able to reliably undertake safety and soundness checks; and (4) businesses that use commercial credit reports for due diligence purposes will struggle to make informed decisions about service providers and partners. This may result in unintended consequences to businesses, particularly small businesses, whose good business credit histories afford opportunities that may otherwise be unavailable.

We request that the Attorney General clarify through rulemaking that the phrase “[p]rofessional or employment-related information” in the CCPA’s definition of personal information excludes information about individuals acting in their business capacities, *i.e.*, personal and related business information used in commercial credit reports. In particular, the Attorney General has specific authority to adopt rules to “updat[e] as needed additional categories of personal information.”⁶ Clarifying through rulemaking that the phrase “[p]rofessional or employment-related information” excludes business representatives and sole proprietors listed in commercial credit reports creates an additional category of personal information pursuant to the law, as it delineates clearly the type of professional and employment information covered by the CCPA.⁷

3. Ensuring the “Explicit” Notice Requirement Does Not Unreasonably Burden Third Parties.

The CCPA prohibits a third party from selling personal information about a consumer that has been sold to the third party unless the consumer has received “explicit” notice and is provided an opportunity to exercise the CCPA right to opt-out of such transfer.⁸ However, the CCPA is silent as to which entity must provide explicit notice to the consumer, whether a third party can rely on the notice provided to consumers by the business who collected the data, whether the online privacy policy of a third party transferee satisfies the law, or whether such third party must provide direct notice to each individual consumer. As a result of the CCPA’s imprecise drafting, and if the law is interpreted to mean that third parties must provide direct notice to individual consumers, third parties may not be in position to comply with the explicit notice rule because they may not have a direct relationship with the consumer whose personal data they hold. As a result, third parties would not be able to transfer data in the marketplace,

⁶ Cal. Civ. Code § 1798.185(a)(1). The California Attorney General also has general authority to adopt rules to “further the purposes of this title.” Cal. Civ. Code § 1798.185(a), (b).

⁷ Although there are material differences between the two statutes, it is noteworthy that California law already distinguishes between consumer and business data and the protections each deserves, insofar as the California Consumer Credit Reporting Agencies Act also makes a distinction between consumer data and business data, classifying commercial credit reports as separate from consumer data in consumer credit reports. Cal. Civ. Code § 1785.41.

⁸ Cal. Civ. Code § 1798.115(d).

resulting in unintentional and unnecessary restrictions on legitimate, lawful, and beneficial data transfers that have no bearing on consumer privacy and are a crucial part of the functioning of the digital economy. This may exclude consumers from receiving beneficial information, offers, or opportunities, even for consumers who may want such information and who have made no election to opt-out.

We request that the Attorney General interpret through rulemaking that a third party may rely on its own privacy policy statements and written attestations from data providers to comply with the CCPA's explicit notice requirement. In particular, the Attorney General has specific authority to adopt rules "[t]o facilitate...the submission of a request by a consumer to opt-out of the sale of personal information."⁹ To best facilitate a request by a consumer to opt-out of the sale of personal information, third parties should provide an opt-out notice online and ensure through contractual commitments from data providers that proper CCPA disclosures were made to consumers in accordance with CCPA requirements. Such activities will create more certainty that opt out notices and instructions are provided to consumers by the entities that have a direct relationship with them.

4. *Clarify the CCPA Public Records Exception.*

According to the CCPA, personal information covered by the law does not include "publicly available" information, but this exception is not clearly defined.¹⁰ Publicly available information means information that is "lawfully made available from federal, state, or local government records,"¹¹ but excludes information that is "used for a purpose that is not compatible with the *purpose* for which the data is maintained and made available in the government records or for which it is publicly maintained."¹² The CCPA does not provide additional details on what this purpose limitation means or how to assess the purposes of various public records.

As a result of the CCPA's imprecise drafting that ties the definition of publicly available to the purpose for which the data is made available, it will be difficult, if not impossible in some cases, to determine if government released records are "publicly available" under the CCPA. The main issue is that when a government agency releases data, the agency may not describe (or fully describe) the purposes for which the data may or must be used. As a result, the CCPA definition will be difficult to apply and government records once legitimately used by the public may become subject to CCPA deletion and opt out rights. Numerous consumer and business products that use government record information would be jeopardized, including commercial credit reports. Commercial credit reports are used for multiple purposes, including by financial institutions to comply with Anti-Money Laundering ("AML") and Know-Your-Customer

⁹ Cal. Civ. Code § 1798.185(a)(4)(A). The California Attorney General also has general authority to adopt rules to "further the purposes of this title." Cal. Civ. Code § 1798.185(a), (b).

¹⁰ Cal. Civ. Code § 1798.140(o)(2).

¹¹ *Id.*

¹² *Id.* (emphasis added).

(“KYC”) regulatory requirements.¹³ AML and KYC rules require certain types of financial institutions (such as banks, credit unions, and broker dealers) obtain and verify information from potential customers to ensure that the financial institution has a reasonable belief that it knows the true identity of each customer.¹⁴ Federal regulators also expect financial institutions to review this information on a periodic basis, and to engage in additional customer due diligence as may be warranted. As a result, financial institutions have a broad and substantial need for access to customer information, such as the type of information contained in commercial credit reports that is based, in part, on government records data, in order to comply with their AML obligations.¹⁵ If data in commercial credit reports is deleted or prevented from being shared under the CCPA because data from government records is not protected by the CCPA’s publicly available records exception, compliance with AML and KYC rules may be hindered.

We ask that the California Attorney General clarify the definition of publicly available information so that information made available by government disclosures can be used unless the government specifically prohibits a certain use. In particular, the Attorney General has specific authority to adopt rules “[e]stablishing any exceptions necessary to comply with state or federal law.”¹⁶ Clarifying through rulemaking the term publicly available information so that information made available by government disclosures can be used unless the government specifically prohibits a certain use would help ensure that government records data can be included in commercial credit reports and used by financial institutions to comply with AML and KYC rules.

5. *Provide Guidance on the Cure Requirement and the Expected Standards for Reasonable Security Procedures and Practices.*

Under the CCPA, a failure to implement and maintain “reasonable security procedures and practices” to protect covered personal information could result in a cause of action by plaintiffs for statutory damages; however, a business has a safe harbor if the business cures the violation.¹⁷ Specifically, no action for statutory damages may be initiated against a business that fails to provide *reasonable security procedures and practices* if “within the 30 days the business

¹³ Although the CCPA creates an exemption for a business to “comply with federal, state, or local laws,” it could be argued that this exemption does not apply to Experian because Experian assembles the data that is used to comply with certain laws (by producing commercial credit reports) instead of directly using the information in commercial credit reports to comply with federal AML and KYC regulations. Cal. Civ. Code § 1798.145(a)(1).

¹⁴ 31 C.F.R. § 1023.210 (2018); *see also* BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL, FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL (2014), located at https://www.ftiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm.

¹⁵ *See* RENA S. MILLER & LIANA W. ROSEN, CONG. RESEARCH SERV., 7-7500, ANTI-MONEY LAUNDERING: AN OVERVIEW FOR CONGRESS 8-9 (2017), available at <https://fas.org/sgp/crs/misc/R44776.pdf>.

¹⁶ Cal. Civ. Code § 1798.185(a)(3). The California Attorney General also authority to adopt rules to update additional categories of personal information and has general authority to adopt rules to further the purposes of the CCPA. Cal. Civ. Code § 1798.185(a)(1), (b).

¹⁷ Cal. Civ. Code § 1798.150(a)(1), (2). Personal information is defined in Section 1798.81.5.

actually *cures* the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur.”¹⁸ The CCPA does not define “cure” or “reasonable security procedures and practices,” which creates uncertainty in the market, obscures what businesses must do to cure a violation, and risks that the cure provision will not be functional or have the desired remediating outcome.

Due to the lack of a definition of “cure” in the CCPA, there is a risk that a business could never cure a data security violation if “cure” is interpreted to mean that all data that was lost, corrupted, or subject to unauthorized access must be retrieved or restored. There also is a risk that unauthorized access to personal information can never be completely cured because the data has at one time been viewed by an unauthorized person. Overly narrow interpretations of the term “cure” such as these would be inconsistent with the law and would render the CCPA’s safe harbor meaningless. The lack of a definition for “reasonable security procedures and practices” exacerbates this problem. Without information about what constitutes a reasonable security procedure or practice, businesses will have little clarity regarding the steps they must take to cure a violation and meet the safe harbor requirements.¹⁹ The CCPA, building off of existing California law on data security,²⁰ recognizes that violations of the California data security standard are for the failure to implement and maintain reasonable security procedures and practices, not for a failure to prevent unauthorized access to, the acquisition of, or the loss of data, which may be fully outside a company’s control (e.g., breaches by foreign state actors). Therefore, the proper cure for a data security failure is to implement the reasonable security procedures and practices envisioned by the law, but such practices must be clearly defined in order for businesses to draw accurate lines between the procedures that are reasonable and those that are not.

We ask the California Attorney General to clarify that the “cure” requirement does not require a company to perform the impossible task of retrieving or restoring all data that may have been lost, corrupted, or subject to unauthorized data access. In addition, we ask the Attorney General to recognize that a business’s documented adherence to accepted cybersecurity remediation standards (such as those proposed by the National Institute of Standards and Technology, the SANS Institute, the International Organization for Standardization, or the Center for Internet Security) constitutes satisfaction of the duty to implement and maintain reasonable security procedures and practices under the CCPA. The Attorney General has specific authority to adopt rules to “further the purposes” of the CCPA.²¹ The interpretation we

¹⁸ Cal. Civ. Code § 1798.150(b) (emphasis added). No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of the title. *Id.*

¹⁹ In related contexts, it has been recognized that merely requiring “reasonable” security procedures and practices is too vague a requirement to be enforceable. *LabMD, Inc. v. FTC*, 894 F.3d 1221, 1236 (11th Cir. 2018).

²⁰ Cal. Civ. Code § 1798.81.5(a)(1) (“[T]he purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information.”); § 1798.81.5(b) (“A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”).

²¹ Cal. Civ. Code § 1798.185(a), (b).

propose would further the purpose of the CCPA. Without it, businesses will have no barometer by which to assess whether a data breach that resulted in unauthorized access of information is fully “cured.” Furthermore, our proposed interpretation would encourage businesses to adopt widely recognized standards of information security, thereby furthering the underlying goals of the CCPA by minimizing future data security risks and incentivizing companies to implement and maintain generally accepted data security protocols.

6. *Clarify that Personal Data Shall Be Provided About Household Members in Response to a Consumer Access Request Only in Limited Circumstances.*

The CCPA states that personal information covered by the law includes data linked to a consumer or household and creates consumer data access rights that could be misinterpreted to include access rights information about other individuals within a consumer’s household. The CCPA’s consumer access right states that “[a] consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer... [t]he specific pieces of personal information it has collected about that consumer.”²² Because the definition of personal information in the CCPA combines consumer and household data in the same definition, there is a concern that a business would need to disclose data about a consumer within a household to another consumer in the household.

If all household information must be provided in response to a consumer access request, there is a risk, at a minimum, of a privacy violation. There also is a risk that information is provided to an abusive or deceitful household member that uses the information for nefarious purposes.

We ask that the California Attorney General clarify that access requests are limited to only the personal information known about the individual consumer making the request or about others in the household if the individual making the request is an authorized representative of others in the household. The CCPA directs the Attorney General to “[e]stablish rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer’s...ability to obtain information...”²³ By establishing rules that more clearly describe when household information should be provided to a consumer, the Attorney General can carry out the directive to facilitate a consumer’s ability to obtain information pursuant to the law.

7. *Clarify that Pseudonymized Data Is Not Personal Information.*

The CCPA covers personal information related to consumers and households and, arguably, creates a distinct category of data once the data has been pseudonymized. According to the CCPA, “personal information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a

²² Cal. Civ. Code § 1798.110(a).

²³ Cal. Civ. Code § 1798.185(a)(7). The California Attorney General also has general authority to adopt rules to “further the purposes of this title.” Cal. Civ. Code § 1798.185(a), (b).

particular consumer or household [including]... [p]rofessional or employment-related information.”²⁴ The CCPA defines pseudonymized as the “processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.”²⁵ “Pseudonymized” is not otherwise referenced in the CCPA other than in the definition of research, where the CCPA lists pseudonymized data in the same category as de-identified data.²⁶ The CCPA does not clearly state whether pseudonymized data is a subset of personal information or whether pseudonymized data, which by definition is no longer attributable to a specific consumer without the use of additional information, is distinct from personal information.

The U.S. digital advertising ecosystem requires multiple entities to distribute IDs—typically pseudonymized IDs—to facilitate interest-based advertising while protecting the privacy and security of consumer identities and personal information. An overly broad reading of the definition of personal information in the CCPA to include pseudonymized data would jeopardize the viability of the digital advertising ecosystem because consumers would be able to delete information or prevent the sharing of pseudonymized information that the ecosystem relies upon. This is particularly a concern because third party businesses can facilitate deletion and opt-out requests for consumers on a mass scale, which would cause immediate detrimental impacts for digital advertising and threaten the availability of free online content. An additional concern with the inclusion of pseudonymized data in the definition of personal information is the unintended effect of forcing business to associate non-identifiable, pseudonymized device data with identifiable information about a specific person seeking to exercise their CCPA rights. For instance, companies that only have pseudonymized information will not have consumers’ names associated with that data. When a consumer makes a request under the CCPA, the business would need to associate the pseudonymous data it holds with the consumer’s name in order to fulfil the consumer’s request. This would remove existing data privacy protections enjoyed by California residents.

We ask that the California Attorney General clarify that pseudonymous data is not personal information under the CCPA. In particular, the Attorney General has specific authority to adopt rules to “further the purposes of [the CCPA].”²⁷ Such an interpretation would further the purposes of the CCPA because when pseudonymized data is not considered personal information, businesses can refrain from employing non-privacy forward practices, such as associating non-identifiable, pseudonymized device data with identifiable information about a specific person seeking to exercise their CCPA rights, in order to comply with the law.

²⁴ Cal. Civ. Code § 1798.140(o)(1).

²⁵ Cal. Civ. Code § 1798.140(r).

²⁶ Cal. Civ. Code § 1798.140(s).

²⁷ Cal. Civ. Code §§ 1798.185(a), (b).

* * * * *

Thank you for this opportunity to provide input into the California Consumer Privacy Act rulemaking. Please contact me at ([REDACTED]) or by email at [REDACTED] with any questions or requests for additional information. We look forward to continuing to work with your office on these important matters.

Regards,

A handwritten signature in blue ink that reads "Jason Engel". The signature is written in a cursive, flowing style.

Jason Engel
Senior Vice President and General Counsel
Experian North America

Message

From: Paige Bartley [REDACTED]
Sent: 3/8/2019 4:17:35 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA Public Comments
Attachments: [2019-3-8] CCPA - Comments.pdf

Hello,

Please find my attached comments on the California Consumer Privacy Act, as a follow-up to my oral comments from the public hearing at Stanford Law School on March 5th.

While I do identify my employer and my role, and my views are naturally influenced by my professional work, these comments reflect my personal opinions on the matter.

Paige Bartley

These comments, while necessarily influenced strongly by my research and work with my current employer, reflect my own opinions. I do cite supporting data that was uniquely available to me only via my relationship with my employer, but the firm I work for has no public stance on CCPA or related regulation. These are my views on the topic, to corroborate and augment the public comments I submitted at the March 5th public hearing at Stanford University.

The time is now for strong data privacy and protection regulation

Consumer awareness of privacy, and corresponding outcries over privacy infringement, are having tangible effects on businesses. Data breaches, unauthorized third-party sharing of data, and the lack of data portability have all become pain points for today's digital consumer, eroding trust in brands. If today's businesses are to forge enduring consumer trust and continue to remain profitable in the digital economy, they must become responsible stewards of personal data. But it is clear they will not forge these standards if left to their own devices. Strong regulation is needed to prompt action and ensure that consumers have recourse if their personal data is abused. In these comments, I will outline why regulation such as CCPA is not a burden for business, but rather an opportunity to optimize internal data management strategy and drive optimal business outcomes. Furthermore, strong data privacy and protection standards will facilitate trade and economic opportunities for California businesses amidst proliferating global regulations that set privacy and protection requirements for the international transfer of data: a key driver for commerce in the modern economy.

The opportunity to set a “gold standard” in the US

In the EU, the General Data Protection Regulation (GDPR) aspired to set a 'gold standard' for the management and processing of personal data, and many other jurisdictions soon forged mirroring policy. CCPA is an extension of this philosophy, aiming to advance high-level standards for data protection and privacy in the US absent federal legislation. With global regulatory requirements proliferating, many businesses are having trouble keeping up. The challenge is not one of simply increasing security or meeting individual technical requirements, but rather one of improving and maintaining core data-control capabilities. For many organizations, GDPR was a wakeup call, highlighting the painful truth that their data management architecture was siloed and ineffective. Data privacy, and the ability to achieve it, requires foundational data control capabilities that have downstream benefits to other data-driven initiatives. With California as the world's fifth largest economy, CCPA is an opportunity to nudge forward best practices for data in the US economy.

Data privacy: a false threat to business models

Data privacy, and the regulatory obligations associated with it, are frequently perceived by the enterprise as a net burden in both cost and time. However, there lies immense business opportunity in the requirements to control personal data. Any data-driven regulation, such as GDPR or CCPA, is a mandate to gain better control of informational assets. Better control of data, ultimately, has downstream benefits for the entire enterprise IT ecosystem and those that depend on it – driving increased data quality and providing more relevant inputs to applications such as self-service analytics tools. Both regulatory compliance and effective leverage of data share the common requirement of granular data control, which needs to be addressed at the architectural level.

But today, regulatory requirements are often approached by the enterprise as a 'checkbox' list of technical requirements that must be fulfilled to obtain compliance for a particular mandate. This approach is neither scalable nor sustainable in a world where privacy and data protection regulation is proliferating, and regional rules are defined by their idiosyncratic nuances.

Data privacy as a concept is largely agreed upon, but the specific rules for ensuring its achievement can vary widely based on jurisdiction. For the enterprise, the implementation of a stand-alone compliance tool for each new regulation that evolves is simply not economically feasible. As a methodology, it is also prone to creating data silos and challenges with data integration. What organizations must increasingly do, as regulations become more numerous and complex, is focus on key data protection and data privacy principles, which are shared across regulatory frameworks.

The common denominator of all data-driven regulation is the requirement for complete, granular control of data within the enterprise IT ecosystem. Organizations cannot protect or provide privacy controls for data if they cannot quickly and consistently locate data, identify and resolve duplicates, accurately associate personal information with identities, and enforce policies. Both structured and unstructured data must be controlled with the same rigor, as today's regulatory definitions of personal data increasingly encompass sources of information that are textual and social in nature, rather than just traditional structured identifiers such as credit card numbers, ID numbers and phone numbers.

Siloed architecture has long been a barrier to this goal of unified control for data. Different applications and repositories each have different capabilities for search and data policy management. Lack of integration prevents the enterprise from obtaining a unified view and access of informational assets. Not only does this create major challenges for meeting regulatory requirements, it also severely limits an organization's ability to leverage data for insight. Survey data conducted in late 2018 found that 'accessing and preparing data' was the most commonly reported barrier to using data platforms and analytics within businesses, with 19% of respondents reporting it as the most significant barrier. In this sense, both reactive compliance capabilities and proactive use of data are two sides of the same data control coin.

Privacy requirements are a business opportunity, rather than a burden

Today's data privacy and data protection requirements, then, should be viewed by the enterprise as an opportunity to optimize data management architecture from the ground up. For many organizations, particularly those that were in traditionally unregulated industries, the attempt to comply with GDPR revealed the true lack of data control that was endemic to IT ecosystems.

That doesn't mean that organizations hadn't felt the pain of insufficient data management capabilities before. Poor data quality, difficulty in gaining a single view of customers, and unnecessary duplicative knowledge worker effort all have been symptoms of this underlying data control disorder. Regulatory mandates simply served as the external impetus for many businesses to seriously reconsider and reassess their data management practices. As data increasingly becomes the enterprise's most valuable asset, it also becomes its biggest risk factor. Complete control of data, both structured and unstructured, is the foundational requirement for the enterprise to defensibly derive value from information.

A shift from data quantity to data quality

The enterprise, in the big-data era, has a persistent phobia of any externally imposed restriction that is perceived to reduce the access to, or the collection of, data. If big data is good, all data must be better – at least the reasoning goes. Key evolutionary trends in computing, such as separation of storage and compute, have made it feasible to collect and store a dizzying array of data sources indefinitely. Most organizations today have a data 'hoarding' philosophy because the economics of modern storage allow for it, and the perception that the data might eventually become useful at some point is pervasive.

Unfortunately for the enterprise, this methodology is directly contradictory to the data minimization principles that are widely shared across many of today's data protection and data privacy regulations. Thus, modern compliance requirements are typically perceived as a major point of friction to the business's overarching strategic objectives, which are to essentially collect and analyze as much data as technologically feasible. It is assumed that the consumer, given more autonomy and control over their data, will share less information. Data minimization principles are assumed to reduce the volume of data available for analysis. Less data, it is assumed, is always a strategic disadvantage.

While this perception is pervasive and is based on a kernel of truth – consumer controls for privacy do, objectively, reduce the volume of data available for unrestricted analysis – it overlooks several inherent benefits. The data control mechanisms that are a core requirement for compliance have broad downstream benefits for data-driven initiatives such as self-service analytics and business intelligence initiatives, because they facilitate the administration of granular data access permissions and allow the enterprise to better understand which informational resources are most relevant and representative of the pressing business questions that need to be answered. With strong data control capabilities, the effects of silos are also minimized, resulting in the ability to aggregate and analyze diverse data sources in a more contextual way.

Data privacy and data protection mandates such as CCPA, effectively, shift the balance of power back from data quantity to data quality. Inherently, the strong data control required for compliance fortifies data quality initiatives, making it easier to identify and resolve duplicate and near-duplicate data. The ability to accurately associate diverse data sources with individual identities, critical for fulfilling data subject rights, is essentially the same construct as customer 360° initiatives. While the data available for unrestricted analysis and processing may be lower in theory, the enterprise will likely find that the pressure to resolve issues with silos will ultimately make more quality data available for analysis.

Consumer trust as a driver of profitability

When consumers or data subjects are given more choices and volition over the use of their data, they may indeed choose to restrict the volume of information that they provide. However, when given these choices and autonomy, trust is fostered. When a trusting relationship is built, more accurate information is volunteered over time. Less obfuscation behavior, such as providing junk email addresses, occurs. Consumer trust, in turn, is correlated with more profitable lifetime relationships, lower churn, and more positive word-of-mouth presence in the market for brands.

As consumers become more aware of the value of their data, and are increasingly given regulatory rights to take control of it, trust will become a competitive differentiator for organizations. Strong data management practices, and the corresponding ability to swiftly fulfil consumer requests for data control and access, are the bedrock of this relationship. Data management, too, is inherently tied to data security capabilities; consumers are acutely wary of headline data breaches. Once a trusted relationship

is established, consumers are more willing to selectively and voluntarily share accurate personal data in exchange for perceived valuable benefits, such as special offers and highly personalized recommendations. The crux here is that consumers, to be motivated to share their accurate personal data in the privacy regulation era, must believe they are getting something of equal value in return – the relationship is transactional.

Current enterprise data analysis trends and the intensifying regulatory landscape bring the issue of consumer trust to the forefront. Survey data from late 2018 found that consumer behavior data is still the most popular data source for analysis, with 58% of enterprise respondents reporting that their organization analyzes it. These organizations are at inherently higher risk of running afoul of data privacy and protection regulations' restrictions on the processing of personal data, and are additionally at risk of raising the ire of increasingly privacy-aware consumers.

Achieving data control, from the ground up

Data control, in summary, is the common requirement for both reactive compliance and proactive data leverage capabilities. It is also, ultimately, essential to building the trust with consumers that drives long-term profitability. If the enterprise is to strategically fulfil compliance requirements while maintaining the ability to competitively maximize the insight it derives from data, to the extent allowed by regulations, it must optimize its data management architecture and strive toward a unified view of data.

This runs contrary to the procurement methodology that many organizations have taken when faced with new regulatory requirements. It is tempting to break down regulations into a list of their respective technical requirements, and purchase a specialty tool (or set of tools) capable of helping achieve them. This ultimately is a temporary approach that doesn't address the much more difficult and enterprise-wide challenge of underlying architectural optimization. Worse, a narrow 'solution' approach to compliance can exacerbate existing architectural challenges, spawning additional silos and making data integration more difficult.

For long-term competitive viability in the data protection and privacy era, organizations today must begin striving toward data control that is achieved from the bottom up via architectural optimization, rather than top down with individual tools. This isn't just a technology problem; it is a people and process challenge as well. The control of data, today, has many more diverse stakeholders than the past, when IT was primarily responsible for architectural and platform decisions. Communication is key, and alignment of objectives at the highest level (with accompanying executive sponsorship) is critical.


A hard pill to swallow, but the medicine must not be diluted

CCPA is an opportunity to set a high standard and example for other jurisdictions. It is an opportunity to push businesses towards the proper course of action in adopting frameworks for the responsible management and stewardship of personal data. To weaken CCPA, even at the behest of powerful business interests, is ultimately doing a disservice to the public and businesses themselves. While corporations may currently view privacy and data protection regulation as a threat or burden, it is because they have not fully assessed or comprehended the long-term benefits that come from the responsible management of data. These businesses will not adopt best practices in absence of regulation. Therefore, it is critical that the standards set initially forth CCPA not be weakened or compromised.

Data is becoming the lifeblood of business, and we increasingly live in a “winner take all” economy where the ownership and exploitation of massive amounts of personal data allows incumbent corporations to grow more powerful and monopolistic, blocking out smaller, innovative organizations with a high barrier to entry into the data-driven economy. If California truly wants to foster healthy competition and business opportunity so that it can remain a hotbed of innovation – the Silicon Valley ethos -- restrictions on the use of personal data will increasingly be necessary. CCPA, as written, is a step in the right direction. It will empower consumers, and force businesses to adopt data management practices that, while potentially initially cumbersome, will ultimately accelerate business outcomes and performance, helping California continue to compete in the global economy. For this reason, it is critical that the law not be weakened.

Paige Bartley

Senior Analyst, 451 Research



Message

From: John Lewis [REDACTED]
Sent: 3/8/2019 5:37:10 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Mickie Ornellas [REDACTED] Lance Suder [REDACTED]
Subject: CCPA question

Our customers are first party lenders and their third-party vendors doing debt collection. They are all using consumer data that they gather and put in our system under GLB guidelines. As a software company storing this data, if a California consumer comes to us are we required to disclose the information our customers gathered on that consumer under GLB guidelines, or does the GLB exemption apply to us as well?

John Lewis
Founder/CEO
[REDACTED]
[REDACTED]

Message

From: Stuart Gross [REDACTED]
Sent: 2/28/2019 9:56:02 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA recommendation
Flag: Follow up

PS: revised
Sent from my iPhone

In the spirit of CCPA I would like to propose that you consider including in the Rules the requirement that every application and Website that uses GPS location, provide three options for GPS Access:

- 1 Never. (Required option)
- 2 Always access GPS (May offer option)
- 3 Only while Using the APP or Website (required option)

Stuart Gross
[REDACTED]

Begin forwarded message:
Subject: Comments on CCPA

In the spirit of CCPA I would like to propose that you consider including in the Rules the requirement that every application that uses GPS location, provide three options

Never Access GPS
Always access GPS

Only Access GPS while Using the APP

Thanks,

Stuart Gross
C-LevelIT Solutions

Sent from my iPhone

Sent from my iPhone

Message

From: Sweeney, Margaret [REDACTED]
on behalf of Friel, Alan L. [REDACTED]
Sent: 3/8/2019 4:51:10 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Friel, Alan L. [REDACTED]
Subject: CCPA Rule-Making Comments
Attachments: Letter to CA Department of Justice Re CCPA Rule Making Comments.pdf

Good Afternoon,

Attached please find our CCPA Rule-Making comments.

Thank you

Alan L. Friel | Partner | BakerHostetler

11601 Wilshire Blvd. | Suite 1400
Los Angeles, CA 90025-0509
[REDACTED]

600 Anton Blvd. | Suite 900
Costa Mesa, CA 92626-7221
[REDACTED]
[REDACTED]

bakerlaw.com

This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.


Any tax advice in this email is for information purposes only. The content of this email is limited to the matters specifically addressed herein and may not contain a full description of all relevant facts or a complete analysis of all relevant issues or authorities.

Internet communications are not assured to be secure or clear of inaccuracies as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. Therefore, we do not accept responsibility for any errors or omissions that are

present in this email, or any attachment, that have arisen as a result of e-mail transmission.

Baker&Hostetler LLP

11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509


www.bakerlaw.com

Alan L. Friel


March 8, 2019

Via U.S. Mail and Email:
PrivacyRegulations@doj.ca.gov

CA Department of Justice
Attn: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Re: CCPA Regulations

To Whom It May Concern:

BakerHostetler LLP has one of the nation's leading privacy and data security legal practices as recognized by numerous rankings and awards, including four-time *LAW360* privacy and data security practice group of the year. We represent businesses of all sizes, and in most industries, directly affected by the California Consumer Protection Act (CCPA). During counseling of clients on CCPA preparedness, we have identified various questions, ambiguities and issues that could be addressed through the attorney general's (AG) broad regulatory authority under the CCPA. We outline some of those and organize our comments by reference to the applicable sections of the CCPA that provide the AG rule-making authority. These comments do not necessarily reflect the opinions or concerns of all of our clients, and not all of our clients that have contributed to these comments necessarily join in all of them. These comments also do not reflect a position statement by the firm.

I. RULE-MAKING

A. Under its authority pursuant to Section 1798.185 (a)(4), the AG should promulgate rules and procedures as follows:

- "To facilitate and govern the submission of a request by a consumer to opt out of the sale of personal information pursuant to paragraph (1) of subdivision (a) of Section 1798.145 [sic]."¹ (Section 1798.185(4)(A).)

¹ The correct reference would seem to be to .135(a)(1).

- While changing the text of the homepage link might seem to require legislative action,² Section 1798.185(a)(b) supports the AG’s authority to promulgate regulations that further the purposes of the title by providing businesses with the flexibility to use different language indicative of data subject rights and choices (e.g., “Privacy Choices”) or add text to give broader application (e.g., “Privacy Choices (e.g., Do Not Sell My Personal Information)”), and giving businesses the flexibility to have that link resolve to a privacy rights and choices page that provides notices and choice tools in addition to the CCPA’s “do not sell” right for California consumers (i.e., a data subject rights management portal). This would further the overall purposes of the title – namely, effectively and efficiently informing consumers of their privacy rights and making it easy for them to understand and exercise those rights. The AG could also harmonize CCPA homepage notices with Shine the Light Act homepage notices under such a general choices link, which would also further the overall purposes of the title.
- “To govern business compliance with a consumer’s opt-out request.” (Section 1798.185(4)(B).)
 - Section 1798.115(d) governs the obligations on a third party regarding personal information that has been sold to it: “A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.” Section 1798.120 provides for a business’ do-not-sell notice and request response obligations. However, since the recipient of sold personal information (i.e., the buyer) might not meet the definition of a business, and .120 does not mention the obligations of buyers (i.e., third-party recipients) of sold personal information, it is not clear that the obligations of .120 apply to all buyers (i.e., a third party that is not also a business) of personal information in a sale, and might even be read as imposing the obligation to stop downstream sales absent notice and opportunity to opt out on the selling business, after it receives a do-not-sell opt-out, rather than on the buyer. The AG could resolve this ambiguity and clarify that upon a sale, the obligations under .115(d) and .120 apply solely to the buyer (i.e., party that received the personal information via a sale) and not to the seller. While the seller may agree with the buyer to pass through the buyer’s notice and opt-out opportunity, it should not be

² If the AG concludes so, it is suggested that the AG seek amendment to permit more flexibility in the text of the homepage link to data subject rights information and tools, especially since there may be many other states that follow with their own consumer privacy laws that may differ from the CCPA, and that such amendment revise Section 1798.83(b)(1)(B) of the Civil Code to have such link also satisfy the homepage link provisions of the Shine the Light Act. A better way to distinguish between a general privacy policy and special data subject rights under the CCPA, and other laws, would be “Privacy Choices” or something similarly simple and generic.

required to do so, and it should not be liable if the buyer should improperly engage in downstream sales without doing so.

- The do-not-sell right, sometimes referred to in the title as an opt-out, is an opt-in for children under age 16 as set forth in Section 1798.120(c). That section refers to “consumers between 13 and 16 years of age” to refer to the group of children who can exercise that right themselves as opposed to having the consent exercised by parent or guardian. The AG should clarify that this means from age 13 to age 16 and not merely 14- and 15-year-olds; otherwise, 13-year-olds are left out entirely.
- “For the development and use of a recognizable and uniform opt-out “button” by all businesses to promote consumer awareness of the opportunity to opt out of the sale of personal information.” (Section 1798.185(4)(C).)
 - Use of this button should satisfy the homepage and privacy notice “Do Not Sell My Personal Information” link obligations,³ as long as that link is on the first page to which the button resolves.
 - Since the CCPA does not pre-empt the Shine the Light Act, this button could also be deemed to satisfy the “Your CA Privacy Rights” homepage link provisions,⁴ as long as that link is on the first page to which the button resolves.
 - The button should be short and simple (e.g., “Privacy Choices”) and be permitted to apply to more than just California if desired by the business.

B. “Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter.” (Section 1798.185(a)(6)).

- Businesses will struggle to meet the pre-collection notice requirements of Section 1798.100 (b) unless the AG provides that compliance with this requirement shall depend on the practicality of providing notice given a collection method and medium. For instance, it should be reasonable and sufficient notice to (1) rely on notices in online privacy notices on homepages or app settings menus for all data practices described therein via that online service, and (2) to allow other parties collecting personal information in connection with such online services to pass notices through to users via a service operator by including notice of and links to that other party’s privacy notice in the operator’s privacy notice, provide a URL address to an online privacy policy where written notice is impractical (e.g., call

³ Section 1798.135(a)(1).

⁴ Civil Code Section 1798.83(b)(1)(B).

center audio disclosures at the beginning of a call, or in text, chat app and other short-form communications), and provide signage at brick-and-mortar locations (e.g., surveillance cameras, point-of-sale devices).

- The provisions regarding reasonable financial incentive, and reasonable differential pricing and services, exceptions to the prohibition on discrimination based on CCPA rights exercise of Section 1798.125(a)(2) and (b)(1) discuss reasonableness in context of “value provided to the consumer by the consumer’s data.” This arguably suggests a consumer-specific subjective determination, which would be practically impossible. To meet the purposes of the title, the AG’s regulations could specify that this value determination can be met by any reasonable objective measures, including costs and benefits to the business itself, and that where there is no good objective measure, the mere offering of a choice to consumers should be presumptively reasonable.
- C. “Establishing rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer’s or the consumer’s authorized agent’s ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business’s determination that a request for information received by a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business’s authentication of the consumer’s identity, within one year of passage of this title and as needed thereafter.” (Section 1798.185(a)(7).)⁵
- Businesses should be given broad flexibility in designing verification policies and procedures that are reasonably designed to minimize the need to collect any additional personal information beyond what has already been collected and to disregard or deny requests that cannot be reasonably verified based on such data limitation principle. To the extent the regulations require collection of additional personal information to verify a requesting party’s identity or residency, the regulations should provide that the business may maintain that information for record keeping.

⁵“‘Verifiable consumer request’ means a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer’s behalf. (Section 1798.140(y)).”

- To the extent the AG promulgates regulations providing what constitutes sufficient verification, businesses should be provided a safe harbor from any liability that might arise out of following such regulations (e.g., claims by a data subject that was impersonated by a party that was able to meet the verification standards of the regulations).
- D. “The AG may adopt additional regulations as necessary to further the purposes of this title.” (Section 1798.185(b).)
- The definition of “consumer” can be read to include nonconsumers such as employees, contractors and business-to-business contacts. This seems inconsistent with the consumer protection purposes of new Title 1.81.5 and conflicts with the existing California privacy and security provisions in Title 1.81 that it supplements, as well as other California privacy law. This could be resolved by further refining the definition of “consumer” to harmonize it with “customer” as defined in Title 1.81 (Data Records; Security and Breach)⁶ and in the Shine the Light Act provisions thereof,⁷ and/or “consumer” as defined by the California Online Privacy Protection Act.⁸ Our clients have expressed myriad likely unintended consequences if employees can be read into the definition of consumer, including providing access to security logs, general email databases and confidential information. We note that the legislature has carefully crafted employee rights to access their personal information under the Labor Code to balance the interests of employees, businesses and other parties. An expansion of the definition of consumer to include employees and contractors would disrupt this balance and would not further the purpose of the title.
 - The use of the undefined term “households” creates problems when used in the definition of personal information. It could be read to suggest that a consumer is entitled to access to and copies of personal information of household members, which would violate those members’ privacy. Use of “household” in Section 1798.140(c)(1)(B) suggests that personal information on non-California residents is to be counted toward the 50,000 pieces of personal information collected that is required in order to meet business coverage thresholds. The same problem

⁶ “Customer” means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business. Civil Code Section 1798.80(c).

⁷ “‘Customer’ means an individual who is a resident of California who provides personal information to a business during the creation of, or throughout the duration of, an established business relationship if the business relationship is primarily for personal, family, or household purposes.” Civil Code Section 1798(e)(1). “‘Established business relationship’ means a relationship formed by a voluntary, two-way communication between a business and a customer, with or without an exchange of consideration, for the purpose of purchasing, renting, or leasing real or personal property, or any interest therein, or obtaining a product or service from the business, if the relationship is ongoing and has not been expressly terminated by the business or the customer, or if the relationship is not ongoing, but is solely established by the purchase, rental, or lease of real or personal property from a business, or the purchase of a product or service, and no more than 18 months have elapsed from the date of the purchase, rental, or lease.” Civil Code Section 1798(e)(5).

⁸ “The term ‘consumer’ means any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes.” Business and Professions Code Section 22577(d).

applies to the use of the term “devices” without reference to California residents. The AG’s regulations must provide clarity needed to resolve these issues.

- The CCPA is internally inconsistent as to whether or not the online notice needs to include the categories of sources from which personal information is collected, the categories of third parties to which personal information is disclosed and the specific pieces of personal information collected about a specific consumer. This should be clarified. Obviously, the last could not practically be done in a general notice, and doing so would be contrary to the privacy purposes of the title.
- Businesses must list the categories of personal information disclosed for a business purpose in the preceding 12 months (or if the business has not disclosed consumers’ personal information for a business purpose in the preceding 12 months, the business must state that). However, there is no obligation to include a list of categories of personal information disclosed for a commercial purpose in the preceding 12 months. This distinction between the underlying purposes does not apply with respect to categories of personal information collected; it applies only to categories of information disclosed. The AG could clarify that there is no need to provide categories of personal information disclosed for a commercial purpose.
- The CCPA permits transfers to a third party of personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with Sections 1798.110 and .115. If the recipient in such a transaction materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it needs to provide to the consumer prior notice of the new or changed practice. However, Sections 1798.110 and .115 are the sections that set forth notice and disclosure requirements of consumer rights under the CCPA regarding businesses that collect personal information, sell personal information or disclose personal information for a business purpose. Presumably, the intent is that the data will continue to be used and shared as described in the privacy policy or notice that included those CCPA rights disclosures. The AG’s regulations could confirm that and resolve the current ambiguity.
- The definition of business includes “[a]ny entity that controls or is controlled by a business, as defined in subparagraph (1), and that shares Common Branding [‘shared name, servicemark, or trademark’] with the business.” As such, the CCPA essentially requires all the members of a similarly branded family of companies that have an entity that meets the definition of a business to also be treated as a covered business. It is arguably not clear whether the intent is that the commonly branded entities must or can be treated as a single business under the

CCPA. The AG should clarify that the intent of Section 198.140(c)(2) is only to bring such an entity under coverage as a business even if it would not otherwise meet the conditions of .140(c)(1)(A)-(C). The AG's regulations could further clarify that such a business, or any other affiliate or subsidiary of a business, may elect to "roll up" to be treated as a single business, or to be separately treated as a distinct business, for CCPA purposes, so long as each business meets the controller requirements of .140(c)(1)(i.e., "determines the purposes and means of the processing of consumers' personal information"). In this regard, a family of companies is treated as a distinct business for CCPA notice and consumer rights response purposes if there is unitary control of the group's consumer personal information, but if affiliates maintain independent control they are separate businesses for CCPA purposes.

- Section 1798.140(c)(1) does not address what happens when a company meets one of the thresholds of (A)-(C). Given the title's 12-month look-back provisions, this could create an impossible burden for a business if application were immediate when a company that was not previously subject to the title later becomes subject. The AG's regulations could provide a grace period for compliance, such as beginning 12 months thereafter.
- The definitions of "business," "collect" and "sale" need to be reconciled when it comes to who is responsible for a business or other party collecting personal information in a manner that has some association with another business or its consumers. Examples include a solicitation firm collecting consumer personal information (e.g., for petitions or product marketing) on the property of a retailer (e.g., in front of the store or even at a booth in-store) or a cookie operator collecting IP addresses and other data from visitors to a retailer's website on which the cookie is associated. Because the definition of sale is "making available ... a consumer's personal information" and not "making available access to a consumer from whom personal information is collected by another party," the determinative factor should be which party controls the actual collection, not the access to the consumer. In both cases above, the solicitor and the cookie operator control the means and methods of collection, even though they would not be able to collect the personal information but for the ability to reach out to the retailer's consumers. This interpretation is consistent with the purpose of the title – namely, to make controllers responsible for the data they collect and control. To take a broader interpretation could have many unforeseen consequences. Practically, some parties controlling certain data collection, such as the cookie operator, may need to pass their pre-collection and other notice obligations through to the consumer with the assistance of another party, such as the website publishers on whose sites they associate their cookies, but that is a matter of the controlling collector implementing its obligations and not of which party controls the means and methods of collection. If the AG were to conclude

otherwise, then it should make its interpretation clear given the current ambiguity regarding this important issue.

- Under the CCPA, “sell,” “selling,” “sale” and “sold” are defined as “selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating a consumer’s personal information to another business or a third party for monetary or other valuable consideration.” Section 1798.140(t)(1). Arguably, any arrangement or agreement between two parties has to have an exchange of valuable consideration in order to be valid, and the proposition that personal information has value is arguably inherent in the title. Accordingly, the AG could resolve ambiguity regarding under what circumstances non-monetary consideration would make a disclosure of personal information a sale. Further, even monetary consideration should not trigger a transaction that includes the transfer of personal information as being a sale unless the consideration (monetary or otherwise) is directly attributable to, and in direct consideration for, the acquisition of personal information for the buyer’s own commercial purposes, as opposed to other business arrangements where the personal information is not the direct subject of the exchange of consideration. For instance, the definition of third party specifically excludes third parties that do not meet the requirements of the definition of service provider (Section 1798.140(v)), which receive personal information for a business purpose pursuant to a contract that limits the use to providing services to the disclosing business for such business purposes and includes other usage and disclosure limitations and a specific certification of compliance. (Section 1798.140(W)(2).) However, unlike qualifying service provider disclosures that are carved out of the definition of sale at Section 1798.140(t)(2)(C), these exempt third-party disclosures are not specifically carved out of the definition of a sale. The engagement by a business of such a vendor has to have an exchange of consideration in order to be valid. That cannot logically mean, however, that a disclosure to such an exempt third-party vendor, where the title’s contractual and certification requirements are met, is a sale because there was consideration to support the engagement. Rather the only logical interpretation of consideration (monetary or nonmonetary) for the purpose of designating a transaction as a sale is where (1) the recipient is allowed to use the personal information for its own and/or third-party commercial purposes; and (2) the consideration is given directly in consideration of the recipient’s ability to use the personal information for its own and/or third-party commercial purposes. At a minimum, the AG’s regulations should clarify that disclosure to a party exempt from the definition of a third party under Section 1798.140(t)(2)(C) is not a sale.
- A business does not “sell” personal information under the CCPA when a consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that

disclosure would be consistent with the provisions of the title. (Section 1798.140(t)(2)(A).) However, a business cannot control what the recipient does or does not do. In order for this provision to be relied on, the AG’s regulations could provide that a business may rely on a commitment from the recipient not to sell the personal information, unless otherwise consistent with the title, in facilitating a consumer’s directions to a business to share personal information.

- The CCPA will regulate “personal information,” broadly defined as “information that identifies, relates to, describes, *is capable of being associated with or could reasonably be linked, directly or indirectly* with a particular *consumer or household*.” (Section 1798.140(o).) Arguably, all data about a person is *capable of being associated with* a particular consumer or household. For instance, demographic data (e.g., gender, profession, race) is capable of being associated with a person, but alone, it will not reasonably enable their identification or be reasonably linked to a specific person. Compare this with the definition of personal information under Title 1.81 of the California Civil Code, which includes California’s customer records security and breach laws, and the Shine the Light Act’s marketing transparency and choice requirements. In that title, there is a top-level definition of personal information that includes “any information ... capable of being associated with a particular individual” to which the duty of reasonable security under the circumstances applies, but more narrow definitions are used regarding a customer’s rights regarding sharing for third-party marketing purposes (“any information *that when it was disclosed identified, described or was able to be associated with* an individual....”) and regarding the type of data that will trigger a breach notification obligation (first initial or name and last name plus an account number or ID number and password). While a broad definition arguably has utility with respect to providing notice of what data is collected, when applied to what data is disclosed or sold, and even more so as applied to opt-out, portability and deletion rights, it is practically unworkable. This problem is made worse by the CCPA’s ambiguities regarding deidentified data and aggregate consumer information, discussed below. The AG’s regulations could resolve this issue and further the purposes of the title by clarifying that “capable of being associated with” means “is able to be associated with an individual in the context of its use or disclosure.”
- The definition of personal information under the CCPA does not include publicly available information. (Section 1798.140(o)(2).) “Publicly available” is defined as “information that is lawfully made available from federal, state or local government records, *if any conditions associated with such information*.” (emphasis added.) The italicized language seems to be a typo or an incomplete thought that the AG’s regulations could complete. Further, under the title, information is not “publicly available” if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. Under the

Freedom of Information Act and state equivalents (e.g., California Public Records Act), all but the most sensitive government records are available to the public for any purpose. Because the uses by a business of public information may differ from the exact government collection purpose (e.g., property title records to establish land chain of title, but used by business for marketing or fraud prevention purposes), a narrow interpretation of this definitional carve-out from personal information would be inconsistent with our system of public access to government records. The AG’s regulations could clarify that any purpose for use of government records not prohibited by applicable law is a compatible purpose for purposes of .140(o)(2).

- Also included in .140(o)(2)’s provisions regarding what is not personal information is deidentified data and aggregate consumer information, suggesting that these types of data are intended to be excluded from the definition of personal information, but this is unclear as the title is currently worded. The CCPA states “‘Publicly available’ does not include consumer information that is Deidentified or aggregate consumer information.” The intent is likely to have used “personal information” rather than “publicly available,” given the context. Further, Section 1798.145(a)(5) provides that “[t]he obligations imposed on businesses by this title shall not restrict a business’s ability to ... collect, use, retain, sell or disclose consumer information that is deidentified or in the aggregate consumer information.” This would seem sufficient to remove deidentified and aggregate consumer information from the data applicable to deletion and do-not-sell rights. Practically, portability rights would also not apply, especially since the CCPA provides that there is no obligation to re-identify deidentified data “not maintained in a manner that would be considered personal information.” However, the other obligations regarding personal information would seem to apply unless the definition of personal information is not clarified to exclude deidentified and aggregate consumer information, which would seem consistent with the intent and purposes of the title. Also, the definition of deidentified suffers from the same problem as the definition of personal information – data “capable of being associated with ... a particular consumer,” which could be cured by taking a narrower approach as already suggested as regards personal information.
- Section 1798.130(a)(2) provides the detail on how to comply with the data portability right outlined in Section 1798.100(d). Section .130(a)(2) provides that the data portability covers only the prior 12 months, i.e., anyone holding an account for more than 12 months preceding the request. However, .100(d) does not include that limitation. The AG should clarify that .130(a)(2) qualifies .100(d) and that they are not independent disclosure obligations.
- Section 1798.105(b) provides broad exceptions to a consumer’s deletion rights under Section .105(a), including broad “catchall” provisions in subsections (7)

and (9). However, like most catchall provisions, the broad language lacks clarity and the AG could provide guidance as to what would and would not be included therein. It is suggested that in doing so, regulations apply the concept of legitimate interest and provide that any retention based on a good faith belief in a legitimate interest for retention shall be permissible so long as the use is limited to that purpose.

- Section 1798.150(a)(1) provides a limited private cause of action for certain types of, but not all, data security breaches (reference is made to a more narrow definition of personal information under Title 1.81 used there for breach notification purposes) in the case of “unauthorized access and exfiltration, theft, or disclosure as a result of the business’ violation of the duty to implement and maintain reasonable security procedures and practices.” The AG’s regulations should clarify whether “unauthorized” applies to all the following conditions, or only some (i.e., whether it applies to both access and disclosure). The AG’s regulations could also clarify the cure provisions of Section 1798.150(b). The CCPA has no express duty regarding data security; those are in Title 1.81. Thus, the reference to the consumer notice to the business of “the specific provisions of this title the consumer alleges have been or are being violated” and an opportunity to cure that breach is confusing -- a remnant of an earlier broader private right of action that was rejected during the legislative process. The AG’s regulations could rectify this by providing that this means providing notice of the alleged unreasonable security that allegedly resulted in the alleged triggering incident. Further, a consumer’s CCPA cause of action is limited to data security failures that resulted in a breach, so it would seem that the only way to provide a meaningful opportunity to cure would be to rectify the security inadequacy on a prospective basis, since retrospective cure is an impossibility. This interpretation is also the only way to give purpose to the provision that the cure be documented by a written remediation and prospective compliance commitment, and that a breach of that written cure statement will revive the ability to seek statutory damages. The AG’s regulations can clarify the intent of this provision and better detail the process for cure.
- Section 1798.155(a) provides the right of businesses to seek the opinion of the AG for guidance on how to comply with the title. It is suggested that the regulations provide that if a business does so and articulates a good faith basis for an interpretation of the title, the AG may not bring an enforcement action based on a contrary interpretation until 30 days after it has given the business notice of the contrary interpretation and a demand to cure. In addition, it is suggested that the regulations provide that the cure notice that the AG is required to provide a business under Section 1798.155(b) before the AG is authorized to commence an enforcement action include a reasonable description of what is required of the business to effect a sufficient cure. Such regulations guiding the opinion and

notice of cure obligations of the AG further the purpose of the title by prioritizing compliance (i.e., “fix it”) over punishment (i.e., “gotcha”), especially as to businesses that can be shown to have acted in good faith.

- Given that the enforcement delay is until the earlier of July 1, 2020, or six months from the promulgation of the final regulations, and the AG has until July 1, 2020, to issue final regulations, it is possible that enforcement could commence with little or no time between the date the regulations are finalized and commencement of enforcement. Accordingly, it is suggested that the regulations provide for a further enforcement delay of six months from the final regulations with respect to any issue that is based on the regulations as opposed to clear from the four corners of the title.

II. CONCLUSION

We appreciate the opportunity to make comments for your consideration and look forward to participating in the formal rule-making process. If you have any questions regarding these comments, please feel free to contact me at 310.860.8860.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'A. Friel', with a stylized, overlapping loop at the end.

Alan L. Friel
Partner

Message

From: Anthony Witkowski [REDACTED]
Sent: 3/7/2019 8:36:21 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA Rulemaking Comment

Hello,

I am a law student at Northeastern University. I am curious how the CCPA provision 1789.150 interacts with the California data breach law 1798.82. There are two Assembly Bills proposing amendments to 1798.82, one of which (AB 1130) also amends 1798.81.5, which is the PI definition used in the CCPA section 1798.150.

Should the amendments pass, it would align the definitions of PI under the two sections, but it is unclear if all "unauthorized access and exfiltration, theft, or disclosure as a result of a business' s violation of the duty to implement and maintain reasonable security procedures and practices..." would also be considered a "breach of security" under 1798.82.

Finally, I am also curious if the allowance to delay data breach reporting to identify scope & restore integrity could be used to delay a report to ensure that no private citizen, upon receiving notice, could institute the private right of action in 1798.150 because the company would just wait until they have "cured" the issue to send the report.

Thank you for your time in assessing my comments.

Kind regards,

Anthony Witkowski
Northeastern University School of Law
JD Candidate 2019

Message

From: Annalee Akin [REDACTED]
Sent: 3/8/2019 4:39:10 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Mike Belote [REDACTED]
Subject: CCPA Rulemaking Comments
Attachments: CCPA Comments from California Advocates.pdf

Good afternoon,

Attached are comments on the CCPA rulemaking from Mike Belote, President of California Advocates.

Best,

Annalee

Annalee Akin

Legislative Assistant

California Advocates, Inc.

925 L Street, Suite 1250

Sacramento, CA 95814





March 8, 2019

Michael D. Belote

Dennis K. Albiani

Faith Lane Borges

Erinn P. Ryberg

Anthony Molina

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

RE: CALIFORNIA CONSUMER PRIVACY ACT RULEMAKING

Dear Privacy Regulations Coordinator:

We have discussed the rulemaking process for the California Consumer Privacy Act with various clients represented by our firm, and appreciate the opportunity to provide input. The right to privacy is not only a right enshrined in the California Constitution, but a fundamental human right that should be respected by all persons, legal and natural, regardless of where they are in the world. We applaud this effort by California to lead by example in passing the CCPA and establishing baseline privacy standards for California consumers and companies.

The CCPA introduces a number of new, valuable privacy rights to individual consumers. While our clients support the goals of the legislation, we believe that both clarity and guidance is necessary to help companies operationalize the law and to help consumers understand what steps to take to exercise their rights. We further encourage the Attorney General to evaluate whether and to what extent guidance can be drafted that allows for meaningful privacy protections and rights while providing sufficient flexibility for businesses to innovate and takes into account the ever-changing world of technology today; what makes good sense in light of today's technologies may not make sense in five years and is highly likely to face robust hurdles in ten. We respectfully ask that that California Attorney General consider the comments below in its rulemaking process.

To Support the CCPA's Transparency Goals and Evolving Technologies, the CCPA Rules Should Provide Businesses with Sufficient Flexibility for Describing Personal Information in Privacy Notices.

We support the goal of ensuring that consumers receive clear notice of business's privacy practices. We do not, however, feel that presenting information according to prescriptive categories is the best or only way to meet the requirements of and protecting the privacy rights of individuals to meaningful notice and transparency.

The CCPA requires that businesses provide consumers with notice as to what personal information they collect and why, with whom they share the personal information, and to whom the personal information is disclosed. It then goes on to request that, for each of collection, sale, and disclosure, the business organize the personal information “by reference to the enumerated category or categories in [the definition of personal information].” While consistent privacy notice formatting across businesses can in some instances be helpful, we have concerns that an unnecessarily strict implementation of this requirement will result in consumers receiving confusing and ultimately unhelpful information, contrary to the goals of the CCPA:

First, the required organization is highly likely to result in long, unnecessarily complicated privacy notices, directly contrary to the goals of the CCPA. First, requiring three separate lists of personal information, one for collection, one for sale, and one for disclosure, each organized by reference to prescriptive categories of personal information will result in lengthy privacy policies that no consumer is likely to read. Second, it eliminates the incentive for businesses to innovate meaningful privacy notices such as just-in-time disclosures, or novel disclosures for small screens, thereby reducing the likelihood that privacy rights and technologies will progress along with the underlying sciences. Third, requiring businesses to organize the information according to the prescriptive categories and not by services or products, will result in increased consumer confusion. For example, assume that an individual signs up for an email service, a photo sharing service, and an online cloud account with a business. Providing that individual with a list of email addresses that the business has in its records that relate to the individual does not tell the individual from where the email address was collected or what service it is associated with. If one of the email addresses was outdated and the individual wanted to update the email address, the individual would need to access each account and look for the outdated email address. Were there flexibility to provide meaningful information in a clear and easily understandable way, the business could have organized the information by service and, within that service, in a clear manner, rather than presenting the consumer with non-non-intuitive lists of data.

We also have concerns stemming from the significant breadth and overlapping nature of some of the enumerated categories in the CCPA’s definition of personal information. For example, section 1798.140(o)(1)(B) includes “[a]ny categories of personal information described in subdivision (e) of Section 1798.80.” The cross-referenced section of the California Civil Code includes “any information that identifies, relates to, describes, or is capable of being associated with, a particular individual.” As a result, it essentially includes all information that qualifies as personal information under the CCPA. Therefore, any type of personal information falls arguably within this category. Additionally, the category directly overlaps with other enumerated categories of personal information. For example, section 1798.80(e) refers to name, telephone number, and passport number,

all of which are expressly referenced in the “identifiers” category of the CCPA’s definition of personal information (category (A)). The CCPA does not provide guidance as to how businesses should describe categories of personal information “by reference to” the enumerated categories when the relevant personal information falls into more than one of the enumerated categories.

In addition, a reference to “section 1798.140(o)(1)(B) of the California Civil Code” is unlikely to have any meaning to an average consumer. Therefore, a consumer that reads a privacy notice or receives a disclosure from a business that states that the business collects this category of personal information is not likely to gain meaningful information. The Attorney General has the ability to and should issue clarifying guidance that this category should only be used where the personal information falls under no other category and, where personal information would fall into this category, a meaningful plain language descriptor should be used to communicate the type of personal information, rather than “section 1798.140(o)(1)(B) of the California Civil Code.”

We are further concerned that broad categories and lack of guidance about how they should be used also create the risk that businesses will provide consumers with vague, high-level information that does not allow a consumer to truly understand the collection and use of their personal information. For example, a business could collect and use various personal information data elements that fall into the “identifiers” category, such as name, email address, and social security number. These data elements vary significantly in sensitivity. However, a business could potentially refer to these different data elements by using the category “identifiers” and, as a result, the consumer would not have a reasonable awareness of how the different data elements are being collected or used. We encourage the Attorney General to draft rules that allow businesses to provide greater clarity so that truly meaningful information about privacy practices will be conveyed to the consumer.

To avoid forcing businesses to provide consumers with potentially confusing and unhelpful information, the Attorney General should draft a rule that allows for a more flexible approach to describing personal information in privacy notices. For example, such a rule could provide that businesses that describe personal information in a clear and easily understandable way in the applicable privacy notice are not also required to describe such personal information by reference to the enumerated CCPA categories. This approach would be reasonably harmonized with other leading global privacy frameworks, including the GDPR, which requires that information presented to the public or the data subject be “concise, easily accessible and easy to understand.” It would also be consistent with the Federal Trade Commission’s guidance, as the agency has long encouraged businesses to use shorter, clearer language in privacy notices and other

required disclosures to enhance consumer understanding, including for example through layered and just-in-time notices.

An additional benefit of a more flexible clear and easily understandable standard for describing personal information is that it would allow businesses to use innovative new ways to present information to consumers that can keep pace with evolving technology. Given the wide range of information that some businesses may collect from consumers, and the potential for new types of information to be developed in the future as technologies evolve, it is important that privacy regulations such as the CCPA rules remain flexible over time. Requiring the use only of the enumerated personal information categories would lock businesses into an unnecessarily prescriptive approach to describing personal information that may not fit with future technology developments.

Therefore, to support the CCPA's transparency goals and the continued development and deployment of innovative technologies, the Attorney General should confirm that businesses that provide the required information regarding data collection and use and do so in a clear and easily understandable way shall satisfy the requirements of the law, even where the information is not organized by reference to the enumerated CCPA categories.

The CCPA Rules Should Also Afford Businesses Sufficient Flexibility in the Manner in Which They Respond to Access, Opt-out, and Deletion Requests so that the Businesses can Meaningfully Effectuate Consumer Intent.

The CCPA rules should confirm that businesses may provide consumers with an additional option to apply their access, deletion, and opt-out requests to a subset of their personal information held by a business.

Currently, the CCPA provides consumers with the right receive information about the "personal information the business has collected;" the right to delete "any personal information about the consumer which the business has collected from the consumer;" and the right to opt-out of the sale of their personal information. However, the CCPA does not indicate whether a business can offer a choice to a consumer that one or more of these actions be applied to only a subset of their personal information. In the absence of further guidance on this issue, it is possible that consumers will face an all-or-nothing choice when deciding whether to exercise their CCPA rights. This could deter consumers from exercising these rights and ultimately undermine the value of the rights for consumers.

For example, under an all-or-nothing approach, a consumer might be seeking personal information related to a specific interest or prior trip. An access request could end up

yielding additional information that is of little practical value to the consumer. And depending on the volume of information subject to the request, providing all of the information would make it more difficult for the consumer to even find the information that he or she actually wants. Similarly, a consumer deletion request could result in the deletion of some personal information that the consumer actually wants to the business to keep (e.g., to continue providing tailored services to the consumer). These outcomes are contrary to the interests of consumers and separately impose an unnecessary burden on businesses seeking to comply with the CCPA.

The Attorney General can help avoid these negative consequences by clarifying that it is permissible for businesses to offer consumers the option to apply their access, deletion, and opt-out choices to a subset of their personal information, provided that consumers still retain the right to request that a business apply their access, deletion, and opt-out requests to the full extent permitted by the text of the CCPA. Such a rule would enhance the goals of the CCPA and provide even more granular consumer control over personal information.

The Attorney General should also clarify what constitutes a “portable” and “readily useable” format.

Currently, the CCPA includes provisions that require certain information to be provided to consumers in a “portable” and/or “readily useable format that allows the consumer to transmit this information to another entity without hindrance.” There is certainly value in ensuring that consumers can easily move their personal information from one service to another. However, additional clarity regarding the meaning of “portable” and “readily useable” is needed to avoid having this requirement become a significant burden that produces unintended negative consequences to competition and intellectual property.

As an initial matter, any obligation to convert files into non-native formats could impose a harmful burden on small businesses and startups that may be less able to spare the financial and human resources needed to convert files for the purposes of fulfilling CCPA requests. Additionally, some businesses may simply be unable to comply with the requirement if they use proprietary technologies that rely on file formats that cannot be readily converted into other commonly used formats.

Importantly, even if a proprietary format can be converted, in some cases there may be a risk that converting all of the information maintained in the proprietary format into a commonly used format could provide competitors with insights that would threaten the security of trade secrets or other intellectual property. Forcing businesses to compromise the security of trade secrets and intellectual property conflicts with the goals of the CCPA drafters, who recognized the need to protect trade secrets and intellectual property from

unintended negative consequences of the CCPA by including 1798.185(a)(3), which calls for the Attorney General to adopt regulations “[e]stablishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights.”

The Attorney General can help mitigate the potential negative impacts of the “portable” and “readily useable” CCPA requirement by drafting a rule that allows for the consideration of at least the following factors when assessing whether a business has complied with the requirement: available technologies, the cost to the business of providing the information in commonly used formats, security concerns, and businesses’ interests in maintaining the confidentiality of proprietary technology.

In connection with the topics addressed above and other areas within the Attorney General’s rulemaking authority, we propose for your consideration the following rules to provide greater guidance and clarity for consumers and businesses working to comply with the CCPA:

Clarity on interpretation of “personal information” to help provide guidance to consumers and businesses and to encourage the development of privacy protective technologies:

For purposes of [the Act], information shall not be considered “personal information” if:

- (a) It is keyed to a non-static identifier;
- (b) It is keyed to an identifier that may be reset by the consumer at their discretion; or
- (c) The business itself cannot use the information to identify, relate to, describe, associate with, or reasonably link to a consumer; *provided*, the business has developed and maintains reasonable and appropriate procedures to prevent use of such information by the business or its service providers to identify a consumer. A contractual prohibition by the business on its service providers on the use of such information by its service providers to identify the consumer shall be presumed to constitute reasonable and appropriate procedures.

Requirements for verifying validity of a request from a consumer to exercise rights under the CCPA:

- (a) Every business shall develop and maintain reasonable and appropriate procedures designed to verify the identity of the person from whom the business receives a request pursuant to [the Act].
 - (1) Such procedures shall be designed to avoid collecting additional personal information from the requestor to the extent practicable.
 - (2) Personal information collected from the requestor in order to verify the identity of the requestor shall be used only for purposes of verifying the identity of the requestor in connection with fulfilling a business’s obligations under [the Act], and for fraud and security purposes.

- (3) A business that receives a consumer request pursuant to [the Act] via an account that the consumer has established with the business for a purpose other than submitting the request, and for which the business provides reasonably appropriate security, may consider such a request to be reasonably verified.
- (b) If the business is unable to verify the identity of the person, the business shall promptly:
 - (1) Deny the request; and
 - (2) Provide the consumer with a notification that the business had insufficient information to verify the request and therefore denied the request.
- (c) If the business is able to verify the identity of the person, the business shall promptly:
 - (1) Fulfill the request; and
 - (2) Notify the consumer that the request has been fulfilled.

Requirements for responding to requests from third parties on behalf of consumers to exercise their right to opt out of the sale of personal information under the CCPA:

- (a) A business that receives a request from a person claiming to have authorization to act on the consumer's behalf to opt out of the sale of the consumer's personal information shall:
 - (1) Verify the identity of the person alleging to have a valid legal authorization establishing authorization pursuant to [citation to regulations regarding identity verification];
 - (2) Verify the person has a valid legal mechanism establishing authorization to act on behalf of the consumer in connection with opting out of the sale of the consumer's personal information;
- (b) If the business cannot verify the identity of the person or verify the person has a valid legal mechanism establishing authorization, the business shall:
 - (1) Promptly deny the request;
 - (2) Provide the consumer with a notification that (i) a person claimed to have a valid legal mechanism establishing authorization to act on the consumer's behalf to opt out of the sale of the consumer's personal information, (ii) the business had insufficient information to verify the request and therefore denied the request, and (iii) the consumer can initiate a request to exercise their rights under [the Act] and information on how or a link to a mechanism for initiating such request.
- (3) If the business verifies both the identity of the person and that the person has a valid legal mechanism establishing authorization the business shall:
 - (1) If executing the request to opt out of the sale of a consumer's personal information would have a material impact on the nature or quality of the service with respect to the consumer promptly notify the consumer, in writing, of the potential material impact, the fact that the consumer may withdraw their request, the time period in which the consumer must withdraw their request which shall not be less than forty-eight (48) hours, and provide a simple mechanism for the consumer to withdraw their request.
 - (A) If the consumer withdraws their request within the noticed time period:
 - (1) The business shall not fulfill the request to opt out of the sale of the consumer's personal information;
 - (2) Promptly provide written confirmation to the consumer and to the person with authorization to act on the consumer's behalf to opt out of the sale of the consumer's information that the request been withdrawn and no action will be taken by the business in response to the request.

- (B) If the consumer does not withdraw their request within the noticed time period:
 - (1) Fulfill the request to opt out of the sale of the consumer's personal information;
 - (2) Promptly provide written confirmation to the consumer and to the person with authorization to act on the consumer's behalf to opt out of the sale of the consumer's information that the request been fulfilled.
- (2) If executing the request to opt out of the sale of a consumer's personal information would not have a material impact on the nature or quality of the service with respect to the consumer:
 - (1) Fulfill the request to opt out of the sale of the consumer's personal information;
 - (2) Promptly provide written confirmation to the consumer and to the person with authorization to act on the consumer's behalf to opt out of the sale of the consumer's information that the request been fulfilled.

Requirements for responding to rights requests, generally: ability for consumers to make granular choices:

- (a) Nothing in [the Act] shall prohibit a business from offering consumers the opportunity to access, delete, or opt out of the sale of a subset of their personal information, provided that the business offers consumers the ability to apply such requests to the full extent permitted by [the Act].

Guidance on portability:

- (a) In determining whether information is in a portable and readily usable format that allows the consumer to transmit this information to another entity without hindrance, the Attorney General shall take into consideration available technologies, the cost of providing the information in commonly used formats, security concerns, and the businesses' interests in maintaining the confidentiality of proprietary technology.

Clarity on nature and method of providing notice and access:

For the purpose of disclosing information to a consumer pursuant to 1798.110 and 1798.115:

- (a) The disclosure must be clear and easily understandable;
- (b) The method of disclosure must be reasonable and appropriate in light of the nature of the service and the sensitivity of the personal information collected to a reasonable consumer;
- (c) A business may disclose the information required by 1798.110 and/or 1798.115 in a single communication or multiple communications; *provided*, however, the nature, timing, and content of the disclosures shall reasonable and appropriate in light of the nature of the service and the sensitivity of the personal information collected to a reasonable consumer. In evaluating whether the disclosures meet the requirements of this section, the following factors shall be considered:
 - (1) Temporal proximity of disclosure to the time at which a consumer may make a decision with respect to the collection, use, or disclosure of their personal information;

- (2) Locational proximity of disclosure to a mechanism the consumer may use to indicate a decision with respect to the collection, use, or disclosure of their personal information;
 - (3) Sensitivity to a reasonable consumer of the personal information collected, used, or disclosed by the business to which the disclosure(s) relates; and
 - (4) Nature of the service provided by the business for which the personal information to which the disclosure(s) relates is collected, used, or disclosed.
- (d) The disclosure(s) shall identify the category(ies) of personal information by reference to a single category that most closely describes the personal information collected using the categories listed in 1798.140(o)(1) unless more than one such category accurately and fully describes the personal information collected, in which case the disclosure shall identify the category that is most easily understandable to a reasonable consumer. Only if multiple such categories are easily understandable to a reasonable consumer shall the business disclose two categories for the same personal information. If no category listed in 1798.140(o)(1) accurately describes the personal information, the business shall instead disclose an accurate, clear, and easily understandable description of the type of personal information.
- (e) In disclosing the specific pieces of personal information, a business shall either:
- (1) Identify by name the specific pieces of personal information using the name that most accurately describes the specific piece of information, for example: Social Security number rather than unique identifier; or
 - (2) Provide the consumer with a copy of the personal information in a portable and readily usable format.

We thank the Attorney General for considering these comments in its rulemaking process.

Sincerely,



Michael D. Belote
President, California Advocates, Inc.

Message

From: Randy Wilson [REDACTED]
Sent: 3/3/2019 6:31:09 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA rulemaking suggestions
Attachments: CCPA_Randy_Wilson.pdf
Flag: Follow up

To whom it may concern:

Thank you for the opportunity to contribute to the rule-making process for the CCPA.

I'm happy to discuss the ideas presented at anytime.

Thanks!

Randy

--

Randy Wilson
RLWilson Consulting

[REDACTED]

[REDACTED]

[REDACTED]

Randy Wilson



March 3, 2019

CA Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.,
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

To Xavier Becerra, Attorney General California,

Thanks for the opportunity to provide input on this important legislation. I am a privacy compliance attorney with CIPP, US/EU and CIPM credentials from the IAPP (International Association of Privacy Professionals.) In addition, I have spent my entire career working with data in a variety of capacities and most recently in a privacy operational setting at top California tech companies. Rulemaking could make or break the success of this legislation. If complying with the CCPA is too onerous for companies, they will not voluntarily comply and enforcement will become impossible given limited resources and the fact that this legislation will impact many thousands of businesses.

As a lawyer and technology professional, I believe that most companies in California will have an incredibly difficult time adhering to this law. While many very large companies have made good faith attempts to adhere to the GDPR, they have struggled mightily to clean their data house and will not be able to rubber stamp that approach onto the CCPA. More significantly many more companies will be required to comply with the CCPA than those adhering to the GDPR (doing significant business in California but not doing business internationally.)

This places significant burden on these rules to make the law a success. It is important to recognize that companies need encouragement as well as penalties if they are to improve their data collection, use and transparency practices. These rules can make it easier from companies to comply with the consumer data rights if the organization wins by improved consumer satisfaction and this in turn builds trust with consumers that their data is being properly protected and respect. If that can happen this legislation will be successful.

Here are a couple specific ways the rules can lead to success:

Use the US Privacy Shield model to certify companies as CCPA compliant

The law doesn't provide a framework for how a company can certify their adherence to basic privacy principles nor how consumers should know if a company is subject to the law. I would look to the [U.S Privacy Shield](#) framework as both a model and perhaps even a source of guidance. Companies that have certified that their privacy programs meet these rigorous standards could be considered subject to

active enforcement by the Attorney General. It would also allow consumer an easy one-stop shop to know who they can make requests to under the CCPA.

All companies that belong to the Privacy Shield receive certification from 3rd parties. Those 3rd parties could be the source for any additional CCPA certification that would be required by existing companies subject to the Privacy Shield and those 3rd parties could then offer similar services to companies that aren't subject to the GDPR but are subject to CCPA. Don't make companies wade through uncertainty and doubt when an existing framework can provide clear and proven guidance for creating robust privacy programs. This will increase adherence to the CCPA and provide greater certainty and confidence to California consumers.

Provide Pre-existing Templates for all Instructions re: 'Categories'

The CCPA requires that companies provide to consumers at least four different categories of information. The most notable are the categories of personal information but the law also specifies categories of sources from which the data is collected, categories of third parties the data is shared with and categories of business purposes.

Rule-making guidance defining these four types categorization would greatly improve the quality of data received by consumers, would provide clear and straightforward guidance to businesses and make enforcement simpler because interpreting whether the categorization meets the requirements would be easier to determine. For example, while the law provides some guidance for the labels for the categories of personal information (found in the 1798.140(o)(1), this should be further refined. How does a 'record of personal property etc.' relate to a specific category of personal data? Is it the thing purchased? Does that mean a category of consumer goods needs to be referenced or created? This scrutiny may help limit the scope of what 'categories' a company is expected to provide but ensure that the categories provided to consumers builds trust in the organizations handling their data.

Bottom line: Repurposing existing privacy standards and guidelines, as well as standardizing data requirement can ease the burden the CCPA will place on companies. It will also provide more genuine value to consumers requesting information to these companies. Please give specific, meaningful and consistent guidance to companies where possible. If it isn't possible, create carve outs in the rules so that companies don't shrug their shoulders, not bother to comply and add the CCPA to the ever-growing pile of onerous regulatory requirements that give meaningful and valuable regulation a bad name.

Thanks for the opportunity to share my thoughts,

Randy Wilson, California attorney [REDACTED] CIPP/E, CIPP/US, CIPM

Message

From: John Horst [REDACTED]
Sent: 3/7/2019 10:05:55 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA Rulemaking

I would like to reiterate my comments made in person at CSU San Marcos...

- 1) Please incorporate by reference the definitions of PII and PHI as provided by the National Institute of Standards & Technology (NIST). This is the basis for common understanding of what things mean in the world of cyber security.
- 2) Please take as light a touch as possible. If a company has an audited security plan/system (e.g. ISO 27001, PCI DSS, HITRUST) they should be considered in compliance. Each company's operations will be different, and so the manner in which they control for cyber risk will be different. Please avoid a one-size-fits-all idea of compliance (it will immediately become no-size-fits-any).
- 3) If a company's systems are approved by FedRAMP for US Government use, they should be considered in compliance. FedRAMP is based on NIST 800-53 Risk Management Framework and requires a third party assessment.
- 4) Do not allow companies to self-assess or self-certify.
- 5) Lastly, and this might go beyond rule making. An "affirmative defense" if a company has a third party assessed security plan/system (as described above) helps establish a clear dollar-sign value to having a third party assessed plan.

John Horst, CISSP® - ISSAP®, NQV

Managing Member for Technology and Innovation

Don't be trapped by dogma, which is living with the results of other people's thinking.

- Steve Jobs, 2005 Commencement Address to Stanford University



NOTICE: This email, and any attachments thereto, is intended for use only by the addressee(s) named herein and may contain information which is protected by attorney/client or work product privileges, or may represent information proprietary to Xanesti Technology Services, LLC.

If you are not the intended recipient of this email, you are hereby notified that any dissemination, distribution or copying of this email, and any attachments thereto, is strictly prohibited. If you have received this email in error, please notify the sender by email, telephone or fax, and permanently delete the original and any of any email and printout thereof. Thank you.

Message

From: Sharon Lewis [REDACTED]
Sent: 3/7/2019 4:12:48 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA Written Comments
Attachments: CHIA CCPA Comments 3-8-19 FINAL.pdf

Dear Privacy Regulations Coordinator,

Attached please find the California Health Information Association's (CHIA) written comments regarding the California Consumer Privacy Act of 2018.

CHIA thanks the California Department of Justice for the opportunity to submit comments regarding this groundbreaking legislation.

Warm regards,

Sharon Lewis

Sharon Lewis, MBA, RHIA, CHPS, CPHQ, FAHIMA

CEO/Executive Director

California Health Information Association

[REDACTED] (CHIA Office)

[REDACTED]
[REDACTED]
www.CaliforniaHIA.org



March 8, 2019

The Honorable Xavier Becerra
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Re: California Consumer Privacy Act of 2018

Dear Attorney General Becerra:

Thank you for this opportunity to submit comments on the California Consumer Privacy Act of 2018 (CCPA) prior to publication of the proposed rule by the Department of Justice.

The California Health Information Association (CHIA) is a component state association of the American Health Information Management Association (AHIMA). CHIA represents more than 9,000 credentialed and certified health information management professionals in California who help ensure that health care information maintained by providers of health care in California is accurate, timely, complete, and secure.

CHIA welcomes the opportunity to support the important new privacy rights afforded to consumers by the California Consumer Privacy Act (CCPA) of 2018. We believe the CCPA introduces needed protections for the personal information of consumers collected and often monetized by businesses. As consumers, CHIA members understand and appreciate the rights this legislation grants regarding the use of their personal information by businesses.

There are many types of business records that include personal information that must, as a necessity, be retained in the ordinary course of business to comply with numerous federal, state, and local laws and the regulations implementing them. Exceptions to consumer rights relating to their personal information are identified in section 1798.145 (c)(1)(A) of the CCPA and makes clear that the medical information governed by the California Confidentiality of Medical Information Act (CMIA) and health information protected under the Health Information and

Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) does not apply to the CCPA.

Although the CCPA exempts medical information governed by the CMIA, CHIA is concerned that there may be some providers of health care who capture medical information but who do not fall under the provisions of the CMIA or HIPAA. It is also noted that the definition of “medical information” in the CMIA is slightly different from the definition of medical information definition in HIPAA. Clarity in these two areas is needed as it pertains to the CCPA regulations.

One significant concern with drafting the regulations implementing the CCPA will be the clear delineation within the regulations of the types of business records and the personal information exempted by the CCPA. It is important that the regulations and any consumer informational literature or media produced in conjunction with implementing the CCPA make the applicability of the consumer rights granted by the CCPA and the exceptions to them readily apparent and easy to understand by both consumers and the businesses that must comply with the CCPA.

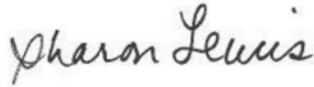
To facilitate the rulemaking process and the implementation of the CCPA, CHIA recommends the following:

- **Clarify the definition of “medical information” for the purpose of the exemptions and consider its application to any providers of health care who capture such information.**
- **Define providers of health care who are impacted by the CCPA that may not fall under CMIA or HIPAA.**
- **Require the implementing regulation to prominently display both the consumer rights granted by the CCPA and delineate the types of business records exempted by the CCPA in plain, easily understood text understood by the general public.**
- **Require any consumer related literature or media produced in conjunction with the implementation of the CCPA to clearly delineate the specific consumer rights granted by the CCPA and the record types that are exempted.**

CHIA further recommends that the State of California assess the potential impact of California Assembly Bill 384 on the CCPA. AB 384 expands the definition of “medical information” to include information in digital health feedback systems. If passed, is there a possibility that AB 384 may make medical information generated by digital feedback systems subject to the CMIA and, therefore, be exempt from the CCPA.

CHIA thanks the California Department of Justice for the opportunity to submit comments regarding this groundbreaking legislation. We look forward to contributing to the successful implementation of the CCPA. Should the Privacy Regulations Coordinator for the CCPA have questions or require additional information from CHIA during the rulemaking and implementation of the CCPA please contact Sharon Lewis, CEO/Executive Director at [REDACTED] or via [REDACTED]

Sincerely,

A handwritten signature in cursive script that reads "Sharon Lewis".

Sharon Lewis, MBA, RHIA, CHPS, CPHQ, FAHIMA
CEO/Executive Director
California Health Information Association
5055 E. McKinley Avenue
Fresno, CA 93727

cc: Maria Alizondo, MOL, RHIT, FAHIMA
2018-19 CHIA President

Message

From: Fatima Khan [REDACTED]
Sent: 3/8/2019 3:05:43 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Timothy McIntyre [REDACTED]
Subject: CCPA Written Comments
Attachments: Okta_PublicComment_CCPA_final.pdf

Hi –

Please see the attached document for Okta's comments. Thank you for your consideration.

Best,

Fatima

March 8, 2019

California Department of Justice
Attn: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

Re: DOJ – California Consumer Privacy Act of 2018
Comments of Okta, Inc.

Okta, Inc. ("Okta") appreciates the opportunity to provide these comments in connection with the California Department of Justice's ("DOJ") preliminary rulemaking for the California Consumer Privacy Act of 2018 ("CCPA").

Okta Overview

Okta is a publicly-traded (NASDAQ: OKTA) cloud computing company that offers identity and access management software-as-a-service to businesses, governments, non-profit entities, and other organizations across the United States and around the world. Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables the company's customers to securely connect people to technology, anywhere, anytime and from any device. The company was incorporated in January 2009 as Saasure Inc., a California corporation, and was later reincorporated in April 2010 under the name Okta, Inc. as a Delaware corporation. Okta is headquartered in San Francisco, California.

Okta's customers use our services to work with some of their mission-critical, sensitive data, including the names, email addresses, and mobile phone numbers of their users. As a growth company, Okta continues to surpass key milestones: just recently, we cleared the 100 million user mark¹. Accordingly, acting with integrity and transparency, so that we earn and maintain our customers' trust, is critically important to all of us at Okta. To that end, Okta maintains privacy protections across its suite of services, as detailed in our third-party audit reports and standards certifications.

Although many companies may view privacy compliance as a burden, Okta views it as a strategic differentiator, and a competitive advantage: we provide tools and resources to our customers, to help ensure that their own systems are kept safe and secure, so that critical data can remain private and protected.

For these reasons, Okta believes that California would benefit from implementing a comprehensive privacy law, provided that such law protects consumers and enables businesses to strengthen their approach to privacy through clear compliance obligations. Okta's approach to privacy aligns with the CCPA, including support for the view that "it is

¹ "Okta Now Has Over 100 Million Registered Users, Says CEO" - <https://finance.yahoo.com/news/okta-now-over-100-million-234824968.html>

possible for businesses both to respect consumers' privacy and provide a high level transparency to their business practices".²

Introduction

Okta agrees with the DOJ's sentiments that today more than ever, strong privacy and security programs are essential to the people of California and our economy.³ As technology advances, California is continuously the leader at the forefront of protecting the privacy and security of consumers and Okta supports the state's efforts. In addition to being a trailblazer in protecting consumer privacy, Okta also encourages the state of California and the DOJ to remain engaged with both federal and other states' efforts to further privacy in order to create regulation and guidance that will best allow companies to strengthen privacy best practices for consumers.

Okta encourages California to continue to advance consumer privacy through risk-based, flexible, privacy regulation that provides clear compliance obligations for businesses. We believe that being unduly prescriptive can result in stifling compliance checklists that inhibit the creation of innovative privacy solutions. Benefits should be measurable and quantifiable, and any new state privacy legislation should first take into account the outcomes sought by consumers, and also align with California residents' understanding of meaningful data protection.

Key Points for Consideration

We offer three key areas for consideration as part of the DOJ's analysis.

First, it is important that the DOJ account for the complexity of technology and the different scenarios that arise through the use of personal information. Although Okta is aware of the risks associated with processing personal information, there are instances when consumers may prefer to share their personal information with companies that are best positioned to protect consumer privacy and security through their services. As follows, it is important to ensure that the CCPA accounts for different business models and enables the use of personal information to further innovation and pro-privacy and security technologies.

Second, security needs are ever-changing based on evolving technology and new threats. As a result, Okta believes that the law should incentivize companies with a litigation and enforcement safe harbor so that companies proactively take preventative measures to adhere to reasonable security standards and implement best practices.

Third, Okta believes that the CCPA would benefit from clarification and alignment with existing global privacy and security standards, provided that such harmonization continues to strengthen consumer rights, emphasize the importance of security, and pass through requirements to service providers.

1. Request for the consideration of different business models and various uses of personal information.

² Cal. Civ. Code Section 2(h)

³ <https://oag.ca.gov/privacy>

As stated in the CCPA, “it is almost impossible” to conduct even the most mundane tasks without sharing personal information.⁴ Based on the pervasive need to collect personal information to carry out tasks, it’s important for the state of California to account for the wide array of business models that need to collect personal information to carry out the services they provide to consumers and to businesses. Okta does not monetize personal information, but provides a cloud-based enterprise solution that helps to streamline identity management and increase efficiencies for companies and their end users to securely access cloud-based applications. The CCPA should elaborate upon the key distinction between businesses and service providers to achieve its goals to protect consumer privacy and maintain companies’ ability to innovate while using personal information to provide services. This section addresses two means to help further these twin goals: (i) the clarification of the definitions of *personal information*, *consumer*, and *sale*; and (ii) the harmonization of the business/service provider distinction with the controller/processor definitions found across existing global legal frameworks.

- a. Request for the clarification of the definitions of *personal information*, *consumer*, *business purpose*, *commercial purpose*, and *sale*.

Okta supports the California legislature’s key drivers for the CCPA that are discussed above, and we believe that a uniformly-applied set of definitions for important terms as well as a few additional slight changes can help achieve those goals. Therefore, any privacy legislation or framework should include terms that map to consumers’ natural understandings of those terms. Such an approach would also facilitate smooth interoperability between the U.S. privacy landscape and those in other countries.

For instance, “personal information” should be defined to mean data that identifies or relates to a specific person. Okta takes a skeptical view of expanding such definition to include IP address, devices, or even households, or all electronic network activity information, as included in the current version of the CCPA.⁵ We encourage a discussion of these data points and the unintended consequences that may arise based on consumer rights to such data which could potentially lead to dangerous outcomes that undermine individual privacy, security and fraud detection efforts, or the ability for businesses to operate. Oftentimes, IP address, device details, and electronic network activity information are not tied to name or other personal information that would directly identify a single individual, thereby creating problems with the ability of businesses to satisfy any related consumer requests without either (i) potentially sharing one person’s data with another person; or (ii) having to collect or tie additional personal information from an individual to be able to satisfy a consumer request for this same information. As an unintended result, businesses may end up undermining consumer privacy through complying with the law unless these categories are removed as per se personal information or additional exceptions are put into place. To further elaborate, consumer requests for access to personal information should be reasonably limited similar to the exceptions outlined for consumer deletion requests. To the extent reasonable and justified, limiting the definition of personal information and creating exceptions to the exercise of consumer rights to such personal information will further consumer privacy

⁴ Cal. Civ. Code Section 2(c)

⁵ Cal. Civ. Code § 1798.140(o)(1)(A)

and enable the legitimate use of such personal information by businesses and service providers.

The current definition for “consumer” includes “professional or employment-related information” per the definition of “personal information”.⁶ Okta suggests the DOJ reconsider the definition of “consumer” and clarify its application to employees and contractors acting in their professional roles, including the impact on the ability for businesses to transact with other businesses and any corresponding rights or limitations that may arise. Companies maintain contact information along with professional or employment-related information as well as related interactions or preferences for legitimate reasons to operate their businesses. Similar to other proposed state legislation, Okta believes there should be an exception within the definition of “consumer” for “a natural person acting in a commercial or employment context”.⁷

Furthermore, we request that the DOJ further clarify “sale”, “business purpose” and “commercial purpose” to understand when a transaction falls within each category based on the use of personal information. Okta recognizes that there are nuances to the methods and purposes used by service providers to process personal information. These varying methods, purposes, and use cases may fall outside of the defined business purposes; therefore, Okta requests that the DOJ consider such nuanced data use situations so as to allow service providers to provide services and conduct data-driven analysis without categorizing these services as “commercial purposes”.

In conclusion, the definitions of “personal information”, “consumer”, “commercial purpose”, “business purpose”, and “sale”, should match consumers’ expectations and conform to existing privacy standards and frameworks to avoid unintended adverse effects on consumer privacy and create clear compliance obligations.

b. Request for the harmonization of the business/service provider distinction with existing legal frameworks for controller/processor

We believe it’s absolutely critical, when developing American federal or state privacy law, to clearly delineate between data controllers (which collect and process personal data for their own purposes and who make sophisticated decisions about those activities) and data processors (which collect and process personal data on behalf of, and in accordance with the instructions provided by, data controllers). In preparation for the EU General Data Protection Regulation (“GDPR”), businesses have categorized themselves as data controllers or data processors for each processing activity, so harmonization of “business” and “service providers” with these existing classifications would both facilitate privacy compliance by businesses and strengthen consumer privacy. Moreover, the controller/processor distinction is top-of-mind for many enterprise cloud computing companies. Such companies are not in the business of monetizing personal data, and rather, operate in the business-to-business sphere, and provide subscription-based services that increase economic efficiencies and protect personal data for other companies throughout the U.S. and the rest of the world. We recommend that lawmakers account for this fundamental distinction and harmonize the concepts of business and service provider with this existing framework. Okta applauds Washington state’s efforts

⁶ Cal. Civ. Code §§ 1798.140(g), (o)(1)(I)

⁷ Wa. State SB 5376 § 3(6)

on harmonization of these concepts through their proposed privacy legislation and believes that it is important to create interoperable legal frameworks for technology companies across states to be able to implement strong privacy controls.⁸

2. Request for the consideration of limitations on the private right of action, including a safe harbor for reasonable security.

Okta strongly supports consumers' right to robust and meaningful privacy enforcement, including the imposition of penalties when violations take place. Although Okta agrees with the California Attorney General's position that companies that collect, store, use, or share personal information should employ reasonable security safeguards to secure these data, we caution that prescriptive approaches to security can be unintentionally limiting: security practices evolve on an almost daily basis, as security experts need to respond and mitigate new forms of attacks from sophisticated – and in some cases, state-sponsored – threat actors. Security requirements should be outcome-driven, and should not impose rigid technical requirements that could have the effect of locking regulated companies into archaic, outdated practices over time.

No matter how robust a company's privacy and security practices are, due to the ongoing, fast-changing pace of security standards, there can still be gaps that lead to security failures that could be interpreted as "unreasonable security" and lead to "unauthorized access" and "unauthorized acquisition, theft, or disclosure".⁹ Because the security landscape changes swiftly, companies should be incentivized to adhere to existing privacy and security frameworks and standards that adapt based on that company's practices, such as undergoing a SOC 2 Type 2 Audit and obtaining ISO 27001 certification. These third-party audit reports and standards certifications should function as a safe harbor from litigation and enforcement in order to incentive companies to implement preventative measures to avoid any potential adverse effects on consumers.

Furthermore, Okta suggests that the DOJ consider harmonizing the 30 day cure period with the GDPR requirement to instead show a remediation plan to mitigate adverse effects.¹⁰ Based on the unique circumstances of each type of security or privacy incident, a 30 day cure period may not be feasible under the specific circumstances even if a business makes a good faith effort to cure a violation and takes concrete remediation steps within that time period.

3. Request for the consideration of alignment of the CCPA with existing privacy principles and legal frameworks.

Finally, we believe that privacy is a concept that varies from culture-to-culture, and that principle is apparent from the differing state privacy laws domestically, and differing privacy laws and frameworks internationally. Accordingly, any new state legislation in this area should reflect California's unique values but also be consistent with existing regulations to ensure that consumers are provided with an easy-to-understand and harmonized approach to privacy that satisfies the spirit of the law. Although certain

⁸ Wa. State SB 5376

⁹ Cal. Civ. Code § 1798.150

¹⁰ GDPR Article 33(3)(d)

aspects of the GDPR may not align with the California approach, we encourage lawmakers to look at the process by which the GDPR was developed: the EU took a deliberative approach, involving stakeholders from the public sector, privacy sector, the high-technology industry, and academia and understood the need to harmonize laws across EU member states. If the CCPA is to be implemented in California, then a multi-stakeholder development process should be followed, and the resulting law should interoperate smoothly with existing privacy frameworks around the world. Harmonization of the CCPA with existing privacy principles and frameworks will enable businesses to comply with the regulation and thereby strengthen privacy protections for consumers.

Conclusion

Okta praises the State of California's work in this area and appreciates the consideration of our views and perspectives. While Okta is firmly in favor of strengthening consumer privacy and security, we also understand the challenges and high compliance costs, productivity losses, and administrative burdens that arise as an effect of disparate regulatory requirements. Okta welcomes further discussions in this area, regarding an expansion of the DOJ's role in a manner that would let it effectively assume additional oversight and enforcement duties.

Respectfully Submitted,

Okta, Inc.
Legal Department
[REDACTED]

Message

From: Ann Marcelo [REDACTED]
Sent: 3/8/2019 2:31:40 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Jason Sebring [REDACTED] Laurie Dechery [REDACTED]
Subject: CCPA
Attachments: Becerra.CCPA.03 08 19 - signed.pdf

Dear Attorney General Becerra:

Please see attached CCPA letter. A hard copy will be sent via Fed Ex delivery.

Regards,

Ann C. Marcelo

Executive Assistant for:

Lisa Blackwood-Kapral, VP & CAO, Michael J. Robinson, VP & CIO, Jason Sebring, VP & GC, Kris Espiritu, VP & Strategic FP&A & Ben Weitzel, VP & CIA

[REDACTED]

SHUTTERFLY 

3800 Bridge Parkway, Redwood City, CA 94065



By U.S. Mail and email to: privacyregulations@doj.ca.gov

March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

Dear Attorney General Becerra:

Shutterfly, Inc. and its wholly-owned subsidiary, Lifetouch Inc., welcome this opportunity to provide our input on the California Consumer Privacy Act (CCPA) to inform the rulemaking process. Shutterfly, Inc. is the leading retailer and manufacturing platform for personalized products; its wholly-owned subsidiary Lifetouch Inc. is the national leader in school photography, built on the enduring tradition of "Picture Day." Schools throughout California trust Lifetouch to capture photographs of their student population for use in yearbooks, student IDs, school safety programs, and other administrative and community-building purposes as well as offering the photos for sale to the students' families.

While we strongly support the objectives of the California Consumer Privacy Act (CCPA), we have concerns about the likely negative impact on California consumers, schools and businesses stemming from a lack of clarity regarding how CCPA applies to the business of photography (including but not limited to school photography) and the sale of photographic products and services (from personalized products offered by Shutterfly to the traditional class group photo and school yearbook). In particular, we believe that further clarification is necessary to address situations where a consumer may seek to exercise rights over photographs that include that consumer's likeness. Such exercise of rights would in many cases have the unintended consequence of violating the rights of others – if not the goals of CCPA itself.

The role of photography in privacy policy presents a case in point for the need for a flexible, context-driven approach that takes into account the intentions and reasonable expectations of all

stakeholders. In the context of school photography, for example, parents know that when their child participates in their school's annual Picture Day, a class group photo will be offered for sale to the parents of children in the class. This transparent and school-sanctioned activity should not be deemed a "sale of personal information" that requires the school photographer to obtain opt-in consent from each parent, or that would allow one parent to void the sale of a class group photo to other parents.

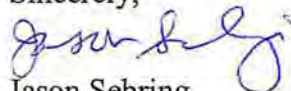
Similarly, CCPA may be deemed to grant a California resident who appears in a photograph contained in a Shutterfly user's account the right to demand deletion of the photo. By extension, that person could submit a request for Shutterfly to identify every photo in every user's account that includes his or her likeness, based upon CCPA's broad definition of what it means to "collect" personal information. Clearly, compliance with such a request would not only be impracticable, it would also violate the rights of account holders who entrusted Shutterfly to store those photos on their behalf.

It does not appear that the California legislature intended CCPA to apply to these scenarios or to regulate the business of photography per se. In enacting CCPA, the California legislature recognized the need to balance the individual rights granted to California consumers with competing or conflicting rights in appropriate contexts. For example, section 1798.105(d) provides that a business is not required to comply with a deletion request where retention is necessary to "...ensure the right of another consumer to exercise his or her right of free speech or exercise another right provided for by law." Moreover, pursuant to Section 1798.185(a)(3), the AG is directed to adopt regulations to "further the purposes of the CCPA," including "establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights."

Grounded in these principles, we urge the AG to address the complexities inherent in defining "personal information" to include photographs. Specifically, we seek regulations that clarify that the mere taking of a photograph is not a "collection" of personal information, nor is the lawful sale of a photograph or personalized product equivalent to a "sale" of personal information to a "third party" that gives rise to consumer rights pursuant to CCPA.

We would welcome the opportunity to work with your office to further address these issues as you move forward with this process.

Sincerely,



Jason Sebring
General Counsel

Message

From: Jill Nissen [REDACTED]
Sent: 3/8/2019 5:21:17 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Sam Chaudhary [REDACTED]; Manoj Lamba [REDACTED] Lindsay McKinley
[REDACTED]
Subject: ClassDojo Comments in Support of CCPA and Seeking Clarification for Education Technology Companies
Attachments: ClassDojo comments in support of CCPA 03 08 19.pdf

Dear Privacy Regulations Coordinator,

On behalf of my client, ClassDojo, I am submitting to the California Attorney General's Office, the attached comments in support of the CCPA as well as seeking further clarification for education technology companies (who are already subject to SOPIPA obligations) on compliance with the CCPA.

Best,

Jill Nissen

Jill L. Nissen, Esq.

Founder & President

Nissen Consulting, P.C.

[REDACTED]

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

March 8, 2019

Re: ClassDojo's comments in support of CCPA and seeking clarity for education technology providers subject to SOPIPA

ClassDojo first wants to take this opportunity to thank Californians for Consumer Privacy, the California legislature and the Attorney General's office for their efforts to pass the California Consumer Privacy Act ("CCPA") and the Attorney General's office for holding the public hearings and soliciting comments during this rulemaking process. The CCPA is an important step in protecting consumer privacy and *ClassDojo fully supports the CCPA*. ClassDojo would, however, like some clarification regarding:

- 1) How the CCPA and California's law protecting student privacy (the Student Online Personal Information Protection Act ("SOPIPA")) function together.
- 2) If education technology providers that have entered into contracts with schools would be considered "service providers" under the CCPA; and if so, what obligations do they have as "service providers" under the CCPA.
- 3) How access and deletion requests under the CCPA should be handled given the contracts that education technology companies have with schools.

Additionally, ClassDojo would like to:

- 1) Inform the Attorney General's office about the financial and resource burdens that the law as currently drafted imposes on education technology companies who have less than \$25 million in annual revenue and whose mission it is to provide free services to schools; and
- 2) Propose a new concept of a possible grant or "fund" for education technology companies to allow these companies to license or purchase technological solutions to better assist them in meeting access and deletion obligations under the CCPA.

Similar to the point raised by other commenters during the various public forums held by your office on the CCPA, ClassDojo hopes that the Attorney General's office will provide input and clarification beyond the seven specific areas set forth under Section 1798.185(a) of the CCPA given Section 1798(b) also allows the Attorney General to "adopt additional regulations as necessary to further the purposes of this title." While ClassDojo's clarifications and comments relate to 1798.185(i) "categories of personal information"; and 1798.185 (3) "exceptions to CCPA", they also cover areas outside of these seven enumerated areas.

As some background, ClassDojo is an education technology company with a mission to help every child have an education they love. *We aim to do so by providing our product free to teachers, a commitment we have made from the beginning.* ClassDojo helps teachers, families, and students communicate and share what's happening at school. While ClassDojo is actively used in 95% of all K-8 schools in the U.S., *we are still a relatively small company with only 40 employees.* We have recently started to test out paid

features for parents – a new product called ‘Beyond School’, the revenue of which will be used to keep ClassDojo free.

CLARIFICATION REQUESTS:

1. CCPA and SOPIPA.

Unlike the specific exceptions for companies and institutions that collect, process, sell or disclose data subject to the Gramm-Leach-Bliley Act (“GLBA”), the Health Insurance Portability and Accountability Act (“HIPPA”), and other laws set forth under the CCPA, the legislature did not exempt student data or “educational records” from the CCPA, and choose to specifically include “education information” as defined under the Family Educational Rights and Privacy Act (“FERPA”) as one of the enumerated subsets of data defined to be personal information. *We too agree that student data or educational records should be included in the CCPA.* However, due to the fact that under SOPIPA, educational technology companies are already subject to strict obligations (even more strict with respect to “selling data” – which is a flat prohibition not an opt-out or opt-in)¹, it is unclear which obligations under the CCPA would in fact apply to educational technology companies that are already subject to SOPIPA. We would propose that you provide clarity and guidance that *any educational technology company (including those that collect data directly from a student or teacher), that has entered into contracts with schools to: 1) meet their obligations under SOPIPA (as well as the more than 120 plus state student privacy laws) and 2) where the school has designated the company as a “school official” for the school’s FERPA exemption/compliance purposes, be considered a “service provider” and not a “business” under the CCPA.* This clarification is also needed due to the fact that a strict reading of the current “service provider” definition in the CCPA states that the service provider is “processing information on behalf of a *business*” and most schools are non-profits, not businesses.

In addition, because of the broad definition of personal information under the CCPA (in particular the language “*is capable of being associated with*” and applying to both a consumer or “*household*”), similar to the comments you heard during the public forums with respect to GLBA and some data collected being outside the scope of exempted GLBA data, yet within the scope of the CCPA given the broad definition of personal information under the CCPA, there may also be data collected by education technology providers that would fall under the definition of “personal information” under the CCPA, but yet would not be student data (or “covered information”) as defined under SOPIPA. Additionally, there may be parent personal information that would be solely subject to CCPA. We welcome guidance and clarity on how to then operate as a service provider in one instance, yet a “business” in another in terms of compliance given the broad definition of personal information under the CCPA.

2. Obligations of Service Providers Under the CCPA.

Assuming that education technology companies providing services to schools (with the parameters set forth in #1 above) are clarified to be deemed “service providers” with respect to student data (and not “businesses”) under the CCPA, we would like additional guidance on what obligations there are under the CCPA for service providers. As stated by a few commentators during the public forums, unlike GDPR (where there is a processor/controller distinction made), it is not entirely clear if there are any additional obligations on service providers under the CCPA. *For example, should service providers still be subject to all of the transparency obligations?* We propose that they should be subject to the transparency obligations— particularly with respect to education technology providers. The “opt-out”, “opt-in”, “Do

¹ See SOPIPA, SB-1177 Section, 22584(b)(1)(3)

Not Sell Button” and other “selling” provisions under CCPA would not need to apply to education technology “service providers” given these companies are already subject to tougher restrictions under SOPIPA with respect to student data. We would also ask for clarity regarding any private right of action provisions as they relate to service providers.

3. Access and Deletion Rights.

Access

While SOPIPA does not directly address “access” rights of students as other state student privacy laws do (which require that any access requests first be sent back to the school), many contracts entered into with California schools, including the Model Contract recommended by the Student Data Privacy Consortium (“SDPC”) in California (which according to the SDPC 1,109 districts in California have signed onto)², mandate that any access requests from parents or students be directed back to the school first. *We are requesting clarification that any access requests received regarding student data be directed to the school first, and then the school can forward any valid requests to the education technology vendor (given the vendor would be deemed to be a “service provider”).* This is not unlike current FERPA obligations (although with a more limited definition of what personal information parents have access rights too). While some may argue that the school is not subject to CCPA so they should not have to honor any access request, and thus the individual effectively has no rights of access under the CCPA, we don’t think this is the right result. ClassDojo would be willing to accept access requests first (even if determined to be a “service provider”), but this would result in a breach of obligations with the terms that most schools have imposed on us. Additionally, regardless of where the guidance comes out on access requests (to the school first (who then forwards on to the service provider) or to the education technology service provider first), *the service provider will likely in both scenarios still be responding to the access request as the schools likely do not have access to the services needed to produce this data.* As mentioned below, given the broad definition of personal information under the CCPA, putting the systems in place and responding to these this will impose substantial costs and resources on small education technology providers.

Also, as mentioned above, given the broad definition of personal information under the CCPA, there may be student personal information that would not be covered under SOPIPA (or parent personal information not subject to SOPIPA) which would present some confusion to parent and students on whether or not they have to submit two separate access requests. ClassDojo is open to suggestions and clarifications on how best to proceed in this situation.

Deletion

Regardless of where the guidance or clarification comes out on access rights (to the school first (who forwards the request to the service provider) or to the education technology company first), *it should be clarified that no deletion requests for student data should come to the education technology provider first.* SOPIPA does address deletion rights (although merely from the standpoint of the service provider having to honor the requests received from the school). This clarification is needed because of various obligations schools have under FERPA (and pass down through contract to their service providers when using the “school official” exemption) as well as the service provider’s obligations under SOPIPA and other state student privacy laws that the school has to maintain “control” of the education record. One can also imagine a situation where a parent or student did not like the student’s grade or school assignment and wanted it deleted from their educational record.

² See https://sdpc.a4l.org/view_alliance.php?state=CA

FINANCIAL AND RESOURCE BURDENS

As mentioned above, ClassDojo is a small company with only 40 employees, yet our teacher base is large – above 50,000 California users - thereby triggering the CCPA. Additionally, ClassDojo wants to be able to continue to provide its services free of charge to teachers. Regardless of where the guidance comes out on how access requests should be directed (to the school first, then to the education technology service provider or to the education technology service provider in the first instance), there are significant costs and personnel resources that will need to be allocated to deal with both access requests and deletion requests. This is in part due to the broad definition of personal information mentioned above (*“is capable of being associated with”*) that many other commentators have already pointed out. It is not as simple of a task as some believe to both build the systems capable of mapping and categorizing this data (*some of which would never “by associated with personal information”*, but must now be produced) throughout many different systems (third party service providers, etc.) and respond to the type of access requests for the types of personal information that is included under the CCPA. Anyone who has worked inside a company or tried to build the systems to enable one to respond to access requests under GDPR (which has a narrower definition of personal information subject to an access requests) knows this all too well.

However, there are some great technologies out there that can assist companies in doing just this – especially those that have personnel constraints as well – such as BigID and others. While larger companies can easily implement and license these technologies and many have, it is financially cost prohibitive for many small education technology companies to do so (i.e. some of these technology licenses start at \$150,000 a year). We believe in the importance of what the CCPA is hoping to achieve and would like to work on a solution that supports the needs of everyone involved while also supporting the important goal of providing services free for teachers.

FUND ESTABLISHED FOR TECHNOLOGY PURCHASE BY SMALL EDUCATION TECHNOLOGY COMPANIES

One potential solution is a “fund” put into place to help assist smaller educational technology companies purchase technology to assist them in complying with access and deletion requests. While Section 1798.160(c) of the CCPA establishes a “Consumer Privacy Fund” to offset Attorney General and state courts costs only, we suggest a portion of this (or some other mechanism established) be used to help aid with CCPA compliance - in particular to purchase technological solutions to help aid with categorizing data and responding to access and deletion requests. Putting money into helping with compliance will also help reduce the amount of violations that occur and can make sure that education technology companies – such as ClassDojo – can continue to remain free for teachers. This fund could also be expanded beyond education technology companies.

Thank you for your consideration.

Sincerely,

ClassDojo

Message

From: [REDACTED]
Sent: 3/8/2019 4:27:18 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Craig C. Page [REDACTED]
Subject: CLTA Comments on Preliminary Rulemaking Activities Relating to the California Consumer Privacy Act
Attachments: CLTA Comments to DOJ RE CCPA Letter 03_08_19.pdf

March 8, 2019

To Whom It May Concern:

Please find attached an electronic copy of the California Land Title Association's Comments on the Department of Justice's preliminary rulemaking activities relating to the California Consumer Privacy Act. These comments are also being sent in a hardcopy format.

Thank you for your time and consideration.

Sincerest Regards,

Sent by Anthony Helton on behalf of:

Craig C. Page

Executive Vice President

and Counsel

California Land Title Association

1215 K Street, Suite 1816 | Sacramento, CA 95814

[REDACTED]

[REDACTED]

[REDACTED]



March 8, 2018

Stacey Schesser, Supervising Deputy Attorney General
Privacy Enforcement and Protection Unit
California Department of Justice
300 S. Spring St.
Los Angeles, CA 90013

RE: CLTA Comments on Preliminary Rulemaking Activities Relating to the California Consumer Privacy Act

Dear Ms. Schesser:

The California Land Title Association (CLTA) appreciates the opportunity to provide comments on the California Consumer Privacy Act (CCPA) on behalf of its members for consideration by the Attorney General and his staff.

CLTA is a non-profit trade organization founded in 1907. Our members employ thousands of professionals throughout California dedicated to the efficient and competent closing of real property transactions and the issuance of title insurance in connection with such transactions.

Based in Sacramento, the Association effectively serves as a resource for both title insurers and underwritten title companies who serve consumers in all 58 counties providing research regarding and insuring the status of title to real property, as well as acting as the escrow and settlement agent in the sale and transfer of real property, refinancing of loans, and other related functions.

CLTA has worked closely with the Attorney General's office in the past in providing comments on the implementation of regulations relating to the electronic recordation of documents, known as the Electronic Recording Delivery System (ERDS), and looks forward to our continued strong working relationship as the Attorney General contemplates regulations relating to the CCPA.

CLTA and the title industry strongly support the goals of the CCPA but we believe regulations are necessary to address the potential unintended consequences of the new law.

CLTA and its members understand and support the intent and purpose of the CCPA as a means to empower California residents with respect to their privacy. However, the broad scope and "one size fits all" approach enacted under the CCPA is likely to have tangible adverse impacts on a significant number of California residents that were likely not contemplated by the authors and proponents of these bills. CLTA is hopeful that these will be addressed in the Attorney General's regulations.

1215 K Street, Suite 1816, Sacramento, CA 95814

* Fax (916) 444-2851 * www.clta.org *

CCPA00000321

In their usual course of business, title and escrow companies provide important services to government that help prevent or remedy fraud and other duplicitous or illegal activity:

In addition to the title industry's role in helping consumers to consummate real estate transactions (buying and selling of real property, refinancing of loans, etc.), title companies work very closely with city, county, state and federal governmental agencies, especially in the escrow process. This close working relationship includes activities such as, but not limited to, the following:

- ***Helping local law enforcement to thwart real property and loan fraud, money laundering, and providing advice in subsequent prosecution.*** In this capacity, we often provide valuable information relating to the parties participating in a transaction.
- ***Helping the Federal Bureau of Investigation to target and often prevent real property fraud and mortgage fraud that occurs in California.***
- Helping the Financial Crimes Enforcement Network ("FinCEN", a government entity operating under the Dept. of Treasury), for which title companies are required to collect personal information of the individual representative reporting for a buyer entity.
- Helping the Department of Child Support and Collection Services and county child support collection agencies to collect approximately \$15-20 million dollars annually through the identification of liens identified in public records (child support abstracts of record recorded against real property or recorded in the general index by name), and a collection of said liens via the escrow process using data to link the obligor parent to the unpaid child support.
- Helping city, county, and state agencies to collect billions of dollars in taxes, special assessments, and uncollected fees annually through the escrow process associated with recorded liens and other documents.

While Civil Code Section 1798.145(a) of the CCPA attempts to provide California businesses with the ability to comply with laws and cooperate with law enforcement agencies, insofar as said cooperation relates to potentially illegal activity, we respectfully request that the AG regulations be drafted so that it is absolutely clear that the intended purpose of this section is to prevent fraud and other criminal conduct, thwart deceptive practices by bad actors, and more clearly allow the title industry to continue to share data within the industry and with local government necessary to collect child support and outstanding taxes.

For this reason, and pursuant to Civil Code Section 1798.185(a)(3), which states that the Attorney General shall adopt regulations to establish "any exceptions necessary to comply with state or federal law", CLTA and its members respectfully suggest that the Attorney General should clarify that the CCPA does not impose obligations upon a Business that, in good faith, is collecting, using, retaining, selling or disclosing personal information in order to protect against or prevent malicious, deceptive or fraudulent activity, or unauthorized transactions, or is seeking to investigate, report, or prosecute those responsible for such illegal activity.

Without this clarification, we are concerned that title and escrow companies' ability to provide the important services described above could be undermined by the CCPA as enacted.

The exemption from “personal information” for “publicly available” information is unclear, putting the continued consummation of California real estate transactions at risk:

Title companies search public records and use aggregate data within those records for the purpose of consummating transactions for consumers who are buying and selling real property, refinancing of loans, etc., and, in the course of conducting those searches, can also provide useful information to government agencies and law enforcement relating to illegal or deceptive activity.

While the CCPA as enacted exempts from the Act any information determined to be “publicly available”, this exemption is sufficiently unclear as to call into question whether it can be relied upon by title companies for the purpose of consummating real estate transactions, let alone providing assistance to government or law enforcement agencies.

Therefore, and pursuant to Civil Code Section 1798.185(a)(1), which states that the Attorney General shall adopt regulations to update “as needed additional categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (o) of Section 1798.140”, CLTA respectfully suggests that the Attorney General should promulgate regulations to clarify the exception in the definition of “personal information” for publicly available information in 1798.140(o)(2) to make clear that “government records” means any data made available by the government to the public voluntarily or as a matter of law; and, “a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained” means, in the absence of an express limitation of use by the government entity holding that data, any legitimate and lawful purpose.

Any narrower definition would raise federal and state constitutional issues, and could be argued to preclude the vital functions carried out by title companies every day with respect to real estate transactions as well as fraud prevention and lien collection, especially if not modified by a “legitimate purpose” exception.

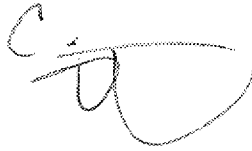
Clarifications are critical to make clear that deadbeat parents, criminal bad actors, and others seeking to violate the law or avoid their financial obligations to the government will be unable to use the CCPA provisions to delete, or preclude the sharing of, their personal information that title companies use to thwart an array of deceptive and illegal activity:

California title companies worry that if the Attorney General is not careful in how the implementing regulations are drafted, the CCPA and/or its regulations could ultimately have the inadvertent impact of creating loopholes that allow deadbeat parents and others owing taxes and fees to evade payment, or perpetuate an unknown quantity of fraudulent and money laundering activity.

In short, if title companies cannot collect and share the data necessary to determine the obligors who owe these obligations, they cannot collect these delinquent child support payments, taxes, and other fees in escrow. Similarly, if title companies can’t share information with law enforcement agencies, they will be unable to assist in the prevention of criminal activity.

For this reason, we strongly believe that the above clarifications are warranted to add clarity in the regulations that, in addition to continuing to provide title insurance, title searches, and settlement services for our consumers, title companies can also continue to work closely with the aforementioned agencies in protecting California consumers and taxpayers.

Respectfully,

A handwritten signature in black ink, appearing to read 'Craig C. Page', with a stylized, sweeping flourish at the end.

Craig C. Page
Executive Vice President
and Counsel

cc: Larry Morse, California District Attorneys Association
Greg Wilson, Child Support Directors Association
Anne Drumm, California Department of Child Support Services
Karen Lange, California Association of County Treasurers and Tax Collectors

Message

From: Valenzuela, Lauren [REDACTED]
Sent: 3/8/2019 11:44:32 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comment from Performant Recovery
Attachments: CCPA Comment from Performant Recovery.pdf

We thank you for the opportunity to present our comments. Please see the attached document.

Sincerely,

Lauren Valenzuela

LAUREN VALENZUELA, ESQ.

Compliance Counsel

PERFORMANT

Performant Financial Corporation
333 N. Canyons Parkway | Suite 100
Livermore | CA | 94551

This email may be privileged and/or confidential, and the sender does not waive any related rights and/or obligations. Any distribution, use or copying of this e-mail or the information it contains by other than an intended recipient is unauthorized. If you received this e-mail in error, please advise me (by return e-mail or otherwise) immediately. For more information on Performant please visit our website at www.performantcorp.com.

CCPA00000325



Sent Via Email:

PrivacyRegulations@doj.ca.gov

CA Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

March 8, 2019

RE: California Consumer Privacy Act (CCPA) Comments

Dear Mr. Becerra:

Pursuant to §1798.185, we are submitting written comments regarding the California Consumer Protection Act (CCPA). We believe it helpful to provide information about our business and industry so that our comments may be understood in the context of which we perform our services.

One of Performant Recovery's main lines of business is collecting debt. Performant Recovery has been providing this financial service to many federal, state, and private entities since 1976. One of the main federal laws governing debt collection is the Fair Debt Collection Practices Act (FDCPA), codified at 15 USC §1692 et seq. California has its own debt collection law as well, the California Rosenthal Act, codified at California Civil Code § 1788 et seq. Protecting and honoring a consumer's privacy is a core tenant of these laws, and law-abiding debt collectors have designed their debt collection processes around protecting a consumer's privacy.

Although protecting consumers' privacy is nothing new to law abiding debt collectors, the CCPA presents many questions when applied to the Accounts Receivables Management ("ARM") industry. We hope that the ARM industry, and those that are part of the financial services space, are provided with guidance on how the CCPA applies to our activities when the rules are designed.

1. Categories of Personal Information

For debt collectors, the categories of personal information collected are very simple: (1) information that helps the collector identify the correct consumer/responsible party who owes the debt, (2) information that assists the collector with contacting the consumer (e.g. contact information for the consumer), (3) information about the debt, such as account specific information, (4) and payment information for the consumer once the consumer agrees to repay their account.



535 El Canyon Parkway, Suite 100
Livermore, CA 94551

2. Exceptions to CCPA

We ask that the rules provide more information about CCPA's exceptions. Specifically:

- (1) Does the Fair Credit Reporting Act (FCRA) exception set forth in §1798.145(d) apply to data that is furnished to credit reporting agencies? Information furnished under the FCRA is not "sold" to/from the consumer reporting agency (refer to the FCRA's regulation at 12 C.F.R. § 1022.40 et seq. for more information about data furnishing under the FCRA). Accordingly, it is unclear whether this exception would apply to furnishing data. We believe that it would be appropriate for furnishing information to fall under this exception.
- (2) We recommend that the rules confirm that the Gramm-Leach-Bliley Act (GLBA) exception set forth in §1798.145(e) extends to the activities related to debt collection. Debt collectors provide services to financial institutions and are subject to provisions of the GLBA, such as its Safeguards Rule. Accordingly, debt collectors collection and processing of consumer personal information should fall under this exception.

3. Submitting or Complying with Requests

If a business receives a consumer request to delete their personal information, and the business may rely upon one of the exceptions set forth in §1798.105, we ask that the rules provide guidance on how to respond to the consumer. A standard form or template is recommended so that there is consistency amongst businesses with how a consumer is responded to in this situation.

Additionally, we ask that the rules provide examples under each of the exceptions listed in §1798.105(d). For example, there are many different state and federal record retention guidelines that a debt collector must follow. It would be helpful for the AG to explain how a business may rely upon the applicable exception in a situation such as this.

4. Uniform Opt-Out Logo/Button

If a company does not "sell" consumer data and/or does not fall under the definition of a "business" under the Act, we ask that you provide clarification whether a company is still obligated to post the opt-out button on its website. Our recommendation is that a business would not be required to do so since its presence on a website may confuse and/or mislead a consumer to thinking that the company does in fact sell personal information. We ask that you provide standard language that a company can post on its website in lieu of the opt-out button if it does not sell information.

5. Notices and Information to Consumer

Section 1798.100(b) of the CCPA requires that *"A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purpose for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section."*

Regarding this section, we have multiple comments for consideration:



- (1) **We ask that the rules clarify this requirement only applies to when the information is being collected from the consumer.** If not, then compliance with this requirement is virtually impossible. For example, often when an account is in collections, it is because the creditor or the debt collector do not have updated or correct contact information for the consumer. When this is the case, collectors will collect information about the consumer (often through third parties) to find updated or correct contact information for a consumer. This process of collecting information about the consumer in order to contact them is called skip-tracing. If a debt collector may not collect information about the consumer without first providing written notice to the consumer pursuant to §1798.100(b), this will restrict a collector's ability to skip trace. Skip tracing is a lawful means to obtain a person's updated contact information, and the FDCPA has specific rules governing what can and cannot be disclosed with third parties during this activity. If consumers are not aware of their debts, then this ultimately harms them (i.e. if they can't be contacted to resolve their debts voluntarily, then debt collectors turn to alternative means to collect a debt, such as through litigation or Administrative Wage Garnishment). Accordingly, we recommend that the rules clarify that §1798.100(b) applies when the information is being collected directly from the consumer.
- (2) Section 1692e(11) of the federal FDCPA requires that collectors disclose in any initial communication with a consumer that the debt collector is "attempting to collect a debt and that any information will be used for that purpose." This phrase is commonly referred to as the "mini-Miranda" and is given at the very beginning of a conversation once a debt collector knows he/she is interacting with the consumer. Although the mini-Miranda is only required in the initial communication with a consumer, it is common practice for a debt collector to provide the mini-Miranda in each communication/interaction with the consumer (e.g. phone call, written communication, online disclosure when logging into an account, etc.) The mini-Miranda is designed to instill transparency between the collector and the consumer – so that the consumer is informed that any information obtained by the debt collector will be used for the purpose of debt collection. **As such, we recommend the AG approves a rule that clarifies that if a collector provides the mini-Miranda to a consumer during a communication or interaction with them, that this would be sufficient to meet §1798.100(b)'s requirement.**
- (3) In order to avoid an unauthorized disclosure and protect a consumer's privacy under the FDCPA, a collector is not allowed to disclose that he/she is a debt collector, the reason for the call, or even the name of their employer to a third party without being asked (see §1692b of the FDCPA). As such, collectors will ask a person to authenticate their identity to ensure they are speaking with the correct person/consumer before disclosing information about a debt in order to avoid an unauthorized third-party disclosure in violation of the FDCPA. Authentication usually involves the collector asking a person they suspect is the consumer to provide/confirm some combination of personal information such as their name, address, date of birth, and/or last four digits of their Social Security number (SSN). This allows the collector to compare that information against the information in their



collection records to determine if they have reached the right party (i.e. the consumer). This process ensures compliance with §§1692b and 1692c(b) of the FDCPA.

As this process illustrates, the FDCPA necessarily requires a collector “collect” consumer information before they may disclose the reason for the call, their identity as a debt collector, or any information related to the debt. It seems, therefore, that §1798.100(b) would require that a collector disclose at the time it asks a person to authenticate their identity the *purpose* for which that information is being collected. If so, this may cause violations of the FDCPA as explained above. **We recommend that the rules clarify that when a collector is asking for personal information to compare it with information already in their possession, that §1798.100(b) is not applicable.**

- (4) Section 1798.130(a)(2) states that when a business discloses and delivers information to the consumer pursuant to a request they have made under CCPA, that the business should deliver that information through the “consumer’s account with the business.” This assumes that the account a consumer will have with the business is an *online* account – which is not always the case. For example, a consumer who is in collections will have an “account” with the collection agency but that does not mean that the account is accessible online. We are simply pointing this out so that the rules can consider this when writing rules.

Additionally, we ask that the rules provide explanation what a “readily useable format” is under §1798.130(a)(2). Does this include, for example, an Excel type of spreadsheet?

6. Verification of a Consumer’s Request

Under both the FDCPA and the Rosenthal Act, a debt collector may not disclose anything about a consumer’s debt to an unauthorized third party. Case law has established that even confirming to a third party that a consumer has an account with the debt collector is enough to breach a consumer’s privacy under these Acts. Accordingly, in order to determine if a collector has reached the correct person, it is common for a collector to ask the person they are speaking with to authenticate their identity by confirming/providing their name, address, date of birth, and/or last four digits of their Social Security Number (SSN). Many of our federal clients require that we authenticate a person’s identity with their SSN. Accordingly, we recommend that if a consumer is requesting that a debt collector disclose the categories and/or specific pieces of personal information they have collected about them, that a financial services company be able to require a consumer (or an authorized third party) to authenticate in any manner consistent with how they currently authenticate a consumer’s identity to comply with applicable laws.


Additionally, the CCPA allows an authorized third party to request information on behalf of a consumer. We ask that the rules provide guidance to businesses about *how* to authenticate the third party’s identity and authority to request such information on behalf of the consumer. This is of great importance in our modern day and age where identity



theft is a real threat. If a consumer's identity is stolen, how does a business protect that consumer from a fraudster who has enough information to "verify" the consumer's identity, potentially giving a fraudster the ability to gather *more* information on their victim? Given the expansive definition of "personal information," a fraudster could in theory gain access to an enormous amount of consumer personal information by using the CCPA. We ask that the rules contemplate this and provide guidance to businesses on how to comply with the CCPA while also best protecting a consumer's privacy and personal information.

Should you or your staff need a knowledge resource in the ARM industry, please know that Performant Recovery would welcome any opportunity to assist you and your staff in this manner.

Sincerely,


Lauren Valenzuela, Esq.
Compliance Counsel



Message

From: Farber, David [REDACTED]
Sent: 3/8/2019 11:34:15 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Susan Murdock [REDACTED]
Subject: Comment Letter -- California Consumer Privacy Act
Attachments: ACP Comment Letter to Attorney General Becerra - March 8 2019.pdf

To Whom it May Concern:

On behalf of the Association of Claims Professionals, enclosed is a comment letter related to the California Consumer Privacy Act. Please contact us if you have any questions or if we can provide any additional information.

Thank you for consideration of these comments.

David Farber

Counsel to the ACP

David Farber : King & Spalding

1700 Pennsylvania Avenue, NW

Washington, D.C. 20006

[REDACTED]

[REDACTED]

[REDACTED]

King & Spalding Confidentiality Notice:

This message is being sent by or on behalf of a lawyer. It is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is proprietary, privileged or confidential or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message.

CCPA00000331



March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

RE: Preliminary Rulemaking Activities related to The California Consumer Privacy Act

Ladies and Gentlemen:

The Association of Claims Professionals (ACP) is pleased to respond to the request for comment on the Preliminary Rulemaking Activities related to The California Consumer Privacy Act (CCPA). While ACP members are strong proponents of individual privacy rights, we have significant concerns that the unintended application of the CCPA to claims professionals will cause widespread confusion and discord among California consumers and result in conflicting regulatory standards for our members. As such, for the reasons below, we ask the California Department of Justice to clarify the intent of the legislature that the CCPA does not apply to the activities of independent claims professionals.

ACP's Interest in Preliminary Rule Making Activities

ACP (formerly known as the American Association of Independent Claims Professionals or AAICP) was formed in 2002 as the only national association representing the interests of the nation's independent claims professionals. ACP members employ thousands of claims specialists and other professionals across the country and handle millions of property and casualty, workers' compensation, disability, and other liability claims annually. Membership is comprised of independent claims adjusters and third-party administrator organizations, many of whom handle claims administration responsibilities for California insureds and their carriers. ACP member companies employ thousands of adjusters in the State of California and manage billions of dollars of claims for California insurers and policyholders.

Comments on the CCPA

- I. The Department Should Clarify that the Claims Adjusting Industry is Exempt from the CCPA.**
 - 1. The California Insurance Code, Labor Code, and health laws extensively regulate the claims adjusting industry in the area of transparency and privacy and already provide greater protection specific to insured consumers.**

The CCPA was intended to fill in gaps in California privacy law, which is why the California legislature believes existing law should be construed to harmonize with the CCPA *if possible* but preempts the CCPA in the event of a conflict.¹ Moreover, California has specifically and comprehensively addressed transparency and privacy in the claims adjusting industry in a manner that provides greater protection to the consumer than what will be afforded under the CCPA when it is implemented. Given this extensive existing regulation, the Department should clarify that the CCPA does not apply to the claims adjusting industry to avoid conflicting regulation, an uncertain preemption analysis, and to protect consumers.

Perhaps most notably, the California Insurance Information and Privacy Protection Act (IIPPA) regulates the claims management industry as “Insurance Support Organizations” in the context of certain insurance transactions for substantially the same purpose as the CCPA.² Indeed, not only are the purposes of the IIPPA substantially similar to the CCPA, but the protections contained within the IIPPA mirrors if not exceed much of the CCPA. For example, insurance institutions or agents must provide a “notice of information practices” upon delivery of a policy or collection of personal information that includes all of the information the CCPA would require *plus* the investigative techniques used to collect such information. Not only that, but California insureds already have rights pursuant to the IIPPA to access, amend, correct, and delete certain information in a manner that actually makes sense in the insurance context.³

Other aspects of the California Insurance Code, Labor Code, and health laws have also required transparency and privacy protection for years. Administrators must provide written notice explaining its relationship with the insurer and policyholder “agents of insurers” and face criminal penalties for unauthorized disclosure of confidential information. The Labor Code severely limits what medical information may be disclosed when processing worker’s compensation claims.⁴ Relatedly, where the CCPA allows requests for the disclosure of relationships with third parties related to a consumer’s personal information, the Insurance Code already requires administrators to provide written notice advising insured individuals of the identity of details regarding the relationship between the administrator, policyholder,

¹ See Cal. Civ. Code §1798.175.

² See Cal. Ins. Code § 791 (“[T]o establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions by insurance institutions, agents or insurance-support organizations; to maintain a balance between the need for information by those conducting the business of insurance and the public’s need for fairness in insurance information practices, including the need to minimize intrusiveness; to establish a regulatory mechanism to enable natural persons to ascertain what information is being or has been collected about them in connection with insurance transactions and to have access to such information for the purpose of verifying or disputing its accuracy; to limit the disclosure of information collected in connection with insurance transactions; and to enable insurance applicants and policyholders to obtain the reasons for any adverse underwriting decision.”); Cal. Ins. Code § 791.02 (defining “insurance support organization”).

³ See Cal. Ins. Code § 791.08. Similar to the CCPA, access requests must be honored within 30 days, although unlike section 1798.100(d), the IIPPA allows a reasonable fee for the expenses incurred, which is not a difference in the level of privacy protection but rather a reasonable business practice. See Cal. Ins. Code §791.10.

⁴ See Cal. Ins. Code §§ 1759.9, 1877.4; Cal. Lab. Code § 3762.

and insurer.⁵ In the context of workers compensation insurance, “agents of insurers” are obligated to keep information confidential and face criminal penalties for unauthorized disclosure of such information.⁶

As referenced above, in addition to the Insurance Code the California Labor Code also limits disclosure of medical information insurers and third party administrators retained by self-insured employers to administer workers’ compensation claims receive to: (1) medical information limited to the diagnosis of the mental or physical condition for which workers’ compensation is claimed and the treatment provided for this condition; and (2) medical information regarding the injury for which workers’ compensation is claimed that is necessary for the employer to have in order for the employer to modify the employee’s work duties.⁷ Again, these protections are greater than those which will be afforded by the CCPA, arguing in favor of a blanket exemption from the CCPA for independent claims adjusters.

Beyond both the Insurance and Labor Codes, a third law -- the Confidential Medical Information Act (CMIA) -- also restricts the use and disclosure of any medical information claims professionals receive. For example, “[n]o person or entity engaged in the business of furnishing administrative services to programs that provide payment for health care services shall knowingly use, disclose, or permit its employees or agents to use or disclose medical information possessed in connection with performing administrative functions for a program, except as reasonably necessary in connection with the administration or maintenance of the program, or as required by law, or with an authorization.”⁸ Further, when claims professionals (“that provide[] billing, claims management, medical data processing, or other administrative services for providers of health care or health care service plans or for insurers, employers, hospital service plans, employee benefit plans, governmental authorities, contractors, or other persons or entities responsible for paying for health care services rendered to the patient receive medical information from health care providers and health care service plans”) receive medical information from health care providers or health care service plans, they cannot further disclose the information in a way that would violate the CMIA.⁹

California has already enacted a significant body of law to increase transparency for and protect the privacy of insured California consumers. If the CCPA was interpreted to apply to the claims adjusting industry the result would be a complicated patchwork quilt of regulation that lessens, rather than increases, consumer privacy. Further, application of the CCPA to the claims management industry would result in uneven application of the law given that each company would need to apply a complicated preemption analysis to nearly every right in the CCPA and decide if existing law or the CCPA is more stringent in the particular scenario.

⁵ See Cal. Ins. Code § 1759.9.

⁶ See Cal. Ins. Code § 1877.4.

⁷ See Cal. Lab. Code § 3762.

⁸ Cal. Civ. Code § 56.26(a).

⁹ See Cal. Civ. Code § 56.10(c)(3).

2. Where the CCPA may be said to apply, the law already contains explicit exceptions for key aspects of the claims adjusting industry, creating confusion for consumers.

The application of the CCPA to the claims adjusting industry will result in widespread consumer confusion without providing additional privacy or transparency protections. Where the law could arguably be read to apply, the CCPA exempts nearly all of the personal information the claims management industry receives in order to process claims: medical information governed by the CMIA, protected health information (PHI) collected as a business associate under HIPAA, information collected as part of a clinical trial, information in consumer credit reports, and in some cases, financial information disclosed pursuant to federal and California law. It is unclear and debatable whether any remaining information that does not fit neatly into the above exempt categories would be subject to CCPA obligations.

Further, claims management activities will constantly trigger CCPA exceptions, particularly when it comes to deletion requests directly from consumers or indirectly from businesses subject to the CCPA. The application of exceptions, which are needed to comply with existing law, will create confusion and likely frustration for consumers trying to exercise CCPA rights.¹⁰ For example, administrators will be exempt from deleting information related to transactions they are required to maintain confidentially in books and records and make available to insurers for at least five years pursuant to existing legal obligations.¹¹ In other words, insureds that lodge deletion requests in accordance with the CCPA rather than the proper procedure for the insurance context provided by the IIPPA will fall within an exception and therefore be rendered meaningless. This is why in addition to drafting the legal obligation exception to deletion requests, the CCPA repeats that the law is not intended to restrict the ability to comply with other laws.

As noted above, wherever the CCPA may be stretched to cover any remaining claims management activities that are not already facially exempt based on the category of information, the law will nevertheless constantly provide exception. Not only does this create a genuine question for members of the claims adjusting industry as to whether the CCPA is relevant to them, but it will undoubtedly create confusion and likely frustration for consumers and CCPA-regulated businesses that may not understand why the industry is exempt from complying with so many of their requests. To avoid both outcomes, the Department should issue a clear statement exempting the independent claims adjusting industry from the scope of the CCPA.

¹⁰ The most common exceptions will include (1) to complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer; (2) to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business; (3) to comply with a legal obligation; or (4) to otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information. See Cal. Civ. Code §1798.105(d).

¹¹ See Cal. Ins. Code § 1759.3.

3. The California legislature did not intend the CCPA to further regulate the pro-consumer claims adjusting industry; the Department should make that explicitly clear.

The preamble to the CCPA emphasizes the intent of the California legislature to create privacy protections in response to business practices proliferated by the age of big data, while acknowledging existing law has already provided such protection in various other contexts. California had the same concerns regarding transparency and privacy protection in the claims management and broader insurance industry and intentionally addressed these concerns effectively throughout the state's legal code. Claims adjusters are specifically covered by existing law. The adjusting industry works on behalf of individuals and businesses in times of need, such as the recent California wildfires, delivering an estimated \$45 billion each year in claims payments. It would be deeply unfortunate if the CCPA were to unintentionally sweep up claims adjusters and double-regulate the industry, likely lessening today's existing protections. These unnecessary gray areas would disrupt functioning privacy compliance programs in the claims industry and even worse, burden claims recovery efforts from proceeding as quickly and smoothly as possible. It is clear that the California legislature intended the CCPA to exempt claims adjusters -- the Department's regulations should remove any ambiguity and clearly reflect that intent.

ACP appreciates the opportunity to provide comments on the Preliminary Rulemaking Activities related to the CCPA. If you have any questions concerning our comments, or if we can be of further assistance, please contact Susan Murdock at [REDACTED]. We thank you for consideration of these comments and welcome any further questions you may have.

Sincerely,



Susan R. Murdock
Executive Director
Association of Claims Professionals
1700 Pennsylvania Avenue, Suite 200
Washington, DC 20006
[REDACTED]

www.claimsprofession.org

Message

From: Bryan Montgomery [REDACTED]
Sent: 1/29/2019 5:57:00 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comment Letter AB375 Implementation
Attachments: SKM_C45819012911380.pdf

Please see the attached comment letter from Oakley Mayor Claire Alaura.

Thank you!

CITY COUNCIL
Claire Alaura, Mayor
Doug Hardcastle, Vice Mayor
Sue Higgins
Kevin Romick
Randy Pope



CITY HALL
3231 Main Street
Oakley, CA 94561
[REDACTED]
925.625.9859 fax
www.ci.oakley.ca.us

January 30, 2019

CA Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street, Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Thank you for the opportunity to comment on the Department's implementation plans for AB 375. These comments presented herein may not align perfectly with the intended privacy provisions of the new law; however, a recent social media threat experienced within the City of Oakley leads us to submit these comments for your consideration.

By way of background, in August of last year a series of violent threats were made via social media (Snapchat) to some underage female students at Freedom High School located in Oakley. The same account holder then began to distribute more threatening messages, first to a group of other students, and then progressed to making violent threats to the entire campus and school staff. Because of the malicious threats, members of our community were terrorized and some suffered significant psychological trauma, wondering if the subject would follow through on his statements. School attendance at all of our campuses was impacted and disrupted by the actions of this individual. Dozens of law enforcement officers, including the State Department of Justice and the FBI worked tirelessly to determine who was making these threats. A key frustration was the ability for the account holder to maintain complete anonymity, coupled with the significant lack of cooperation from Snapchat – citing the privacy of their customers. Fortunately, the person making the threats made a critical error while posting a threat, was located, arrested and is now being prosecuted by the Contra Costa District Attorney's Office.

This experience leads us to recommend that the Department seriously consider a requirement that anyone creating email addresses and establishing social media profiles provide valid and verified contact information. Further, the email and social media companies should have a



Celebrate Oakley 20 Years!

clearly designated contact for law enforcement. One of the initial problems that we had with our investigation was getting anyone from Snapchat to talk with us. If law enforcement has a problem or issue it should be able to call the company and tell them about the problem and then get guidance on how their company responds to criminal events involving their business. With Snapchat, there was no way for us to talk to anyone. They publish no telephone numbers, they have no law enforcement contact information - nothing. We need laws and regulations that require social media companies doing business in California to have a law enforcement reference guide that lets the 5,000 police agencies across the country know how they can talk to someone about the company's product, how to get an account suspended immediately, how the police agency can get the information that they need to learn about the basics of a subscriber, and more about the services that subscribers are able to access through the social media company.

It appears the intent of SB 375 is to protect consumer privacy, but please consider the experience in Oakley as a reminder that the bad actors of the world can inappropriately take advantage of such protections – particularly if an entity like Snapchat can thwart a criminal investigation under the guise of privacy. As you might expect, this incident caused significant angst in our community, and we very much hope the Department considers regulations that keep the investigatory needs of law enforcement in mind as AB 375 is implemented.

Respectfully submitted,



Claire Alaura
Mayor



Eric Christensen
Chief of Police

cc: Senator Steve Glazer
Oakley City Council



Celebrate Oakley 20 Years!

Message

From: [REDACTED]
Sent: 3/6/2019 1:41:35 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comment Letter on CCPA
Attachments: Comment letter on CCPA.docx
Flag: Follow up

Dear Privacy Regulations Coordinator,

Please find attached our comment letter regarding the California Consumer Privacy Act of 2018. We hope you find it useful. We look forward to your rulemaking this fall.

Thank you.

Jay Hartlove, CRCM
Compliance Manager
[REDACTED]

[REDACTED]
Patelco Credit Union | 5050 Hopyard Rd, Pleasanton, CA 94588



===== DISCLAIMER =====

Information contained herein is the sole and exclusive property of Patelco Credit Union. The information within this document or item is confidential; it shall not be disclosed to a third party or used except for the purpose of the recipient providing a service to Patelco Credit Union or for the benefit of Patelco Credit Union. Your retention, possession or use of this information constitutes your acceptance of these terms.

Please note that the sender accepts no responsibility for viruses and it is your responsibility to scan attachments (if any).

Dear Attorney General:

I am writing to you representing Patelco Credit Union which serves over 350,000 members in Northern California, and has over \$6.8 billion in assets. Thank you for this opportunity to give our input on the implementation of the California Consumer Privacy Act (CCPA).

The law, as amended in September 2018, does not give a clear plan for how companies are to respond to consumers exercising their new rights. In your crafting of regulations to implement this law, please address the following points.

Section 1798.145(e) exempts data from this law that is collected under the Gramm Leach Bliley Act (GLBA) or the California Financial Information Privacy Act (FIPA). As a federally insured California credit union, nearly all the personal identifying information (PII) we collect is protected under GLBA and all the PII we share with third parties is protected under FIPA. Does that mean we can advise consumers this data is already protected under other laws and is not available for viewing or deletion under the CCPA?

If this is a correct reading, we will need safe harbor disclosures, for both points where we take in information and for public posting of policy. This safe harbor disclosure should tell consumers their data is already protected under existing laws. May we suggest wording such as this. "The California Consumer Privacy Act of 2018 gives you certain rights over the personal data we collect about you that is not already protected by existing privacy laws. The personal data we collect about you for supplying you with our financial products and services is already protected under existing federal and California state privacy laws, and is therefore exempt from the new California law."

We will also need similar safe harbor disclosures for rejecting a deletion request under Section 1798.105.

What are the categories of data and the categories of sources of data under Section 1798.110 and 1798.115? Does Section 1798.115 only cover data that is collected outside GLBA and FIPA, since those are exempted?

How is Section 1798.120 different from the FIPA opt-out financial institutions already follow?

Section 1798.100 says consumers can request access to their data. Signatories on contracts with our credit union are not consumers of our goods, they are employees of suppliers of services to the credit union. Their data, such as names, email addresses, and phone numbers, should be exempt from this law. Their names often end up on vendor lists and strategy documents that we cannot disclose without jeopardizing confidentiality, competitiveness, and trade secrets.

Section 1798.145(h) says we can share information with service providers and not be liable for a service provider breach if at the time we shared the data, we did not know or have reason to believe the vendor was going to leak the data. Under GLBA, we do thorough information security due diligence on all the vendors with which we share our member data. What further protections or duties does this section add to GLBA?

Section 1798.145(h) also exempts data bought or sold to or from consumer reporting agencies. The implementing regulation should clarify this exemption covers any use of said data that is already covered under FCRA and FDCPA.

Does this law cover the data we passively collect from our online users, for whom we may or may not assign a random identifier, but do not collect any personally identifying data? Since we never learn who they are, how are we to gather and disclose their data if they approach us to exercise their new rights under this law? We do not match these scraps of data with any other data to create personally identifying information. The law defines covered data too broadly. We agree that data that is matched to become PII should be covered, but if non-PII is not matched, it poses no threat to a consumer's privacy. Might the implementing regulation limit coverage to data where we can tell who it belongs to?

We collect transaction information including IP addresses, geolocation, and spending patterns in our efforts to protect against fraudulent activity. We do not share this information with anyone other than our service provider who gives us the data. Is all this data exempt under Sections 1798.100 and 1798.105? We need a regulation that clarifies such a blanket exemption for data used in fraud detection.

We would never give preferential treatment or incentives to a consumer for allowing us to share their PII. We think this creates opportunities for discrimination that run counter to the stated intent of the law to not discriminate. We recommend this portion of Section 1798.125 be nullified in the implementing regulation.

Credit unions network together to share branches and ATMs to give our members greater transactional access. Section 1798.100 says businesses do not need to disclose one-time transaction data if that data is not sold or matched up with other data to create personally identifiable information. Can we please have a clarification in the regulation that transaction data moved through shared networks is not brought under this law because other credit unions handled the data in stream?

California Labor Code 1198.5 gives employees and former employees the right to see and copy information in their personnel records. How is this access different under the CCPA? The CCPA should exempt data and disclosures that are already covered by Labor Code 1198.5.

In summation, the regulations that implement this law need to cover the situations companies will face. The law describes a general scheme of what is protected and what is not. We need to know how to apply the concept into specifics.

Thank you again for the opportunity to add our concerns to your deliberations.

Sincerely,

Jay Hartlove
Compliance Manager
Patelco Credit Union

A solid black rectangular box used to redact the signature of Jay Hartlove.

Message

From: Paul Donahue [REDACTED]
Sent: 3/8/2019 2:01:49 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: [REDACTED]
Subject: Comment Letter Re: CCPA / Subject: Workers' Compensation
Attachments: Comment Letter - CA DOJ Privacy Regs. Coordinator RE - Workers Comp. (3-8-19).pdf

Greetings:

Attached to this email are written comments concerning the Privacy Regulations, now under pre-rulemaking consideration by the Department of Justice pursuant to the CCPA.

The comments are submitted on behalf of the following entities:

American Association of Payers, Administrators and Networks (AAPAN)
Anthem Workers' Compensation
Coventry
MEDEX Healthcare
Risk and Insurance Management Society (RIMS) – California
Small Business California

Thank you for for consideration.

Very truly yours,

Paul Donahue
Kammerer & Company, Inc.
[REDACTED]

[attachment]

Kammerer & Company, Inc.

1215 K Street, 17th Floor

SACRAMENTO, CA 95814

March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

VIA EMAIL ONLY
privacyregulations@doj.ca.gov

TO WHOM IT MAY CONCERN:

This Comment Letter is submitted on behalf of the following entities:

American Association of Payers, Administrators and Networks (AAPAN)
Anthem Workers' Compensation
Coventry
MEDEX Healthcare
Risk and Insurance Management Society (RIMS) – California
Small Business California

**The Attorney General Should Exempt the Workers' Compensation System
From the California Consumer Privacy Act**

The California Consumer Privacy Act (CCPA) directs the Attorney General to adopt regulations to further the purposes of the CCPA, including “...[e]stablishing any exceptions necessary to comply with state or federal law, ... within one year of passage of this title and as needed thereafter.”¹

**An Exception From CCPA is Necessary to Comply With the California Constitution
and State Laws Governing the Workers' Compensation System**

1) The workers' compensation system is established and regulated pursuant to the state Constitution.

The state Constitution confers plenary power on the Legislature to enact a comprehensive worker's compensation system. Section 4 of Article XIV of the state Constitution vests the Legislature with “plenary power, unlimited by any provision of this Constitution, to create, and enforce a complete system of workers' compensation, by appropriate legislation.”² This constitutional mandate gives the Legislature “complete, absolute and unqualified power to create

¹ Civil Code §1798.185 (a) (3)

² Cal Const. Article XIV, § 4

and enact the workers' compensation system."³ California courts have interpreted this grant of broad power to mean that "absolutely nothing" in Section 4 "purports to limit the Legislature's authority to enact additional appropriate legislation for the protection of employees."⁴

The constitutional grant of power has "compelled the conclusion" that Section 4 of Article XIV of the state Constitution supersedes the state Constitution's Due Process clause with respect to legislation passed under the Legislature's plenary powers over the workers' compensation system.⁵ Courts have held that, even if conflicts existed between Section 4 [workers' compensation] and other state Constitutional provisions governing Separation of Powers or Due Process, "the plenary powers conferred by Section 4 would still control."⁶

The courts have unambiguously held that the provisions of the California Constitution governing workers' compensation are not limited by other provisions of the state Constitution, including the Due Process and Separation of Powers clauses.

These interpretations lead to a likely conclusion that, by its own terms, the constitutional provisions governing workers' compensation will also control over state constitutional provisions in Section 1 of Article I pertaining to the right to Privacy, so long as the Legislature has employed its "...plenary power, *unlimited by any provision of this Constitution*, to create, and enforce a complete system of workers' compensation, by appropriate legislation."⁷

2) Pursuant to its constitutional mandate, the Legislature by statute has enacted a comprehensive workers' compensation system.

Section 4 of Article XIV of the state Constitution provides in part that "[a] complete system of workers' compensation includes...full provision for vesting power, authority and jurisdiction in an administrative body with all the requisite governmental functions to determine any dispute or matter arising under such legislation." The intent behind Section 4 "was to endow [the Legislature] expressly with exclusive and 'plenary' authority to determine the contours and content of our state's workers' compensation system."⁸ The only limitations on the Legislature's plenary powers are that the Legislature cannot act outside of its authority to create and to enforce

³ *Facundo-Guerrero v. Workers' Comp. Appeals Bd.* (2008) 163 Cal.App.4th 640, 650 [intent behind Section 4 "was to endow [the Legislature] expressly with exclusive and 'plenary' authority to determine the contours and content of our state's workers' compensation system"].

⁴ *City and County of San Francisco v. Workers' Comp. Appeals Bd. (Wiebe)* (1978) 22 Cal.3d 103, 114

⁵ *Hustedt v. Workers' Comp. Appeals Bd.* (1981) 30 Cal.3d 329, 343 ["It is well established that adoption of [Section 4] 'effected a repeal pro tanto' of any state constitutional provisions which conflicted with that amendment"]; see also *Greener v. Workers' Comp. Appeals Bd.* (1993) 6 Cal.4th 1028 [article VI of the state Constitution governing courts' jurisdiction inapplicable to extent Legislature has exercised its powers under Section 4]

⁶ *Stevens v. Workers' Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

⁷ (Emphasis added) Cal Const. Article XIV, § 4

⁸ *Facundo-Guerrero v. Workers' Comp. Appeals Bd.* (2008) 163 Cal.App.4th 640, 650

a complete system of workers' compensation or enact a provision that conflicts with federal law.⁹ The state Constitution, and the cases interpreting it, confirm that “nearly any exercise of the Legislature's plenary powers over workers' compensation is permissible so long as the Legislature finds its action to be ‘necessary to the effectiveness of the system of workers' compensation.’ ”¹⁰

Acting under this power, the Legislature enacted the workers' compensation law to govern compensation to California workers who are injured in the course of their employment.¹¹

The underlying premise behind this statutorily created system is the “compensation bargain, [under which] the employer assumes liability for industrial personal injury or death without regard to fault in exchange for limitations on the amount of that liability. The employee is afforded relatively swift and certain payment of benefits to cure or relieve the effects of industrial injury without having to prove fault but, in exchange, gives up the wider range of damages potentially available in tort.”¹² The workers' compensation law requires employers to secure the payment of workers' compensation benefits either by purchasing third-party insurance or by self-insuring with permission from the Department of Industrial Relations.¹³

In addition, where the “conditions of compensation” exist, the right to recover such compensation is the “sole and exclusive remedy” of the employee or his or her dependents against the employer when acting within the scope of his or her employment.¹⁴

3) Existing privacy protections in the workers' compensation system

There are several privacy requirements within the Labor Code directly applicable to workers' compensation. Labor Code Section 138.7 provides in part:

“A person or public or private entity not a party to a claim for workers' compensation benefits shall not obtain individually identifiable information obtained or maintained by the division on that claim. For purposes of this section, ‘individually identifiable information’ means any data concerning an injury or claim that is linked to a uniquely identifiable employee, employer, claims administrator, or any other person or entity.”

⁹ *Hustedt v. Workers' Comp. Appeals Bd.* (1981) 30 Cal.3d 329; see also, *Stevens v. Workers' Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

¹⁰ *Stevens v. Workers' Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

¹¹ Division 4 (commencing with Section 3200) of the Labor Code

¹² *Charles J. Vacanti, M.D., Inc. v. State Comp. Ins. Fund* (2001) 24 Cal.4th 800, 811. See also, *Shoemaker v. Myers* (1990) 52 Cal.3d 1

¹³ Labor Code § 3700

¹⁴ Labor Code § 3602 (a)

There are limited exceptions to that rule, but it is unlawful for any person who has received individually identifiable information from the division pursuant to this section to provide that information to any person who is not entitled to it.¹⁵ In a similar way, Labor Code Section 3762 (c) states:

“An insurer, third-party administrator retained by a self-insured employer pursuant to Section 3702.1 to administer the employer’s workers’ compensation claims, and those employees and agents specified by a self-insured employer to administer the employer’s workers’ compensation claims, are prohibited from disclosing or causing to be disclosed to an employer, any medical information, as defined in Section 56.05 of the Civil Code, about an employee who has filed a workers’ compensation claim, except as follows: (1) Medical information limited to the diagnosis of the mental or physical condition for which workers’ compensation is claimed and the treatment provided for this condition. (2) Medical information regarding the injury for which workers’ compensation is claimed that is necessary for the employer to have in order for the employer to modify the employee’s work duties.”

Insofar as electronic billing purposes are concerned, Labor Code Section 4603.4 (b) specifies that that billing standards developed by the Division of Workers’ Compensation (DWC), “...shall be consistent with existing standards under the federal Health Insurance Portability and Accountability Act of 1996.”

Labor Code Section 4610.5 (m) states that when a claims administrator is transmitting medical records pursuant to a request for independent medical review, “The confidentiality of medical records shall be maintained pursuant to applicable state and federal laws.” Confidentiality of medical information was also addressed by the Legislature in Labor Code Section 4903.6 (d):

“With the exception of a lien for services provided by a physician as defined in Section 3209.3, a lien claimant shall not be entitled to any medical information, as defined in subdivision (g) of Section 56.05 of the Civil Code, about an injured worker without prior written approval of the appeals board. Any order authorizing disclosure of medical information to a lien claimant other than a physician shall specify the information to be provided to the lien claimant and include a finding that the information is relevant to the proof of the matter for which the information is sought.”

In summary, privacy protections within the Labor Code extensively address protection of medical information.

4) Workers’ Compensation is a comprehensive statutory medical, legal and adjudicatory system that is incompatible with the provisions of the CCPA.

Each day, personal and medical information concerning hundreds of thousands of injured workers is circulated from a Medical Provider Network (MPN) or insurance claims administrator

¹⁵ Labor Code § 138.7

to the physician, to the physician specialist to whom an injured worker may be referred, to the Utilization Review Organization, an Independent Medical Review (IMR) service, an Independent Bill Review (IBR) organization, and Electronic Billing Review organization, Pharmacy Benefit Managers, Vocational Rehabilitation Counselors, Job Training and Supplemental Job Displacement Benefit entities, and more.

Additionally, MPN administrators and self-insured employers are required to report injured workers medical information to the Office of Self-Insured Plans, Workers' Compensation Information System, Workers' Compensation Appeals Board and the Workers' Compensation Insurance Rating Bureau, all mandatory reporting requirements that would trigger disclosure notifications under the CCPA.

Because an injured worker cannot, and would clearly not wish to frustrate the adjusting of a claim by not allowing information to be disclosed to those who are integral to the workers' compensation medical treatment and benefit payment system, the disclosures nevertheless must be provided to the workers' compensation claimant or applicant. Failure to do so can result in penalties and enforcement actions from the California Department of Justice and the Department of Industrial Relations.

For example, Civil Code § 1798.115(a) of the CCPA states that the consumer has a right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer (1) the categories of personal information that the business collected about the consumer, (2) the categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold, and (3) the categories of personal information that the business disclosed about the consumer for a business purpose.

Section 1798.115(a) would likely apply to nearly all workers' compensation claims transactions. As noted above, medical records are sent to a medical provider network (MPN), medical records are sent to a utilization review organization (URO), and medical records are sent to an independent review organization (IRO). "Personal information" would clearly include payment information sent to a payment processing center falling within the definition of "service provider." A vocational evaluator would clearly need to know "professional or employment-related information" that is included within the definition of "personal information" in Civil Code Sec. 1798.140(o)(1)(I).

During the routine administration of a workers' compensation claim, especially a claim involving indemnity benefits, considerable "personal information," as defined in Civil Code Sec. 1798.140(o), must be collected so that the claim can be processed and the injured worker can be treated and compensated. For physicians and other service providers, an injured worker's personal information is collected during the payment and remittance process. In addition, the placement of insurance, including providing and disclosure claims information, is a vital function in the workers' compensation system.

By law, workers' compensation claimants are considered "consumers" for purposes of the Insurance Information and Privacy Protection Act.¹⁶ Therefore, the notice of information practices required by Insurance Code Sec. 791.04 applies to workers' compensation insurers.

Although these are just a few examples, the fact remains that each and every referral or transmittal cited above would, pursuant to the CCPA, trigger a disclosure notification to the injured worker.

Yet, every one of these transactions are already governed by a comprehensive body of *existing state law*. Moreover, because workers' compensation is the sole and exclusive remedy for all injuries and illnesses that occur within the course and scope of employment, the injured employees would not be allowed to opt out of participation as is provided for within the CCPA.

Therefore, although an injured worker cannot prevent the adjusting of a claim by refusing to allow information to be given to workers' compensation service providers, the notification disclosures nevertheless must be sent if the CCPA were to apply. Failure to do so can result in penalties and enforcement actions from the Department of Justice.

5) A regulatory exception from CCPA is needed in order to comply with the comprehensive constitutionally mandated and legislatively enacted workers' compensation system.

The workers' compensation system is a unique body of state law that is breathtaking in its scope and applicability. The workers' compensation system has its own legal and court adjudication system. Medical treatment offered within the workers' compensation system is completely separate and apart from the state's health care delivery system. Nearly every aspect of an injured worker's medical care, vocational rehabilitation, and benefit payments is governed by state law and subject to extensive oversight by the Division of Workers' Compensation within the state Department of Industrial Relations.

This petition for an exception from CCPA in order to comply with state law, as authorized pursuant to Civil Code Section 1798.185 (a) (3), is presented herein on account of the fact that these extremely complex and comprehensive transactions that take place every day concerning the medical treatment and monetary benefits of injured workers in this state are already regulated extensively by an all-inclusive statutory structure.

Importantly, the right to recover compensation and treatment under the workers' compensation system is the sole and exclusive remedy for injury or death of an employee against the employer or co-employee acting within the scope of his or her employment,¹⁷ making participation in the workers' compensation system mandatory for both employers and employees.

Thus, we respectfully submit that all aspects of the workers' compensation statutory and constitutional system should be exempted entirely from CCPA. We therefore strongly urge that

¹⁶ Insurance Code § 791 et seq.

¹⁷ See, Labor Code, § 3602 (a)

the Attorney General adopt regulations to establish an exception from the CCPA for the workers' compensation system, as specifically authorized in Civil Code Section 1798.185 (a) (3):

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas: [...]

(3) *Establishing any exceptions necessary to comply with state or federal law*, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter. (Emphasis added)

Workers' compensation is a heavily regulated system, with an extensive body of statutory and constitutional laws governing it. We strongly believe that exempting workers' compensation from the CCPA is appropriate, and we respectfully urge this action be taken as it is "...*necessary to comply with state law*..."¹⁸

Suggested regulatory language is provided as follows:

Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code does not apply to medical or personal information collected by a business, medical provider network, third party administrator, insurer or other third-party entity for the purpose of providing medical treatment or administering claims pursuant to Division 4 (commencing with Section 3200) of the Labor Code.

Thank you for your consideration.

Sincerely,

Lori C. Kammerer
KAMMERER & COMPANY

cc: Assembly Member Ed Chau
Chair, Assembly Committee on Privacy and Consumer Protection
1020 N Street, Room 156A
Sacramento, CA 95814



¹⁸ Civil Code § 1798.185 (a) (3)

Message

From: Halpert, Jim [REDACTED]
Sent: 3/8/2019 10:42:26 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comment re CCPA Pre-Rulemaking.DOCX
Attachments: jjh -- Letter re CCPA Regulations.DOCX

Thank you for your consideration

Jim Halpert
Partner



DLA Piper LLP (US)
500 Eighth Street, NW
Washington, DC 20004
United States
www.dlapiper.com [\[dlapiper.com\]](http://dlapiper.com)

Please consider the environment before printing this email.

The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use, disclosure, dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please reply to the sender and destroy all copies of the message. To contact us directly, send to postmaster@dlapiper.com. Thank you.



DLA Piper LLP (US)
500 Eighth Street, NW
Washington, DC 20004
www.dlapiper.com

Jim Halpert

F 202.799.5441

March 8, 2019

Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

Dear Privacy Regulations Team,

I am writing you in my personal capacity – not on behalf of any client – with suggestions that I hope you will seriously consider including in Attorney General Becerra’s very important California Consumer Privacy Act (“CCPA”) rulemaking.

I am a Chambers and Legal 500 ranked lawyer with more than 22 years of privacy experience, have worked with lawyers for privacy organizations on potential clarifying amendments to the CCPA, and am currently helping many clients with practical CCPA compliance.

I write specifically to suggest that, as the Attorney General’s Office considers proposed rules regarding compliance with consumer requests, as required by §§ 1798.185(a)(7), (b) and (a)(3), it include provisions that:

(1) clarify and simplify obligations to comply with CCPA requests, for example through a “reasonable compliance” standard, or by specifying that businesses do not need to combine non-identifiable data with identifiable data or to search unstructured data in order to comply with a request.

(2) solve for the risk of fraudsters or battering spouses obtaining sensitive consumer data or business competitors obtaining authorization to opt out consumers out of competitors’ business activities, and

(3) as it develops a clear, uniform Do Not Sell My Personal Information button, it avoid First Amendment compelled speech obligations on businesses that do not sell personal information.

The CCPA is a path-breaking privacy law, and if clarified and implemented thoughtfully, can provide important new rights for California consumers in a way that can be scaled and implemented across the State. With appropriate clarifications and with public education as to the requirements of the law, consumers will see these rights respected. Without them, consumers are likely to be frustrated in the exercise of their rights and many California businesses and consumers will have great difficulty understanding it.

As your office is likely aware, the CCPA is a rambling, nearly 10,000 word law, whose sections are not organized by the rights that the law creates, and with statutory language contains numerous drafting errors (including cross-references to the wrong number, definitions that do not clearly relate to one another, contradictory language regarding the same obligation, and even a few stray words and phrases that were not fixed by legislative counsel).

What is more, while CCPA consumer rights are laudable overall, compliance with CCPA rights requests as to the huge range of non-identified data that is subject to the law is operationally very complex for most businesses (as discussed further below).

General Becerra has now put his name behind S.B. 561, a bill that would not only: (1) create potentially huge minimum statutory damage class action risk for any privacy violation of the CCPA, but would also (2) eliminate the 30 day right to cure that appears to be the only barrier to strict liability under the CCPA, and (3) relieve the AG's Office of the obligation to issue guidance regarding what the law means.

The AG's Office needs to include in its final rules clarifications that provide guidance about practical and efficient ways to comply with this law, including as to any definitional issues that the legislature does not clarify this legislative session. Without these clarifications, the CCPA risks being a source of significant and unnecessary confusion and anti-privacy defensive measures by businesses to combine all user "personal data" in one place in order to be able to respond fully to user requests.

Moreover, if S.B. 561 or similar legislation is enacted, the CCPA would become an intense source of wasteful litigation over both the many uncertainties in the law and technical violations, such as a failure by a well-intentioned defendant to locate and delete every piece of a California consumer's non-identified "personal data" (such as every IP address or device ID).

None of these consequences would materially advance privacy and all are avoidable, if the AG's Office considers and addresses in its final rules the practical compliance obstacles that the CCPA presents.

1. Clarifying and Simplifying CCPA Rights Compliance

Exercising CCPA rights should be convenient for consumers. Complying with CCPA requests should likewise be practicable and efficient, and avoid needless "burden on business".
§ 1798.185(a)(7).

It is important to recognize that compliance with a CCPA request typically involves multiple steps:

- (1) verifying the identity of the requester (so as not to give personal data to a fraudster);

(2) determining whether the requester is a California resident (and in preparing for compliance whether “personal data” in a business’ systems is that of a California resident so must be retrievable);

(3) addressing data quality issues that may impede locating and associating data;

(4) establishing household relationships to associate requests to the individuals in a “household”;

(5) actually locating and retrieving the “personal data” that relates to the requester, even if it is not personally identified or in an unstructured format, such as buried in an email message about a customer service request; and

(6) if asked to do so, resolving conflicting deletion or do not sell requests across households or different users of a device.

Assuming that the CCPA’s scope is limited to B2C operations, businesses must be able to retrieve a wide range of personal data that may be stored incidentally across a wide range of business operations that collect some element of personal data, including simply an IP address or device ID number. Business operations that may collect this information include: website, mobile app and any other online interactions, phone interactions, brick and mortar store interactions, emails, customer support, marketing, online advertising, data acquisition, analytics, machine learning, *etc.*

If B2B and employment data are in scope (despite the statute consistently using the term “consumer” in its title and throughout the obligations in its privacy sections), the range of affected business processes is even broader: HR and employee benefits operations, IT support, email, recruiting, system security monitoring, CRM operations, B2B marketing, *etc.*

Retrieving and associating with a particular requester both non-identified data and unstructured data across these many operational data collection points is complex and 100% compliance by well-intentioned businesses seeking to comply is very difficult and burdensome.

Second, if businesses face significant operational burden or significant potential liability for honest mistakes missing some data in response to a request, businesses will be incentivized to combine all “personal data” in data lakes or other centralized repositories in order to be able to comply readily and more reliably with “consumer” requests. This sort of data combination actually *disserves privacy* by making more information identifiable and making it easier for businesses to use for additional purposes, instead of leaving it separated and unused for those secondary purposes.

The source of this compliance conundrum is found in the development of A.B. 375. When Alistair McTaggart’s Initiative was transposed into A.B. 375, as Mr. McTaggart testified last week before the Senate Judiciary Committee, it added data subject rights of access, deletion, and data portability that were not in the Initiative. They were tacked onto A.B. 375 during a compressed negotiation without consideration of how those rights would work with the

amorphous and expansive definitions of “collect”, “personal data”, “consumer”, and “sale”, and the largely circular exception for “deidentified data”. As Justin Brookman of Consumer’s Union noted at the Sacramento workshop, these definitions had been drafted largely to address the Do Not Sell right in the Initiative.

The expansive definition of “personal information” works by and large in this context because businesses presumably combine information that they sell and can readily know what they are selling. However, it raises difficult compliance problems with regard to access, portability, deletion and “non-discrimination” rights because in those contexts, businesses do not combine such data.

For all reasons, it is very important that the final rules either make clear that “reasonable” compliance with data subject requests is sufficient, or that failure to locate non-identified consumer data if those data are not stored together with identified data or not stored in structured format is not a violation. This is consistent with § 1798.145(i)’s proviso that the CCPA should not be construed to require re-identifying information, and with the consideration in § 1798.185(a)(7) to consider “burden on business”. It is also net pro-privacy because it prevents an incentive to make more data identifiable and usable.

2. Avoiding Fraud and Other Risks to Consumers from Data Access and Data Portability Requests

The proposed rules should contain proposals to address “security concerns”, § 1798.185(a)(7), in two regards. The first is to avoid fraudulent “pretext” requests to obtain consumer data. This is a very strong concern with regard to requests for access to or portability of data creates risk of identity theft or fraud. There is also some risk of fraudsters making fraudulent requests to delete these data and later submitting fraudulent data in its place. For these reasons, the proposed rules should consider more stringent authentication, such as multi-factor authentication.

The second risk arises from access, portability or deletion requests submitted by one household member with regard to data of other household members – for example, one roommate requesting another roommate’s social security number, or deleting the other roommate’s information, out of spite. The risk is particularly severe in the case of a battering spouse seeking location information of a victim spouse who is listed as a co-resident of a household, but has fled the home.

Third, the proposed rules should contain safeguards against business competitors engaging in anti-competitive behavior by obtaining authorizations to opt-out consumers against sales of data to or from a competitor of the businesses obtaining the authorization.

3. Businesses That Do Not In Fact Sell Personal Information Should Not Be Required to Post a “Do Not Sell My Personal Information” Button, Although They Could Be Required to Post A Prominent Link to a Page Regarding Rights Under the CCPA


In order to “comply with . . . federal law”, § 1798.185(a)(3), the AG’s Office should recognize an exception to the requirement to post a “Do Not Sell My Personal Information” button for businesses that do not sell personal information. As to these businesses, this requirement is inaccurate, compelled speech that gives the false impression that the business is selling consumer when it is not doing so. Inaccurate, compelled speech is highly vulnerable to a First Amendment challenge and the AG’s Office should avoid conflicts with the First Amendment in its regulations as to this and other features that violate freedom of speech.

The proposed rules instead could suggest some other, accurate standard label for these businesses’ websites, such as “Your CCPA Rights”.

Lastly, if the legislature does not fix the drafting error in the definition of “Home Page” that it also means every web page where personal information is collected, § 1798.140(l), the AG’s Office should propose to fix this drafting error in its final rules to avoid littering every web page with these buttons. All web pages collect the IP address of visitors, so necessarily collect personal information, and a requirement to post the button on every web page would make for a terrible web site visitor experience and subject the CCPA to needless ridicule from web users.

Thank you for considering these views.

Respectfully submitted.

Jim Halpert


Message

From: Amal Abu-Rahma [REDACTED]
Sent: 2/8/2019 1:29:49 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments for Pending Privacy Regulations- AB 375- CCPA
Flag: Follow up

Dear Department of Justice (DOJ):

Thank you for the opportunity to comment on the pending privacy regulations per Assembly Bill 375 (the California Consumer Privacy Act of 2018- CCPA).

Issue:

It is now common practice for insurance companies to use the CarFAX database to rate new and existing consumers who purchase automobile policies with their companies. (CarFAX is an entity that acquires and stores vehicle-related information like DMV information, sales records, maintenance records, mileage, accident reports, etc.) Some of the information on CarFAX is public (i.e., DMV vehicle registration and sales records), but most of CarFAX's information is not publicly attainable. **It is the acquisition of this data that is objectionable.** It is respectfully requested that the DOJ consider this issue when promulgating its CCPA regulations to protect California consumers from this common and unlawful data acquisition.

Facts:

Insurance companies are accessing the information tied to a Vehicle Identification Number (VIN) which is obtained by CarFAX. CarFAX is acquiring this information from service dealerships and repair shops (cumulatively referred to as "shops") who contract with CarFAX. These shops sell or give this information to CarFAX, and sometimes in exchange for free or discounted use of the CarFAX database. This database is populated via unsuspecting consumers visiting those shops to obtain maintenance or repair services. Without notice, or permission thereof, consumer information is then uploaded to CarFAX on an agreed upon and regular schedule; data is usually in the CarFAX database within 2-3 days of the consumer's visit.

As a result of the above, automobile owners who are seeking, or who already have, insurance with specified companies are being rated, and possibly even being denied coverage, in part based on the CarFAX information that is obtained. Consumers are never advised of this practice, or provided an opportunity to object to, or opt out of, this third party sharing of information. In fact, the shops believe that because they are not providing owner names, addresses, or other specific personally identifiable information (i.e., birth date, social security numbers, driver's license numbers, etc.), they have a right to give that information to CarFAX. In addition, insurance companies are denying culpability as well because they say they are not involved in

the original exchange of the information, merely third party beneficiaries thereof. This said, all the parties involved readily agree that this process assists them in either insuring, or further selling, or buying, the vehicle in question when maintenance records, mileage, and other vehicle-specific information (i.e., accident repairs) are stored via a third party vendor. However, those same parties readily admit that they never contemplated such easy access to this information, and are merely taking advantage of a loop-hole in the system. In fact, CarFAX, which is a non-California-domiciled company, is also taking advantage of this loop-hole in California law, and all seem to be conspiring to the detriment of California's residents.

Consequences:

This unbridled process is harming consumers in a number of ways, including, but not limited to, the ability to re-sell those vehicles and/or acquire reasonable automobile insurance thereon. When insurance companies use the CarFAX data to rate, or even deny coverage to, these unsuspecting consumers, and, consumers are finding it difficult to sell their vehicles with damaging information posted to CarFAX, this process should deserve much greater scrutiny. To complicate things further, consumers do not have the ability to easily rebut the information on CarFAX, correct errors to the data, or defend themselves against the improper use of such information (i.e., like they would for medical records), particularly if they are not even aware of the practice. Finally, it is an incorrect presumption by the shops that such information is NOT personally identifiable because the VIN eventually, and inextricably, is traced back to the current or new owner of the vehicle, who then struggles in dealing with its improper use and disclosure. It is uncontroverted that vehicles do not repair themselves; consumers (usually the owners) are taking them in to shops to get repaired. As such, the activities and services of those consumers are being tracked without their express permission, and in violation of the spirit of California's privacy laws.

Conclusion:

All of the above is a breach of confidential information that is the exclusive property of the consumer (the owner of the VIN information), and the entire process, as described above, should be unlawful. Therefore, the Attorney General should consider non-public information, tied to California consumers' VIN, as personal information that should be protected from disclosure, and allow every consumer the right to know of its third-party use and prospective dissemination prior to any disclosure, and with the full opportunity to "opt out" if they so wish.

Thank you for your time in reading these comments regarding the CCPA.

Please be so kind as to acknowledge receipt of this email. Thank you.

Message

From: David LeDuc [REDACTED]
Sent: 3/8/2019 2:36:42 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Tony Ficarrotta [REDACTED]; Leigh Freund [REDACTED]; Stacey Schesser [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Stacey Schesser131]; Lisa Kim [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Lisa Kimf4f]
Subject: Comments from the Network Advertising Initiative (NAI)
Attachments: PastedGraphic-1.tiff; NAI_UnderstandingRTB; NAI_UnderstandingAds.pdf; NAI_AdBenefits; NAI Comment Letter - CCPA Implementing Regulations (3.8.2019) .pdf

Thank you for the opportunity to submit comments regarding the Department of Justice's request for comments regarding implementing regulations it may promote under the California Consumer Privacy Protection Act of 2018 (CCPA). Please find enclosed comments from the NAI, as well as reference materials developed by the NAI to help illustrate how digital advertising works and how it benefits both businesses and consumers. Please feel free to reach out with questions or to discuss these comments in greater detail.

Best regards,

David

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
409 7th Street, NW, Suite 250
Washington, DC 20004
[REDACTED]



Understanding Digital Advertising

Real-time Bidding (RTB)

What is it?

Real-time Bidding (RTB) is the automated process that powers Interest-Based Advertising (IBA) and Cross-App Advertising (CAA) by enabling websites, mobile apps, and online platforms to serve relevant advertising instantaneously as online content loads (i.e., in real-time). This is in contrast to more traditional methods where advertisers or their ad agencies negotiate directly with content producers for ad placements ahead of time (e.g., in radio, broadcast TV, or print news). Because RTB is an auction process, it enables advertisers to place higher bids for relevant ads while maximizing ad revenue for websites and apps.

Does RTB involve the sale of consumers' personal information?

RTB involves an auction for ad space, not personal information. The information used to facilitate RTB is typically limited to pseudonymous identifiers such as cookie IDs or mobile ad IDs, and associated data, rather than information that directly identifies a person or that is linked to an identified person. The various steps in the process for auctioning ad space are explained in detail below, but the auctions do not require the sale of information at any point in the process.

Instead, a website, app or online platform with ad space to sell sends a request for an ad to ad tech companies it has partnered with so the ad-tech companies may bid on the ad space on behalf of brand advertisers. The information included in such requests generally includes cookie or mobile ad IDs and IP addresses, but may include other information about the browser or device. Further, the ad-tech company receiving the information in the bid request does not purchase it from the website or app requesting the ad; it is transmitted only to allow the ad space to be bid upon and a relevant ad to be selected. The "bidstream" information received by an ad-tech company is used in real-time to help advertisers decide if they will bid on the opportunity to show an ad on a particular browser or device.

What Choices and Protections Exist for Consumers?

The NAI Code of Conduct requires NAI members to contractually prohibit anyone to whom they transmit bidstream data (or other data that is linked to a particular browser or device) from merging it with any other information intended to identify a particular individual without first providing robust notice and choice to the individual. The NAI and its member companies are also committed to providing consumers with clear information and education about IBA and CAA, and empowering them to choose whether information for IBA/CAA is collected on their web browsers or devices.

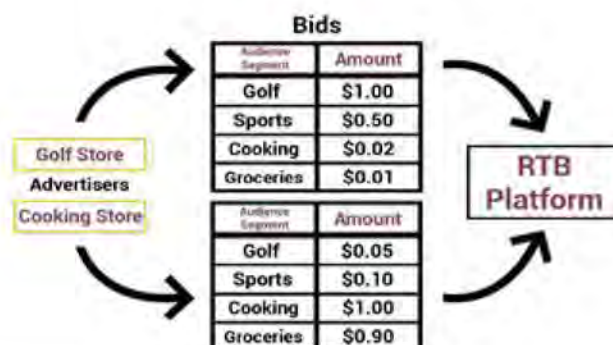
In addition, NAI members must take steps to ensure that websites, mobile apps, or online platforms that use pseudonymous information for IBA/CAA provide notice to users and a link to an opt-out mechanism such as the industry-wide opt out offered by the NAI. The NAI offers consumers the ability to opt out of web-based IBA through its centralized and easy-to-use opt-out tool. Meanwhile, NAI members operating in the mobile environment respect device platform controls, such as "Limit Ad Tracking" on Apple devices and "Opt out of Ads Personalization" on Android devices, treating those flags as opt outs from mobile CAA. When NAI members encounter an opted-out web browser or device, they do not collect any information from that browser or device for IBA/CAA purposes.

Understanding Digital Advertising

Real-time Bidding (RTB)

How does RTB work in practice?

1. Advertisers decide what kind of audience segments they want to reach and how much they are willing to pay to show an ad to a browser or device in that segment (e.g., those with a demonstrated interest in golf or cooking). They then pass this information to their RTB partners.



2. Websites, mobile apps, and online platforms with advertising inventory also partner with RTB platforms to enable their ad inventory to be sold for the highest price advertisers are willing to pay to reach their audiences.

3. When a user visits a website, mobile app, or online platform that has partnered with an RTB platform, the bidding process begins. First, a pseudonymous ID (such as a cookie ID or mobile ad ID) associated with the web browser or device is transmitted to the RTB platform's server with a request for an ad.



4. Next, the RTB platform may determine which audience segments have been associated with the pseudonymous ID. For example, a pseudonymous ID may have been assigned to a 'golf interest' audience segment.

For more information on how pseudonymous IDs are associated with audience segments for IBA/CAA, please see "Understanding Digital Advertising: How does IBA/CAA work in practice?"

Understanding Digital Advertising

Real-time Bidding (RTB)

5. The RTB platform may then determine the amount that its advertising partners have agreed to bid to show ads to browsers in the 'golf interest' audience segment.

Advertiser Bids for Golf Interest Category

Advertiser	Bids
Golf Store	\$1.00
Cooking Store	\$0.05

6. Finally, an ad from the advertiser that placed the highest bid, in this case the golf store, will be served on the website, mobile app, or online platform.



The RTB process occurs every time a webpage or application with available ad space is loaded from an RTB platform, and occurs within a fraction of a second (see steps 3-6 above). The entire process is driven by computer programs, which is why the term "programmatic" advertising is sometimes used to describe this process. So, while humans write the software programs and set up the parameters of the RTB system, there are no humans directly involved in the process of communicating the pseudonymous IDs and associated audience segments between websites and/or devices and RTB platforms.

Please visit the NAI website (<http://networkadvertising.org>) to learn more about digital advertising and consumer choices.

What is it?

Digital advertising is a broad term used to describe the paid advertising that publishers put on their websites and mobile apps to enable them to provide content and services for free or at a low cost. Some digital advertising is tailored to consumers' likely interests by companies promoting their products or services. Ad-tech companies facilitate this type of advertising, in partnership with website/app publishers and brand advertisers, by collecting information about a specific browser or device and its interaction with different websites, mobile apps, and other content. This is known as Interest-Based Advertising (IBA) when it occurs across websites and Cross-App Advertising (CAA) when it occurs across apps.

What type of data is collected? Does IBA/CAA rely on consumers' personal information?

The information website/app publishers and brand advertisers share with ad-tech companies for advertising purposes is typically not associated with identified individuals. Instead, ad-tech companies generally collect information using technologies such as cookies and mobile advertising IDs that are associated only with a given device or web browser. These technologies distinguish between unique visitors to a site, or users of an app, on a "pseudonymous" basis without using personal identifiers such as name, postal or email address, or phone number. Browsers or devices identified in this way are then placed in interest categories based on inferences drawn from their prior interaction with a variety of websites and apps. Interest categories can include sports, home & garden, music, dining, and many others. The relevance of digital ads may be improved in some cases by using additional data, such as IP address or geolocation data. For example, advertisers may wish to deliver their advertising only in cities where they have retail locations.

While it is technically feasible in some circumstances to connect "pseudonymous" information like cookie IDs with a personally identified individual given enough information from different sources, the NAI Code of Conduct prohibits NAI members from linking information collected from websites and apps with personally identified individuals without first providing robust notice and choice.

What kind of data is collected?



How does IBA/CAA work in practice?

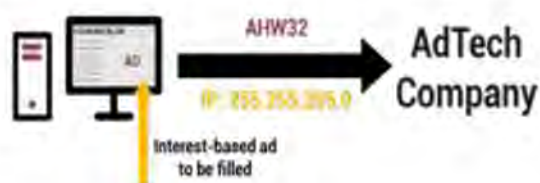
Fundamentally, IBA/CAA works by placing browsers or devices into interest categories based on information such as websites or apps visited. This process begins when a web browser or device visits a website or uses an app that has partnered with an ad-tech company for advertising purposes.



Consider, for example, what may happen when a web browser navigates to a golfing website that has partnered with an ad-tech company. As the golfing site loads on the browser, it sends a request to the ad-tech company to set a cookie on the web browser. This cookie contains an alphanumeric string that uniquely identifies the web browser, but it does not personally identify the user. The value of the cookie in this case could be 'AHW32'.

COOKIE	GOLF
ABC54	NO
JWE12	NO
897SD	YES
AHW32	YES
OKS45	NO
XY713	YES

Once the ad-tech company stores its cookie on the web browser, it can recognize the browser in the future. Further, because the ad-tech company set its cookie through a golfing site, it might associate the cookie ID with a 'golfing' interest category on its server.



After visiting the golfing website, if the web browser then navigates to a cooking blog that has partnered with the same ad-tech company, the ad-tech company can recognize it as a browser that has previously visited a golfing site. Because the cooking blog is funded by ad revenue, it sends a request to the ad-tech company to select an ad to show when the blog loads on the web browser. The blog will send its request with the 'AHW32' cookie ID that was previously stored on the browser, as well as the web browser's IP address (which may be used to infer the approximate geographic location of the browser).

AHW32



COOKIE	GOLF
ABC54	NO
JWE12	NO
897SD	YES
AHW32	YES
OKS45	NO
XY713	YES

When the ad-tech company receives the blog's request for an ad, it compares the cookie ID with the interest categories saved on its server and determines that the web browser is assigned to its 'golfing' interest category.



The ad-tech company might also determine that the browser's IP address originated in the Boston area. In this case, the ad-tech company has also partnered with a golf course near Boston to show its ads to users located nearby who are interested in golfing. So, the ad-tech company responds to the blog's request for an ad by selecting and serving the golf course's ad on the cooking blog.

COOKIE	GOLF	COOKING
ABC54	NO	NO
JWE12	NO	YES
897SD	YES	NO
AHW32	YES	YES
OKS45	NO	YES
XY713	YES	NO

At this point, the ad-tech company may also associate the cookie ID 'AHW32' with the 'cooking' interest category on its server because the browser had navigated to a cooking blog.

Going forward, if the web browser navigates to another website that has partnered with the same ad-tech company, it is more likely to serve ads on that website from advertising partners selling cooking products.

The intent of interest-based ads is to reach the consumers sitting behind web browsers, but ad-tech companies typically do not personally identify consumers for those ads to work as intended, and NAI members are prohibited from doing so for advertising purposes without first providing notice and choice to consumers.

NAI members must also restrict third parties with whom they share data from linking it with a personally identifiable individual without that individual's affirmative consent. However, if brand advertisers have an existing first-party relationship with a consumer, the advertiser may have an agreement with the consumer permitting the advertiser to link information that personally identifies the consumer with their digital advertising data. In such cases, the advertiser would be directly permitted by the consumer to associate the consumer's digital advertising data with their full profile for the purposes specified in their agreement, such as ad attribution and other reporting purposes.

Does IBA/CAA involve a sale of consumers' personal data?

The commercial reality of IBA/CAA involves the sale of ad space, not personally identifying information. For example, if a web browser navigates to a cooking blog funded by IBA, the blog may make a request to an ad-tech partner to serve an ad on the blog. That request would be transmitted with a pseudonymous cookie ID, which is typically a randomly generated alphanumeric ID such as 'AHW32'. The cookie ID only allows the ad-tech company to distinguish that browser from countless other browsers visiting the blog. Using the cookie ID and consumer-interest information stored on its servers, the ad-tech company may be able to determine "the browser with cookie ID 'AHW32' is likely to be interested in golf," and serve the ad space on the cooking blog with an ad for a golf course (for more information on how pseudonymous IDs are associated with interest categories for IBA/CAA, please refer to "Understanding Digital Advertising: How does IBA/CAA work in practice?").

The monetary transaction taking place for IBA/CAA in this example, and others like it, is the sale by the cooking blog of ad space to the golf course, which occurs without personally identifying a specific individual. The pseudonymous information the ad-tech company may process as an intermediary to the transaction for ad space simply allows the golf course to select which browser to serve its advertising on more effectively by focusing on audiences more likely to be interested in golf. The result is beneficial for everyone: consumers usually see ads more relevant to their interests, publishers earn more ad revenue, and businesses are better able to reach their target audiences.

What choices do consumers currently have about IBA/CAA?

The NAI and its member companies are committed to providing consumers with clear information and education about IBA/CAA and empowering them to choose whether information is collected from their web browsers or devices for this kind of advertising. The NAI offers consumers the ability to opt out of web-based IBA through its centralized and easy-to-use opt-out tool. Meanwhile, NAI members providing CAA typically respect device platform controls, such as Limit Ad Tracking and Opt out of Ads Personalization flags on Apple and Android devices respectively, treating those flags as opt outs from CAA. When NAI members encounter an opted-out web browser or device, they do not collect any information from that browser or device for IBA/CAA purposes.

Please visit the NAI website (<http://networkadvertising.org>) to learn more about IBA/CAA and consumer choices.

Who Benefits from Interest-Based and Cross-App Advertising?

Interest-Based Advertising (IBA) and Cross-App Advertising (CAA) are mutually beneficial to consumers, online publishers and app developers, as well as advertisers.

Consumers have demonstrated strong support for receiving a wide range of ad-supported digital content for little or no cost. NAI consumer research shows that 67% of U.S. consumers think online content should be ad-supported, while only 11% prefer a subscription model.¹ Using IBA/CAA ads instead of traditional contextual or direct-buy ads also improves user experience by providing ads that consumers are more likely to be interested in engaging with.

Advertisers are willing to pay significantly more for ad placements that are more likely to be relevant to the consumers they are trying to reach. This often means publishers can show fewer ads overall to fund their content, which improves user experience. Additionally, IBA/CAA greatly benefits smaller publishers and app providers who lack the resources to negotiate directly with larger advertisers. This is because smaller businesses can rely on ad-tech companies to make their ad inventory available to a broad array of advertisers interested in displaying ads based on consumer interests, not just the content the ads will appear with.

IBA/CAA is also particularly beneficial for small business advertisers, providing effective advertising for companies working with limited marketing and ad budgets. For instance, a local gourmet cheese shop can use IBA/CAA not only to reach potential customers nearby, but also to reach primarily those consumers who are most likely to have an interest in gourmet cheese. IBA/CAA also allows advertisers to be results-driven and flexibly reallocate budget to reach audience segments driving actual sales.

Benefits of IBA/CAA

Consumers	Online Publishers and App Developers	Advertisers
<ul style="list-style-type: none">• Increased access to digital content for little or no cost• Fewer ads overall• Ads more likely relevant to their interests	<ul style="list-style-type: none">• Rich digital content funded without subscriptions or direct payment• Content funded with fewer, more valuable ads, improving user experience	<ul style="list-style-type: none">• Increased ad effectiveness for small businesses, even with limited advertising budgets• Enhanced consumer engagement due to greater ad relevance

¹ NAI Consumer Survey: Digital Advertising, Online Content, and Privacy, <http://www.networkadvertising.org/blog-entry/nai-consumer-survey-digital-advertising-online-content-and-privacy/>.

Network Advertising Initiative
409 7th Street NW, Suite 250
Washington, DC 20004

March 8, 2019

VIA ELECTRONIC MAIL: PrivacyRegulations@doj.ca.gov

The Honorable Xavier Becerra
Attorney General
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

RE: Implementing Regulations for the California Consumer Privacy Act of 2018

Dear Mr. Becerra:

The Network Advertising Initiative (“NAI”) is pleased to submit this letter in response to the Department of Justice’s request for comments regarding implementing regulations it may promulgate under the California Consumer Privacy Act of 2018 (“CCPA”).¹

Overview of the NAI

Founded in 2000, the NAI is the leading self-regulatory organization representing third-party digital advertising companies. As a non-profit organization, the NAI promotes the health of the online ecosystem by maintaining and enforcing high standards for data collection and use for digital advertising in multiple media, including web, mobile, and TV.

All NAI members are required to adhere to our FIPPs-based, privacy-protective Code of Conduct (the “NAI Code”), which underwent a revision in 2018,² and will be updated again in 2020 to keep up with changing business practices and consumer expectations. Member compliance with the NAI Code is backed up by a strong accountability program, which includes a comprehensive annual review by NAI staff of member companies’ business models, policies and practices to ensure their compliance with the NAI Code, even as their individual businesses, and the industry as a whole, evolves.

¹ CAL. CIV. CODE §§ 1798.100 *et seq.*

² See NETWORK ADVERTISING INITIATIVE, 2018 NAI CODE OF CONDUCT (2018) [hereinafter NAI CODE OF CONDUCT], http://www.networkadvertising.org/sites/default/files/nai_code2018.pdf.

Several key features of the NAI Code align closely with the underlying goals of the CCPA, such as the NAI Code's requirement that NAI members provide consumers with an easy-to-use mechanism to opt out of Interest-Based Advertising (IBA),³ its requirement that NAI members disclose to consumers the kinds of information they collect for IBA, and how such information is used.⁴ The NAI Code's privacy protections also go further than the CCPA in some respects. For example, the NAI Code includes outright prohibitions against the secondary use of information collected for IBA for certain eligibility purposes, such as credit or insurance eligibility, regardless of whether such information is ever sold, and even when a consumer has not opted out.⁵

The NAI also educates and empowers consumers to make meaningful choices about their experience with digital advertising through its easy-to-use, industry-wide opt-out mechanism.⁶

Outline of NAI's Comments

Part I: Definitions

- A. The CCPA should be amended, or implementing regulations should clarify, that deidentified information is not personal information.
- B. Regulations implementing the CCPA should clarify that the definition of "sale" applies only when the purpose of a transaction is the exchange of personal information for consideration.
- C. Regulations implementing the CCPA should clarify the application of certain exceptions from the definition of "sale."
- D. CCPA implementing regulations should clarify the circumstances under which probabilistic identifiers also constitute unique identifiers.

Part II: Consumer Exercises of CCPA Rights and Business Responses

- A. In order to maximize consumer privacy, regulations implementing the CCPA should provide flexibility for how businesses may respond to consumer requests regarding information that has been pseudonymized.
- B. CCPA implementing regulations should clarify that consumers may make specific choices with respect to both opting out of sales of personal information and requesting the deletion of personal information.
- C. CCPA implementing regulations should not prevent businesses from relying on strong verification procedures when responding to consumer requests.

³ See *id.* § II.C.1.a. The NAI Code of Conduct defines Interest-Based Advertising as "the collection of data across web domains owned or operated by different entities for the purpose of delivering advertising based on preferences or interests known or inferred from the data collected." *Id.* § I.F. Capitalized terms used but not defined herein have the meanings assigned to them in § I of the NAI Code of Conduct. See generally *id.* § I.

⁴ See *id.* § II.B.

⁵ See *id.* § II.D.2.

⁶ For more information on how to opt out of Interest-Based Advertising, please visit <http://optout.networkadvertising.org>.

Part III: Disclosure obligations

- A. CCPA implementing regulations should clarify that a business is not required to disclose the specific pieces of information it has collected about a consumer in its online privacy policy.
- B. CCPA implementing regulations should allow businesses reasonable flexibility regarding the placement of the “Do Not Sell My Personal Information” link.
- C. CCPA implementing regulations should clarify the disclosure requirements associated with third-party sales.
- D. CCPA implementing regulations should clarify the application of the 12-month lookback period.

Part IV: Other issues

- A. CCPA implementing regulations should clarify that businesses may charge a reasonable fee for goods and services as an alternative to ad-supported goods or services.
- B. CCPA implementing regulations should clarify that businesses are not required to extend their data retention policies to respond to consumer requests.

Part I: Definitions

A. The CCPA should be amended, or implementing regulations should clarify, that deidentified information is not personal information.

The original bill that made the CCPA a law⁷ was subsequently amended⁸ to modify, among other things, the CCPA’s definition of “personal information” (“PI”) by adding the text bolded below.

*“Personal information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following **if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household**[.]”⁹*

The addition of the bolded text by the amendment clarifies that the scope of PI should not extend beyond information that “identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly” a particular consumer or household.

However, as written, the CCPA lacks clarity in a number of ways that threaten the objectives of the legislation. First, while the law clearly intends for deidentified and aggregate consumer information to fall outside the scope of PI, there could be confusion caused by the structure of the definitions of those terms. Implementing regulations can further promote the CCPA’s privacy-protective purposes by ensuring that deidentified information and aggregate consumer

⁷ A.B. 375, 2017-2018 Leg. Sess., Reg. Sess. (Ca. 2018).

⁸ S.B. 1121, 2017-2018 Leg. Sess., Reg. Sess. (Ca. 2018).

⁹ See *id.* § 9 (emphasis added).

information are clearly excluded from the definition of PI. Doing so would promote consumer privacy because it gives businesses an incentive to use deidentified and/or aggregate information instead of PI wherever possible, as businesses would not need to comply with the CCPA's onerous requirements when they take the additional steps required to scrub data in such a way to render it deidentified or by aggregating it.

Indeed, for the same reasons, the CCPA missed an opportunity to further enhance consumer privacy by more strongly incentivizing the use of pseudonymous information by businesses. Business should be incentivized to take the extra steps necessary to use pseudonymous information like cookie IDs and mobile ad IDs (instead of, e.g., clear email addresses or phone numbers), and to avoid associating those pseudonymous identifiers with directly identifying information when processing information about consumers. This approach is a common practice in digital advertising and should be leveraged by CCPA implementing regulations to provide an extra degree of privacy protection for consumers. The European Union's General Data Protection Regulation ("GDPR") also recognizes the importance of promoting the use of pseudonymous information, as it relaxes some of its more stringent requirements when businesses make the effort to use pseudonymous information.¹⁰

However, because the CCPA's definition of PI takes more of an "all or nothing" approach by defining a consumer's social security number on par with cookie IDs, businesses are less likely to take additional steps to rely on pseudonymous consumer information and to avoid associating such data with other PI. We recognize that limiting the scope of what constitutes PI under the CCPA by excluding pseudonymous information likely falls outside the scope of this rulemaking process. Therefore, we are proposing a focus for the implementing regulations to promote privacy-enhancing uses of pseudonymous information. For NAI's specific recommendations on how the CCPA's implementing regulations can encourage the use of pseudonymous information in some circumstances, please refer to § II.A *infra*.

Nonetheless, to avoid ambiguity with respect to deidentified and aggregate consumer information, CCPA implementing regulations should clarify that they are outside the scope of PI. The CCPA defines "deidentified" as follows:

"Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

- (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.*
- (2) Has implemented business processes that specifically prohibit reidentification of the information.*
- (3) Has implemented business processes to prevent inadvertent release of deidentified information.*

¹⁰ See, e.g., Gabe Maldoff, *Top 10 operational impacts of the GDPR: Part 8 – Pseudonymization*, IAPP (Feb. 12, 2016), <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization>.

(4) Makes no attempt to reidentify the information.¹¹

Note that both the amended definition of PI and the definition of “deidentified” information are directly keyed to the concept of information that identifies, relates to, describes, is capable of being associated with, or that could be linked, directly or indirectly, to a particular consumer. To be included in the definition of PI, at least one of those conditions must be met. But to fall under the definition of “deidentified” information, none of those conditions may be met. It follows that information meeting the definition of “deidentified” should never fall under the definition of PI. Implementing regulations should clarify that fact.

Proposed Regulatory Language:

For purposes of paragraph (1) of subdivision (o) of Section 1798.140 of the Act, information shall not constitute “personal information” where such information is deidentified or is aggregate consumer information.

B. Regulations implementing the CCPA should clarify that the definition of “sale” applies only when the purpose of a transaction is the exchange of personal information for consideration.

Today’s digital economy relies on data flows of all kinds. Indeed, the very structure of the Internet requires the transmission and receipt of data about web browsers, devices, and networks that arguably are PI under the CCPA’s broad definition of the term. While these data flows are critical for many functions of the Internet, they are not accurately characterized as sales of data because the purpose of the transactions wherein those data are transmitted is generally not the exchange of information for monetary consideration. Instead, those data flows are merely the means businesses use to enable functions that are recognized business purposes – for example, loading a webpage or serving a digital advertisement.

Like almost all web-based Internet activity, selecting and serving digital advertisements involves the transmission of information like IP address, user agent, and cookie IDs. However, the purpose of digital advertising is the sale of ad space, not information. For example, if a web browser navigates to a cooking blog funded by advertising, the cooking blog may make a request to an ad-tech partner to serve an ad on the blog. The blog’s request for an ad would be transmitted with a pseudonymous cookie ID such as “AHW32” that distinguishes the browser currently visiting the blog from all other web browsers that have visited the blog. Using this information, the ad-tech company might see that the browser is visiting a cooking site and show an ad for a kitchen appliance, or it might look to the cookie ID and information stored on its servers about the web browser’s online activity, to recognize that “*the browser with cookie ID ‘AHW32’ might be interested in golf,*” and fill the ad space on the blog with an ad for a nearby golf course.

¹¹ CAL. CIV. CODE § 1798.140(h).

The purpose of the transaction taking place in this example, and others like it, is the sale of ad space from a website to an advertiser, which can occur, and usually does, without identifying a specific individual. The information the ad-tech company may process as an intermediary to the transaction for ad space simply allows, for example, the kitchen appliance manufacturer or golf course to select which web browsers to serve its advertising on more effectively by focusing on audiences who are likely to be interested in their products and services. The CCPA's implementing regulations should recognize these current realities and privacy-protective practices and seek to encourage them.

However, because the CCPA combines an expansive definition of "sale" with an expansive definition of PI, there is a risk that data processing necessary to complete a sale for ad space could be mischaracterized as a sale of PI, even when such processing does not identify a specific individual. To avoid this result, the CCPA's implementing regulations should recognize that data processing that is merely an incidental part of a transaction undertaken for another business purpose is not itself a sale of PI under the CCPA.

CCPA defines "sale" as follows:

"Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.¹²

We believe the legislature intended this definition of sale to broadly cover any transmission of PI by a business to another business or third party, but only when the transmission takes place *for the purpose of* receiving valuable consideration directly in exchange for that information. By adopting a purpose test that clearly ties the valuable consideration to the PI provided, implementing regulations can look through the complicated structure of data flows to capture true sales, while avoiding overbroad application to data transmissions that, while necessary to complete certain transactions, are merely the means used to effect them. Application of a purpose test to interpret when the CCPA's definition of "sale" applies would be practical and consistent with other state laws where the "sale" or activity of "selling" is a central focus.

Consider the following illustrative example provided by a Wisconsin Supreme Court case involving the question of when a "sale" takes place for purposes of assessing a sales tax.¹³ In that case, the Wisconsin Department of Revenue wanted to collect sales tax from the Milwaukee Brewers baseball organization on the value of the paper admission tickets the Brewers gave to baseball game attendees. The Department's position was that because the paper tickets were included with the price of admission paid by attendees, they were sold by the Brewers to those attendees.

¹² CAL. CIV. CODE § 1798.145(t) (emphasis added).

¹³ See Wis. Dep't of Revenue v. Milwaukee Brewers, 331 N.W.2d 571 (Wis. 1983).

However, the Court held that the physical admissions tickets provided to attendees of baseball games were not “resold” to those attendees as part of the price of admission, and hence the tickets themselves were not subject to sales tax when given to attendees. This holding demonstrates the idea that something may be a means for completing a transaction without it being the reason why the transaction took place. A purpose test would also correctly decide that the consideration ticketholders paid to the Brewers was given for the purpose of gaining admission to watch a ballgame, not to take possession of a paper ticket.

Proposed Regulatory Language:

For purposes of § 1798.140(t) of the Act, a business will not be deemed to have sold personal information as part of a transaction when the transmission of such personal information is merely the means used to effect a transaction undertaken for a purpose other than the exchange of personal information for consideration, including, but not limited to:

- 1) the transmission of personal information incidental to the delivery, display, measurement, selection, or analysis of an online advertisement.*

C. Regulations implementing the CCPA should clarify the application of certain exceptions from the definition of “sale.”

The CCPA exempts from its definition of “sale” the processing of PI in several specific contexts, but these exemptions suffer from ambiguities that could lead to confusion and higher compliance costs. Businesses seeking to rely on these exemptions would benefit from additional clarification on their operation and application. Providing such clarification through implementing regulations will allow businesses to rely on clear exceptions they are entitled to under the law, while reducing the risk of erroneous uses of the exceptions.

1. Exceptions for disclosures at a consumer’s direction.

The CCPA’s first exception from the definition of “sale” covers certain cases where a consumer directs a business to disclose PI to a third party:

For purposes of this title, a business does not sell personal information when:
(A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer’s intent to interact with a third party.¹⁴

¹⁴ CAL. CIV. CODE § 1798.140(t)(2)(A).

The application of this exception depends on a consumer's intent to cause a business to disclose PI about them to a third party. It singles out certain consumer actions that a business may not treat as sufficient to infer a consumer's intent, but it does not provide any further guidance on what consumer actions a business may rely on to infer intent. To provide clarity, implementing regulations should stipulate certain consumer actions that businesses may rely on as a manifestation of intent.

Proposed Regulatory Language:

A consumer is deemed to have intentionally interacted with a third party for purposes of § 1798.140(t)(2)(A) if the consumer takes an affirmative action, such as a click or tap, indicating their intent to cause an interaction with that third party.

2. Exceptions for disclosures to service providers for a business purpose.

Another exception from the definition of “sale” covers certain disclosures of PI by a business to a service provider for a business purpose:

For purposes of this title, a business does not sell personal information when:

...

(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:

(i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.

(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.¹⁵

This application of this exception relies on the operation of two defined terms: “business purpose” and “service provider.” CCPA implementing regulations should clarify how the definition of “business purpose” operates in the context of this exception.

The term “business purpose” is defined as follows:

“Business purpose” means the use of personal information for the business’s or a service provider’s operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are . . .¹⁶

¹⁵ *Id.* § 1798.140(t)(2)(C).

¹⁶ *Id.* § 1798.140(d).

CCPA implementing regulations should clarify that the list of business purposes included in §1798.140(d)(1)-(7) is not exhaustive. This is an important clarification because there are a range of other legitimate purposes, beyond those specifically identified in the CCPA, for which businesses may need to disclose information to service providers who process such information on their behalf, subject to appropriate contractual restrictions. It is also supported by the CCPA's text, as the definition of "business purpose" also includes the use of PI for "operational purposes" or other "notified purposes" in addition to the purposes listed in §1798.140(d)(1)-(7).

Proposed Regulatory Language:

The business purposes specified in §§1798.140(d)(1)-(7) are not exhaustive, and personal information disclosed by a business to a service provider for other operational purposes not specified in §§1798.140(d)(1)-(7) are business purposes if they otherwise meet the requirements of §1798.140. A business that discloses personal information to a service provider for purposes it sets forth in its privacy policy required pursuant to § 1798.130 are disclosures made for a "notified purpose" under §1798.140, and such disclosures are made for a business purpose if they otherwise meet the requirements of §1798.140.

D. CCPA implementing regulations should clarify the circumstances under which probabilistic identifiers also constitute unique identifiers.

The CCPA uses the concept of a "unique identifier" or "unique personal identifier" to inform two other key definitions: that of a covered "consumer" and that of covered "PI." It is defined as follows:

"Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.¹⁷

The definition of "unique identifier" in turn relies in part upon the definition of "probabilistic identifier":

"Probabilistic identifier" means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.¹⁸

¹⁷ *Id.* § 1798.140(x).

¹⁸ *Id.* § 1798.140(p).

The fact that the CCPA's definition of PI encompasses probabilistic identifiers is conceptually flawed because these so-called identifiers do not in fact relate to any one unique consumer. An inevitable consequence of including them in the definition of PI is that, in some cases, information associated with them will relate to more than one consumer or device that may, or may not, even be part of the same household. One example for how this may work is a method of serving advertisements to devices based on IP address and user agent.¹⁹ This set of information may relate to a specific device being used by one consumer, but not always. In a workplace setting, for example, computers provided by an employer may all be sharing an IP address, be running the same operating system, and have the same web browser enabled by default. In those circumstances, a probabilistic ID based on IP address and user agent may relate to multiple different coworkers who do not share a household. Clearly this kind of information would not be personal to any one of those coworkers. For the same reasons, probabilistic IDs present problems for consumer access requests – because probabilistic IDs are not directly associated with any one identified consumer, it is not practical for businesses to provide a single consumer with access and deletion rights under the CCPA under these circumstances, or to verify any such consumer requests.

In addition, businesses that use probabilistic identifiers do not necessarily assign a specific degree of probability to the proposition that they identify one particular consumer or device. Instead, many businesses simply make practical assumptions about these identifiers, without making, or even being capable of making, an objective assessment of probability. In those circumstances, implementing regulations should clarify that the mere fact that a business treats a probabilistic identifier as being linked to a unique device or set of devices for practical purposes, such as the serving of tailored advertising, is not sufficient on its own to make it “more probable than not” that the probabilistic ID constitutes personal information.

Proposed Regulatory Language:

A business will not be deemed to have collected, used, disclosed, sold, or otherwise processed a probabilistic identifier as that term is defined by § 1798.140(p) unless the business has actual knowledge that the identifier identifies a consumer or a device to a degree of certainty of more probable than not.

Part II: Consumer Exercises of CCPA Rights and Business Responses

A. In order to maximize consumer privacy, regulations implementing CCPA should provide flexibility for how businesses may respond to consumer requests regarding information that has been pseudonymized.

As discussed above, the CCPA's definition of PI has a broad scope that extends much more broadly than just traditional personal identifiers like name and social security number. It also extends substantially beyond the traditional scope of data that is “reasonably linked or linkable”

¹⁹ User agent includes the type of operating system being used (e.g., Mac OS or Windows) and the type of web browser being used (e.g., Safari or Chrome).

to an identified person. The NAI Code takes a similar approach by extending important privacy protections, including notice and choice, for information associated with pseudonymous identifiers such as cookie IDs and mobile ad IDs.²⁰ A key feature of the NAI Code is the fact that it tailors its privacy protections to the sensitivity of the information at issue. For example, the NAI Code requires NAI members to offer consumers a choice to opt out of IBA using pseudonymous IDs tied only to a browser or device,²¹ but in most circumstances they must obtain opt-in consent for the use of personal identifiers like email addresses, names, or phone numbers for advertising purposes.²² This tailoring of privacy protections to the sensitivity of data enhances consumer privacy and security by providing an incentive for NAI members to maintain and use only pseudonymous identifiers where possible.

Implementing regulations for the CCPA have an opportunity to similarly enhance consumer privacy and security by providing an incentive for businesses to use pseudonymous information wherever possible. They can accomplish this goal by clarifying that businesses are not required to associate traditional personal identifiers with pseudonymous identifiers or information that has undergone pseudonymization to comply with certain CCPA requirements. Doing so would provide companies an important incentive to avoid using more sensitive information about consumers where possible – a result regulations cannot achieve by taking an “all or nothing” approach and treating a consumer’s name, email address, social security number, or other personally identifying information on par with an IP address and unique advertising IDs in all cases.

One area where implementing regulations could accomplish this privacy-protective goal consistent with the intent of the legislature and the text of the CCPA is through the existing exception from certain CCPA requirements when compliance with these requirements would require a business to re-identify or re-link certain information:

*This title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that **would be considered** personal information.*²³

Implementing regulations should clarify that information maintained by a business in a pseudonymous form is not maintained “in a manner that would be considered personal information.” We note that had the legislature intended to create an exemption from connecting non-PI with PI, it could have used language along the following lines: “This title shall not be construed to require a business to reidentify or otherwise link information that is not personal information.” Instead, we believe the intent of the legislature was to prevent businesses from

²⁰ Under the NAI Code of Conduct, cookie IDs and mobile ad IDs are considered Device-Identifiable Information (DII), which is defined in part as “any data that is linked to a particular browser or device if that data is not used, or intended to be used, to identify a particular individual.” See NAI CODE OF CONDUCT, *supra* note 2, at § I.E.

²¹ See *id.* § II.C.1.a. (providing an opt-out choice for Personalized Advertising based on information identified only with particular device or browser).

²² See, e.g., *id.* § II.C.1.c. (requiring Opt-In Consent for the use of PII to be merged with previously collected DII for Personalized Advertising).

²³ CAL. CIV. CODE § 1798.145(i) (emphasis added).

having to re-link or reidentify information maintained pseudonymously, which would ordinarily not be considered personal information, with traditional identifiers that would be.

Proposed Regulatory Language:

For purposes of subdivision (e) of Section 1798.100, paragraph (2) of subdivision (d) of Section 1798.110, and subdivision (i) of Section 1798.145 of the Act, information maintained by a business that (i) is deidentified; (ii) is aggregate consumer information; or (iii) has undergone pseudonymization, is deemed not to be maintained by the business in a way that would be considered personal information.

B. CCPA implementing regulations should clarify that consumers may make specific choices with respect to both opting out of sales of personal information and requesting the deletion of personal information.

Section 1798.105 of the CCPA gives consumers the right to request that a business delete any PI about the consumer which the business has collected from the consumer, while § 1798.120 gives consumers the right to opt out of a business's sale of PI about them.

The statutory language creating those rights is broad and clearly establishes the right of consumers to direct a business to delete all the PI it has collected from them and to direct a business not to sell any of the PI a business has about them. However, the CCPA does not explicitly permit a business to offer a consumer the choice to delete or opt out of a sale regarding some, but not all, types of PI. Regulations implementing the CCPA should clarify that businesses are permitted to offer more specific choices, and that consumers are entitled to receive those choices.

For example, the CCPA gives consumers the right to request that businesses disclose to them the business or commercial purposes for collecting or selling PI about them.²⁴ If a consumer receives this disclosure from a business, it might specify that the business both collects and sells PI from consumers to (1) offer the product or service to consumers without charging a fee; (2) help advertisers who are interested in reaching consumers to better understand consumers' interests based on their use of the business's products or services; and (3) for research purposes that may help the business or a third party improve their products or services. In this example, consumers should be able to specifically direct a business not to sell their PI to a third party for research purposes, while continuing to allow a business to engage in sales to advertisers that enable the consumer to use the product or service without paying a fee.

In addition, the CCPA gives consumers the right to request that a business disclose to them the categories of PI it has collected from them.²⁵ If a consumer receives this disclosure from a business, it might specify that the business has collected (1) email address; (2) full name; (3)

²⁴ *Id.* § 1798.110(a)(3).

²⁵ *Id.* § 1798.110(a)(2).

postal address; and (4) visual information such as a full-face picture. In this example, consumers should be able to specifically direct a business to delete their full-face picture even if it wants the business to retain the other categories of PI to allow the business to continue communicating with the consumer.

Because the CCPA gives consumers the right to know the different kinds of PI a business has collected about them, as well as the purposes for which the business has collected or sold such information, consumers should be empowered by that knowledge to make specific choices about how businesses collect and use PI about them.

The federal Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act provides a strong precedent supporting more flexible choices for consumers. The CAN-SPAM Act, which requires the provision of an opt-out choice with certain email messages, allows the initiator of such messages to offer recipients the opportunity to choose the specific types of messages the recipient wants to receive or not receive, so long as an option to not receive any commercial electronic mail messages from the sender is also made available.²⁶

Proposed Regulatory Language:

- a) *Business compliance with a consumer request for deletion: A business may, in response to a verified consumer request to delete personal information pursuant to subdivision (a) of Section 1798.105 of the Act, present the consumer with a reasonable list of the categories of personal information the business has collected about the consumer along with a reasonable method for the consumer to direct the business to either delete or retain each such category of personal information, provided that the list includes an option under which the consumer may direct a business to delete all of the personal information the business maintains about the consumer.*
- b) *Business compliance with a consumer opt-out request: A business may, in response to a verified consumer request to opt out of the sale of personal information pursuant to subdivision (a) of Section 1798.120 of the Act, present the consumer with a reasonable list of the purposes for which it sells personal information and the categories of third parties to which it sells personal information along with a reasonable method for the consumer to opt out of sales of personal information for each such purpose or category of third party, provided that the list includes an option under which the consumer may choose to opt out of all sales of personal information the business maintains about the consumer.*

²⁶ See 15 U.S.C. § 7704(a)(3)(B) (“More detailed options possible. The person initiating a commercial electronic mail message may comply with subparagraph (A)(i) by providing the recipient a list or menu from which the recipient may choose the specific types of commercial electronic mail messages the recipient wants to receive or does not want to receive from the sender, if the list or menu includes an option under which the recipient may choose not to receive any commercial electronic mail messages from the sender.”).

C. CCPA implementing regulations should not prevent businesses from relying on strong verification procedures when responding to consumer requests.

The CCPA requires businesses to take certain actions upon receipt of a “verifiable consumer request” in order to respect various consumer rights granted under the CCPA.²⁷ The emphasis on verifiable requests is appropriate, as it is critically important for businesses to release PI to a consumer only when that consumer’s identity can be confirmed. The CCPA recognizes this in its definition of “verifiable consumer request.”²⁸ Unfortunately, the CCPA’s requirements pose challenges for businesses, potentially resulting in a requirement to release PI about a consumer without proper verification. Implementing regulations can help avoid this result and the significant security and privacy risks attending it.

Regulations implementing the CCPA should clarify how businesses may verify consumer requests. However, regulations should not prescribe specific authentication methods that are not sensitive to the size or complexity of a business, or to the type of PI involved in the request. Instead, regulations should provide businesses with flexibility in how they verify consumer requests. This will allow businesses to develop methods that are reasonable with respect to their business processes and the kinds of PI they process, and to avoid the likelihood that any prescribed authentication method may at some time become obsolete or irrelevant.

Allowing flexibility with respect to how businesses verify consumer requests is particularly important because the CCPA prohibits businesses from requiring consumers to create an account for verification purposes.²⁹ As businesses often verify or authenticate consumers during the course of account formation, this prohibition makes verification more difficult. As such, businesses should have discretion to use reasonable verification methods and exercise caution to avoid disclosing PI when a consumer has not been properly verified.

A clear example of when a business should be enabled to impose more stringent verification procedures is with respect to requests made by an authorized agent on behalf of a consumer.³⁰ Releasing a consumer’s PI to a person or entity misrepresenting themselves as the consumer’s authorized agent would be an unacceptable privacy and security risk, particularly if such a person or entity is purporting to make access requests on behalf of multiple consumers. Businesses must have the flexibility to rigorously authenticate such requests, or to refuse them if they cannot be satisfactorily verified. Another clear example where more stringent verification

²⁷ See CAL. CIV. CODE §§ 1798.100(c)-(d); 1798.105(c); 1798.110(b); 1798.115(b); 1798.130(a)(2)-(4) (detailing actions a business must take in response to a verifiable consumer request).

²⁸ See *id.* § 1798.140(y) (“A business is not obligated to provide information to the consumer . . . if the business cannot verify . . . that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer’s behalf.”).

²⁹ See *id.* § 1798.130(2) (“The business shall not require the consumer to create an account with the business in order to make a verifiable consumer request.”).

³⁰ See *id.* § 1798.185(a)(7) (referring to access requests made by a consumer’s authorized agent).

procedures are called for is when a business receives a request to disclose specific pieces of PI that are relatively sensitive, such as social security number or other government identifier.

Further, implementing regulations should clarify that if a business is unable to verify a consumer request using reasonable methods, the business is not required to obtain additional personal information from a consumer in order to verify the request, and is not required to accept any additional personal information offered by a consumer to verify a request. Instead, regulations should clarify that when a business is unable to verify a consumer request, the business is required only to communicate that fact to the consumer making the request, but it is not required to take any further action with respect to that particular unverified request. Requiring businesses to collect and process additional personal information to verify requests is inconsistent with the goals of the CCPA, as well as the longstanding Fair Information Practice Principle (FIPP) of data minimization.

Finally, implementing regulations should clarify how service providers should respond to access requests and how they interact with businesses for which they provide services in connection with such requests.

Proposed Regulatory Language:

- a) *A business shall establish a reasonable and accessible method for verifying that a consumer making a request to exercise rights under the Act is the consumer about whom the business has collected personal information, or is a person authorized by the consumer to act on such consumer's behalf.*
- b) *If a business cannot verify a consumer's identity based on the information initially provided by the consumer for purposes of verification, then the business shall use a reasonable method to send the consumer, or the person authorized by the consumer to act on the consumer's behalf, an explanation that the business could not verify the consumer's identity and therefore cannot take the action requested by the consumer. A business is not required to request or accept additional personal information from a consumer to verify a consumer request.*
- c) *If a service provider receives a request directly from a consumer, the service provider may respond with an explanation that the consumer's identity could not be verified or that the request should be submitted to the business with the direct relationship with the consumer. The service provider shall, taking into account the nature of the processing and the relationship with the business, upon the business's request, assist the business in fulfilling the business's obligation to respond to the consumer's request, insofar as this is reasonably possible.*

D. CCPA implementing regulations should provide guidance regarding the extent of business responses to verified consumer requests for disclosure of specific pieces of information.

The CCPA gives consumers the right to request that a business disclose to them both the categories of PI and the specific pieces of PI the business has collected about them.³¹ However, if a business is required to provide voluminous operational data in a “data dump” responding to a request for specific pieces of PI, this would only serve to confuse and overwhelm consumers seeking to obtain only information relevant to the services they receive from a business.

To avoid this potential for unhelpful “data dumps,” businesses should not be required to disclose specific pieces of PI the business uses only for its internal operational purposes. Providing operational data to a consumer would not provide a benefit to the consumer commensurate with the costs a business would have to incur to disclose the data.

Proposed Regulatory Language:

A business is not required to provide specific pieces of personal information that it uses only for its own operational purposes in response to a consumer request under paragraph (5) of subdivision (a) of Section 1798.110 of the Act.

Part III: Disclosure Obligations

A. CCPA implementing regulations should clarify that a business is not required to disclose the specific pieces of information it has collected about a consumer in its online privacy policy.

The CCPA gives consumers the right to request that a business provide them with the specific pieces of information it has collected about them, and a corresponding obligation on the business to provide such information to a consumer upon receipt of a verified consumer request.³²

However, there is some confusion about whether the CCPA also imposes an obligation on a business to disclose the specific pieces of information it maintains about a consumer independently of any verified consumer request by posting such information in its online privacy policy. This confusion arises as follows. Under § 1798.110(c)(5) of the CCPA, a business that collects PI about consumers must disclose the specific pieces of PI it has collected about that consumer “pursuant to” § 1798.130(a)(5)(B), which in turn states:

(a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

...

³¹ See *id.* § 1798.100(a).

³² See *id.* § 1798.100.

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its Internet Web site, and update that information at least once every 12 months:

...

(B) For purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.³³

The interaction of §§ 1798.110(c)(5) and 1798.130(a)(5)(B) referenced above are confusing because the former appears to require the disclosure of specific pieces of PI in a business's online privacy policy, while the latter refers only to the disclosure of categories of PI to meet the same requirement. We believe the intent of the CCPA here is to require businesses to disclose only categories PI. A requirement to publicly disclose specific pieces of PI in an online privacy policy would not be practical for businesses because they not only collect different types of PI from different consumers in many circumstances, but also therefore maintain vastly different sets of specific information across consumers. Publicly disclosing PI in an online privacy policy would also create clear privacy and security risks.

Implementing regulations should resolve this confusion by specifying that a business may comply with § 1798.110(c)(5) of the CCPA by disclosing only the required *categories* of personal information in its privacy policy, and not any specific pieces of PI.

Proposed Regulatory Language:

A business is deemed to comply with paragraph (5) of subdivision (c) of Section 1798.110 of the Act by disclosing the categories of personal information it collects about consumers pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130 of the Act.

B. CCPA implementing regulations should allow businesses reasonable flexibility regarding the placement of the “Do Not Sell My Personal Information” link.

The language in § 1798.135(a) of the CCPA, coupled with the definition of “homepage” in § 1798.140(l), creates substantial ambiguity as to where the required “Do Not Sell My Personal Information” link is required to appear. Specifically, the definition of homepage is “the introductory page of an Internet Web site and any Internet Web page where personal information is collected.”³⁴ This is broader than, and inconsistent with, any common definition of a website's homepage, and it could be interpreted to include any web page engaged in digital advertising, depending on the interpretation of various other provisions of the law.

³³ *Id.* § 1798.130(a)(5)(B).

³⁴ *See id.* § 1798.140(l).

Additionally, businesses that do not maintain what may be traditionally perceived as a “homepage” would benefit from clarification as to where the required link should be placed in order to best reach consumers. For example, a business should be permitted to place the required link alongside or in conjunction with the link to its privacy policy or page, as that is the location consumers generally visit to learn about their choices and manage any offered privacy preferences.

Proposed Regulatory Language:

A business shall be deemed in compliance with paragraph (1) of subdivision (a) of Section 1798.135 of the Act where the business places the “Do Not Sell My Personal Information” link on the introductory page of an Internet Web site, or alongside the link to its privacy policy page, or in another clear and prominent position on the business’s Internet Web site or mobile application.

C. CCPA implementing regulations should clarify the disclosure requirements associated with third-party sales.

Section 1798.115(d) of the CCPA prohibits a third party from re-selling PI about a consumer that has been sold to the third party by a business, unless the consumer has received explicit notice and is provided an opportunity to exercise their right to opt out of such re-sale pursuant to § 1798.120(a). This provision clearly allows third-party sales of PI if consumers receive appropriate notice and choice. However, the statutory language does not specify who is required to provide such notice and choice to the consumer.

Businesses who sell PI to third parties are well positioned to meet this requirement because they can easily disclose the fact that PI they sell to third parties may then be re-sold by those third parties. They are also well suited to provide an opportunity to opt out of such third-party sales in the disclosures they are required to provide to consumers under § 1798.130 of the CCPA. In contrast, consumers are generally not in a position to interact directly with third parties. CCPA implementing regulations should therefore clarify that the obligations specified in § 1798.115(d) fall upon the business, not the third party to whom the business seeks to sell PI.

In addition, because third parties must rely upon businesses to provide the disclosure required by § 1798.115(d), implementing regulations should clarify that third parties are entitled to rely on contractual assurances by a business that the business has provided consumers with the required notice and choice in advance of a sale.

Proposed Regulatory Language:

The requirement that a consumer receive explicit notice and an opportunity to opt out of third-party re-sales of personal information pursuant to subdivision (d) of section 1798.115 of the Act shall be met by the business that originally collected the personal information from consumers if such business is seeking to sell such personal information

to a third-party re-seller. Third-party re-sellers may rely on contractual assurances from businesses from which they obtain personal information that such businesses have met the requirements of subdivision (d) of section 1798.115 of the Act. Third parties do not have an independent obligation to provide consumers with explicit notice and an opportunity to opt out of third-party re-sales of information pursuant to subdivision (d) of section 1798.115 of the Act when they have obtained such contractual assurances.

D. CCPA implementing regulations should clarify the application of the 12-month “lookback” period.

Section 1798.130 of the CCPA requires in several places that a business provide consumers with information regarding the business’s collection, processing, or sale of PI in the 12 months preceding a consumer request for the same. However, the NAI does not believe that the CCPA’s drafters intended to place compliance obligations on businesses with respect to activity that preceded the Act’s effective date.

Therefore, we recommend that implementing regulations clarify that any 12-month lookback periods a business is subject to under the Act will not extend to any time before the Act’s effective date, or the date on which the implementing regulations take effect.

Proposed Regulatory Language:

Where a business is otherwise required by the Act to take any action in response to a consumer request with respect to information collected, processed, or sold by the business in the 12 months preceding the business’s receipt of a consumer request, a business is not required to take such action with respect to information collected, processed, or sold only before the later of the effective date of the Act or the effective date of these regulations.

Part IV: Other issues

A. CCPA implementing regulations should clarify that businesses may charge a reasonable fee for goods and services as an alternative to ad-supported goods or services.

Digital advertising allows websites, mobile apps, and other online platforms and services to provide ad-supported content or services to consumers for free or low-cost. To remain economically viable, online publishers and service providers must be able to charge a reasonable fee, or subscription, as an alternative to offering ad-supported content for those consumers who have exercised their right to opt out of popular data-driven advertising practices used to generate significant revenue. The CCPA recognizes this by explicitly not prohibiting a business “from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer’s data.”³⁵ However, businesses would benefit from clarification

³⁵ *Id.* § 1798.125(a)(2).

that they can rely on an assessment of fair market value for consumer use of the app, site or service, in lieu of consumer data-driven advertising. It would be unreasonable and impractical to expect companies to derive customized pricing on a per-user basis, depending on a calculated or estimated value of each individual consumer's data.

Proposed Regulatory Language:

The requirements of section 1798.125 of the Act shall not be construed to prevent a business from charging a reasonable fee for goods or services as an alternative to free or reduced-cost goods or service supported by advertising.

B. CCPA implementing regulations should clarify that businesses are not required to extend their data retention policies to respond to consumer requests.

Data minimization, including limits on retention of PI, is a critical element of the FIPPs and a common privacy protective practice employed by many companies to minimize the risk of unintended harmful uses of personal and sensitive personal information. The CCPA could conflict with this critical practice due to its lack of clarity regarding obligations for companies to reply to consumer requests.

Specifically, many companies are likely to delete consumer information stored after a period of a few months, while the CCPA places requirements on companies to share information with consumers collected for 12 months prior to a consumer request being made. CCPA implementing regulations should clarify that there is no obligation for a business to retain PI solely for the purposes of fulfilling a consumer request under the CCPA. Although § 1798.100(e) of the CCPA states that a business is not required to retain certain PI, implementing regulations should clarify its application to cover all the obligations under the CCPA. Any interpretation to the contrary would create additional privacy and security risks to PI by potentially requiring organizations to retain data longer than they otherwise would.

Proposed Regulatory Language:

Under no circumstances is a business required to retain PI solely for the purpose of fulfilling a consumer request made under the Act.

Conclusion:

The NAI is grateful for the opportunity to comment on the CCPA rulemaking process. In addition to these comments, we are also including reference materials developed by the NAI that can help illustrate how digital advertising works, and how it benefits both businesses and consumers. If we can provide any additional information or otherwise assist your office as it engages in the rulemaking process, please do not hesitate to contact David LeDuc at

[REDACTED]

Respectfully Submitted,

The Network Advertising Initiative

BY: David LeDuc
Vice President, Public Policy

Enclosures

Message

From: Melanie Tiano [REDACTED]
Sent: 2/19/2019 4:16:51 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Gerard Keegan [REDACTED]
Subject: Comments of CTIA on CCPA
Attachments: 190219 CTIA CCPA CA AG Comments.pdf
Flag: Follow up

To Whom It May Concern:

Attached please find written comments in response to the CCPA Rulemaking Process.

Please feel free to contact me with any questions.

Thank you,

Melanie Tiano



Melanie K. Tiano

Director, Cybersecurity and Privacy

1400 16th Street, NW

Washington, DC 20036





Before the
STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
ATTORNEY GENERAL'S OFFICE
Los Angeles, CA 90013

In the Matter of)	
)	
California Consumer Privacy Act Rulemaking)	Public Forums on the California
Process)	Consumer Privacy Act
)	
)	

COMMENTS OF CTIA

Gerard Keegan
Vice President, State Legislative Affairs

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th St. NW, Suite 600
Washington, DC 20036
[REDACTED]
www.ctia.org

February 19, 2019

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY	1
II. CTIA SUPPORTS COMPREHENSIVE, TECHNOLOGY-NEUTRAL FEDERAL PRIVACY LEGISLATION.....	2
III. THE ATTORNEY GENERAL SHOULD DEVELOP CCPA IMPLEMENTATION AND ENFORCEMENT POLICIES THAT MINIMIZE UNINTENDED CONSEQUENCES TO CONSUMERS AND MAJOR DISRUPTIONS TO BUSINESSES.	4
A. The Attorney General Should Adopt Rules That Prevent The CCPA– And Its Compliance Obligations – From Becoming Unmanageably Broad.	5
1. The Attorney General Should Clarify The Definition Of “Consumer.”	5
2. The Attorney General Should Adopt Limiting Interpretations Of “Personal Information.”	6
B. The Attorney General Should Adopt Interpretations of the CCPA That Minimize Privacy And Security Risks.	8
1. Privacy And Data Security Considerations In Standards Governing Verifiable Consumer Requests Must Be Paramount.	8
2. Businesses Should Not Be Required To Provide Consumers With “Specific Pieces Of Personal Information” That Create Privacy And Data Security Risks.	9
3. Requiring Businesses To Provide Personal Information About Someone Other Than The Individual Making The Request Runs Counter To The Goals Of The Law.	9
4. Businesses Should Not Be Obligated To Retain Personal Information.	10
C. The Attorney General Should Adopt Regulations That Mitigate Serious Practical Compliance Challenges.	10
1. The CCPA’s Opt-Out Requirements Warrant Clarification.	10
2. The Consent Requirements Concerning Minors’ Information Need Clarification.	11
3. The Date of Compliance Obligations Under the CCPA Needs Clarification.	13
4. The Look-Back Period For Access Requests Needs Clarification.	13
5. The Attorney General Should Clarify The Standard Governing Discount and Incentive Programs.	14
IV. CONCLUSION.....	15

Before the
STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
ATTORNEY GENERAL'S OFFICE
Los Angeles, CA 90013

In the Matter of)	
)	
California Consumer Privacy Act Rulemaking Process)	Public Forums on the California Consumer Privacy Act
)	
)	

I. INTRODUCTION AND SUMMARY.

CTIA¹ welcomes this opportunity to respond to the California Attorney General Office's invitation to comment on regulations to implement and further the purposes of the California Consumer Protection Act of 2018 ("CCPA" or "Act").² CTIA members are committed to protecting the privacy of their customers. Consumer trust is essential for the continued growth of the mobile ecosystem, and appropriate privacy protections are integral to building and maintaining this trust. Members of the wireless industry therefore have strong incentives to develop robust privacy programs and practices.³ As a result, for years, recognizing that

¹ CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

² Codified as amended at Cal. Civ. Code § 1798.100 *et seq.* Unless otherwise noted, all statutory citations in this comment are to the codification of AB 375 in the California Civil Code, as amended by SB 1121 (published Sept. 24, 2018 9:00 PM).

³ See Comments of CTIA, *In the Matter of Developing the Administration's Approach to Consumer Privacy*, Nat'l Telecoms. and Info. Admin ("NTIA"), Request for Comments, Docket No. 180821780-8780-01 (Nov. 8, 2018) ("CTIA's Nov. 8 Comment to NTIA").

protections must not stop at compliance with existing regimes, the wireless industry has embraced a leadership role on privacy.

In these initial comments CTIA identifies key concerns and challenges with implementation of the CCPA that warrant attention by the Attorney General's Office. We take as a guiding principle the Legislature's intent of protecting consumers' privacy through the CCPA. To that end, CTIA urges the Attorney General to use the authority granted by the Act to develop and implement regulations that bring clarity to the unclear or ambiguous statutory provisions discussed, that otherwise will operate to the detriment of consumers and businesses. CTIA looks forward to working with your office as this rulemaking process proceeds. To that end, CTIA is currently working on proposed regulatory language to address some of the issues of concern identified in this comment.

II. CTIA SUPPORTS COMPREHENSIVE, TECHNOLOGY-NEUTRAL FEDERAL PRIVACY LEGISLATION.

CTIA commends the Attorney General's Office for conducting an open, inclusive comment process before beginning more formal rulemaking proceedings. The complexity associated with the CCPA outstrips earlier instances in which California was the first state to legislate on consumer privacy and data security matters.⁴ Therefore, given the CCPA's breadth and brief timetable to prepare for compliance, it is appropriate that the Attorney General is seeking comment from stakeholders.

Still, CTIA wishes to clarify its position that consumer privacy is a national issue that is best addressed through nationally uniform, technology-neutral federal privacy legislation. Such legislation should avoid duplicative obligations and distinctions based on who holds or collects

⁴ See, e.g., California Online "Eraser" Law, Cal. Bus. & Prof. Code §§ 22580 – 22582; California Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575 – 22579; California data breach notification law, Cal. Civ. Code §§ 1798.29, 1798.82.

personal information.⁵ The current U.S. approach to consumer privacy, which is fragmented by industry and national and state borders, strains companies' resources and creates uncertainty for both consumers and businesses.⁶ As the U.S. Department of Commerce's National Telecommunications and Information Administration recently noted, the "patchwork of competing and contradictory baseline laws" fails to improve privacy outcomes, creates the risk of confusing customers about how their data will be treated and what their rights are, and burdens the private sector with serious compliance challenges and other costs.⁷

CTIA and the wireless industry long ago took action to address many of the concerns that lie behind the enactment of the CCPA and debates about federal consumer privacy legislation. For example, CTIA and wireless carriers enshrined their commitment to protecting privacy online through a set of core privacy principles: the ISP Privacy Principles.⁸ These principles reflect the wireless industry's commitment to transparency, consumer choice, data security, and notifying consumers of security breaches. Other industry commitments likewise reflect the industry's view of transparency, for example, CTIA's *Consumer Code for Wireless Service*.⁹ These principles and guidelines also provide businesses with flexibility in developing and maintaining processes and systems to operationalize privacy and data security practices within their businesses. By contrast, overly broad and prescriptive privacy laws could impede

⁵ See CTIA's Nov. 8 Comment to NTIA at 3.

⁶ *Id.* at 3.

⁷ See NTIA, Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48,600, 48,602 (Sept. 26, 2018) ("NTIA RFC").

⁸ CTIA et al., *ISP Privacy Principles* (Jan. 27, 2017), <https://api.ctia.org/docs/default-source/default-document-library/final---protecting-consumer-privacy-online.pdf>.

⁹ See CTIA, *Consumer Code for Wireless Service*, <https://www.ctia.org/the-wireless-industry/industry-commitments/consumer-code-for-wireless-service>; see also CTIA, *Wireless Industry Commitments*, <https://www.ctia.org/the-wireless-industry/industry-commitments>.

industry's ability to innovate, limit beneficial uses of data, and inhibit businesses' ability to deliver services that consumers demand.

CTIA urges the Attorney General's Office to consider these and other instances of industry leadership as well as strong and broad support for a uniform national approach to consumer privacy¹⁰ through its public forums and the development of regulations to implement the CCPA.

III. THE ATTORNEY GENERAL SHOULD DEVELOP CCPA IMPLEMENTATION AND ENFORCEMENT POLICIES THAT MINIMIZE UNINTENDED CONSEQUENCES TO CONSUMERS AND MAJOR DISRUPTIONS TO BUSINESSES.

The CCPA requires the Attorney General to issue regulations to implement certain portions of the CCPA and grants broad authority to adopt regulations that further the purposes of the Act.¹¹ CTIA urges the Attorney General to use this authority to bring clarity to several CCPA provisions that are unclear or ambiguous, to the detriment of both consumers and businesses. In these initial comments CTIA identifies key challenges that warrant attention by the Attorney General's Office. Most of these issues involve not only ambiguity in the statutory text, but also tension with the Legislature's intent of protecting consumers' privacy through the CCPA.¹² For instance, CCPA's broad access and portability requirements combined with a capacious definition of personal information are overly burdensome on businesses and in tension with data minimization and other privacy principles.¹³

¹⁰ A review of the more than 200 comments filed in response to the NTIA RFC revealed support for federal privacy legislation among a broad array of stakeholder groups and widespread support for uniform federal consumer privacy standards among industry commenters.

¹¹ See Cal. Civ. Code §1798.185(a).

¹² See AB 375 § 2(i) (declaring that "it is the intent of the Legislature to further Californians' right to privacy by giving consumers an effective way to control their personal information" through the rights defined under the CCPA).

¹³ See e.g., Peter Swire and Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 Md. L. Rev. 335, 339 (2013),

A. The Attorney General Should Adopt Rules That Prevent The CCPA – And Its Compliance Obligations – From Becoming Unmanageably Broad.

1. The Attorney General Should Clarify The Definition Of “Consumer.”

CCPA’s definition of “consumer” is extremely broad and appears to encompass all natural persons who are California residents, even in their capacities as employees, independent contractors, or persons involved in business to business transactions.¹⁴ This potential interpretation is contrary to the Legislature’s intent to protect the privacy of individuals in relation to the collection, use, and disclosure of personal information for commercial purposes – *i.e.*, in the commonly used sense of “consumer.”¹⁵

CTIA urges the Attorney General to clarify that the definition of “consumer,” and therefore the rights accorded under the Act, only apply to individuals whose personal information is obtained as a result of their purchase or use of a product or service for personal, family, or household purposes. In particular, the Attorney General should not interpret the CCPA to apply to personal information that businesses collect and maintain about employees and independent contractors, or collect in the course of the employer-employee relationship. Extending the full set of individual rights created under the CCPA could affect businesses’ ability to comply with a broad range of laws, from state employment law where, for example, California law already establishes rights and obligations concerning personnel and wage

<http://digitalcommons.law.umaryland.edu/mlr/vol72/iss2/1/>(noting that “One moment of identity fraud can turn into a lifetime breach of personal data); Mark Warner, *Potential Policy Proposals for Regulation of Social media and Technology Firm*, Draft White Paper (2018), p. 21, https://regmedia.co.uk/2018/07/30/warner_social_media_proposal.pdf (acknowledging that data portability can pose a number of cybersecurity risks if not implemented correctly).

¹⁴ See Cal Civ. Code § 1785.140(g). See also *id.* § 1798.140(o)(1)(I) (including “professional or employment-related information” in the definition of “personal information”).

¹⁵ See AB 375 §§ 2(c)-(h) (published June 29, 2018 4:00 AM).

records,¹⁶ to federal anti-money laundering laws.¹⁷ The Attorney General has the authority to issue regulations to prevent the CCPA from interfering with such compliance obligations.¹⁸

2. The Attorney General Should Adopt Limiting Interpretations Of “Personal Information.”

a. Clarify that “Personal Information” should be reasonably linkable to an individual.

The CCPA’s extremely broad definition of “personal information”¹⁹ could lead to unintended negative consequences for both consumers and businesses, ranging from enabling the release of an individual’s personal information to others to impeding the use of information that poses little or no privacy risk. Unlike the definition of “consumer data” in the Federal Trade Commission’s 2012 Privacy Framework, which is limited to information that “can be reasonably linked to a specific consumer, computer, or other device,”²⁰ the CCPA’s definition of “personal information,” deems several categories of information – including, for example, olfactory information and the characteristics of groups of consumers – to be personal, provided they are “capable of being associated” with an individual.²¹

This breadth creates enormous implementation and compliance obstacles for businesses. It is unclear how a business could be expected to respond to “verifiable consumer requests” to provide consumers with all personal information it holds about the consumer making the request

¹⁶ See, e.g., Cal. Labor Code §§ 1198.5, 226(b), 432.

¹⁷ Businesses are required to maintain complete and accurate records for certain commercial transactions. Allowing consumers to delete and alter personal information could make it impossible for businesses to comply with these laws.

¹⁸ See Cal Civ. Code § 1798.185(a)(3) (requiring the Attorney General to adopt regulations “[e]stablishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, . . .”).

¹⁹ See Cal Civ. Code § 1785.140(o).

²⁰ FTC 2012 Privacy Report at 22.

²¹ See Cal Civ. Code §§ 1798.140(o)(1)(C), (H).

if some information is merely “capable of being associated” with that consumer or a device. Therefore, CTIA urges the Attorney General to follow the FTC’s and other privacy frameworks, and clarify that personal information is limited to information that is linked or reasonably linkable to a particular consumer. A contrary interpretation, under which businesses might be required to attempt to “match up” unlinked information to consumers, would increase the potential for privacy harms and make the information a more attractive target for identity thieves.

b. *Clarify that businesses have the right under the CCPA to create deidentified, aggregate, and pseudonymized information.*

Deidentification and aggregation create privacy and security benefits, such as facilitating information sharing, turning useful data into a less attractive target to bad actors, and improving traffic flow and transportation infrastructure.²² Although Section 1798.145(a)(5) appears to recognize the important benefits of aggregate and deidentified information, the CCPA does not explicitly grant businesses the right to create such data—a necessity for businesses to be able to use the data. Notwithstanding the amendments to the definition of personal information made by SB1121, CTIA is concerned that the definition is extremely broad, and that coupled with the narrow definition of deidentified information, these privacy-protective uses of data may be foreclosed. To give effect to the CCPA’s allowing businesses to “collect, use, retain, sell, or

²² See Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data*, 64 Stan. L. Rev. Online 63 (2012), <https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data/> (discussing manifold public interest benefits from big data analytics and arguing that sophisticated re-identification should underscore, rather than undermine, importance of de-identification); Ann Cavoukian & Khaled El Emam, *Dispelling the Myths Surrounding De-Identification* (2011), <https://www.ipc.on.ca/images/Resources/anonymization.pdf>; see also Reply Comments of T-Mobile USA, Inc., WC Docket No. 13-306, at 3-7 (Mar. 4, 2014) (addressing studies and concluding that “the risk of privacy harm from re-identification is significantly lower than many risks we take without concern” (internal quotation marks omitted); *id.* at 7-8 (recounting various uses of de-identified data in the public interest).

disclose” deidentified or aggregate consumer information,²³ CTIA recommends that the Attorney General issue rules to explicitly permit the creation of such data.

Similar benefits apply to pseudonymous information, in which identifying fields in a data set are replaced with pseudonyms, thus de-linking the information from an individual or device and reducing concerns about data retention and data sharing. The Attorney General should clarify that pseudonymous information is a form of deidentified information and may be treated as such under the CCPA.

B. The Attorney General Should Adopt Interpretations of the CCPA That Minimize Privacy And Security Risks.

1. Privacy And Data Security Considerations In Standards Governing Verifiable Consumer Requests Must Be Paramount.

The Attorney General’s Office should carefully consider privacy and data security risks when developing standards governing “verifiable consumer requests.”²⁴ In many industries, joint accounts are common; thus, multiple users’ personal information could be collected on one registered account through sub-accounts or separate profiles. Many companies already have procedures in place to address the difficult privacy and data security challenges that may arise from the creation of sub-accounts or separate profiles. In developing regulations to verify consumer requests, the Attorney General’s Office should allow companies flexibility in how to verify consumer requests. This will allow for the development of innovative and accurate methods to address data security risks and ensure that consumers’ personal information is not erroneously disclosed.

²³ Cal Civ. Code § 1798.145(a)(5).

²⁴ See *id.* §§ 1798.140(y) (defining “verifiable consumer request”) and 1798.185(a)(7) (requiring the Attorney General to establish rules and procedures governing, among other things, “a business’s determination that a request for information received by a consumer is a verifiable consumer request”).

2. Businesses Should Not Be Required To Provide Consumers With “Specific Pieces Of Personal Information” That Create Privacy And Data Security Risks.

Compliance with the CCPA should not entail the creation of additional privacy or data security risks, but the CCPA’s access provisions create this danger. The Attorney General should adopt interpretations that mitigate those risks.

For example, Section 1798.100(a) requires businesses to provide “specific pieces of personal information the business has collected” about consumers, which can create cybersecurity and fraud risks. While the statute does not explain how extensive this obligation is, or define what it means by “specific pieces of personal information,” certain categories of information that are included in CCPA’s definition of personal information, such as social security numbers, driver’s license numbers, and passport numbers, are especially attractive to identity thieves. CTIA recommends that the Attorney General issue regulations, pursuant to the grant of authority in Section 1798.185(a)(7)²⁵ to exclude these and other categories of sensitive information that raise particular concerns. California’s data security law²⁶ is instructive in this regard, as it identifies categories of information that require businesses to have practices and procedures to protect.

3. Requiring Businesses To Provide Personal Information About Someone Other Than The Individual Making The Request Runs Counter To The Goals Of The Law.

The CCPA requires businesses to respond to “verifiable consumer requests” for personal information by providing personal information it holds about not only the requester, but also anyone in the requester’s household, including, potentially, an abused spouse or a roommate.

²⁵ Section 1798.185(a)(7) requires that the Attorney General take into consideration security concerns, among other things, when establishing rules and procedures to facilitate a consumer’s ability to obtain information a business holds about them.

²⁶ See Cal. Civ. Code § 1798.81.5.

This requirement to turn over information about another person runs counter to the privacy goals of the CCPA by creating privacy risks and even potential physical harms. To the extent permissible, the Attorney General should interpret the CCPA’s access provisions to require responses that relate only to information about the specific individual who makes a request and not others (*e.g.*, members of a household) who might be captured by the definition of “personal information.”

4. Businesses Should Not Be Obligated To Retain Personal Information.

The CCPA provides that businesses are not required to retain personal information of consumers collected for a “single one-time transaction” if it would ordinarily delete the information is the normal course of business.²⁷ Although this provision appears to be intended to encourage companies to adhere to data minimization principles by deleting personal information they do not need, the narrowness of this exception could be construed to imply that businesses are required to retain personal information outside of “single one-time transactions” in order to fulfill consumer data access requests. Such an obligation would create additional privacy and data security risks as well as impose significant unnecessary costs on businesses. Accordingly, the Attorney General should clarify that even beyond “single one-time transactions,” businesses do not need to retain data they otherwise would not in order to fulfill verifiable requests from consumers.

C. The Attorney General Should Adopt Regulations That Mitigate Serious Practical Compliance Challenges.

1. The CCPA’s Opt-Out Requirements Warrant Clarification.

The interaction between the CCPA’s opt-out provisions and the opt-in practices of many companies presents practical challenges. One issue is that “right to opt-out” appears to envision a

²⁷ See Cal. Civ. Code §§ 1798.100(e), 110(d)(1).

single, globally applicable choice that does not take into account prior choices that consumers have made.²⁸ For example, in many instances consumers opt in to specific uses or disclosures of their personal information, such as enrolling in business loyalty programs. Providing consumers with a single global opt-out could negate any prior choices consumers may have made and could clash with their expectations. Therefore, CTIA recommends that the Attorney General develop regulations that would allow businesses to provide both a global opt-out choice, as well as more granular opt-out choices to consumers.

Relatedly, the Attorney General's Office should clarify that the definition of "homepage" on which a business is required to provide a clear and conspicuous "Do Not Sell" link, does not require the link to appear on every web page on which a business collects personal information.²⁹ The CCPA definition of "homepage" could be interpreted to require such a result, which would be inconsistent with the word's common meaning, not necessary for consumers to exercise their opt-out rights, and would create unnecessary costs for businesses.³⁰

2. The Consent Requirements Concerning Minors' Information Need Clarification.

a. CCPA's "actual knowledge" standard should not trigger a duty to inquire.

The CCPA provides an opt-in rule for the sale of minors' personal information when a business has "actual knowledge" that the consumer is less than 16 years old.³¹ The provision however also contains an inconsistent sentence that appears to suggest that "willful disregard" of

²⁸ See *id.* § 1798.120(a)-(b).

²⁹ See *id.* §§ 1798.140(l); 1798.135(a)(1).

³⁰ Merriam-Webster defines "homepage" as "the page typically encountered first on a website that usually contains links to the other pages of the site."

³¹ See Cal. Civ. Code § 1798.120(c).

a consumer's age would be deemed to create actual knowledge of the consumer's age. Willful disregard is not part of an "actual knowledge" standard, and not part of similar laws related to children's privacy, including the federal Children's Online Privacy Protection Act ("COPPA").³²

In fact, in amending the COPPA rules in 2013, the FTC considered and rejected such a standard ultimately deciding to impose requirements on operators of general audience websites or online services only when they *have actual knowledge* they are collecting personal information online from a child under 13 years of age. Specifically, the FTC considered a "knows or had reason to know standard," but rejected it, concluding "it would be impossible to determine the type of notification that would provide a 'reason to know.'"³³ It would be similarly impossible to determine the type of notification that would evidence a "willful disregard." Including this standard would trigger an affirmative duty to inquire, and would force businesses to review data they otherwise would not, thereby creating unnecessary privacy and data security risks.

b. Opt-in consent requirements for the sale of consumers' personal information do not apply to 16-year-old consumers.

The CCPA prohibits the sale of a consumer's information, absent opt-in consent, if the consumer is "*less than 16*," meaning 15 or younger. The provision however, allows the business to receive an opt-in from the consumer when the consumer is "*between 13 and 16 years of age*". Since the statute states that the heightened opt-in standard only applies to consumers age 15 and younger, the Attorney General should clarify that businesses should not be required to obtain such consent from consumers beyond that age.

³² 15 U.S.C. §§ 6501 *et seq.*

³³ Federal Register Vol. 78, No 12 at 3978 (Jan 17, 2013).

3. The Date of Compliance Obligations Under the CCPA Needs Clarification.

Although SB 1121 helpfully extended by six months the deadline for the Attorney General to issue certain implementing regulations, this amendment also created an unfortunate potential compliance challenge. Businesses' obligations under the CCPA go into effect on January 1, 2020.³⁴ The deadline for the Attorney General to issue required regulations is July 1, 2020,³⁵ and the Attorney General can begin bringing enforcement actions either six months *after* "publication of the final regulations" or July 1, 2020, whichever is *sooner*.³⁶ This situation could require companies to be in compliance with the CCPA before the Attorney General's regulations are published.³⁷ Moreover, given the ambiguity and tension between several CCPA provisions and the purposes of the Act as a whole, these regulations could significantly change businesses' compliance obligations. This situation creates needless uncertainty and significantly increases the burdens on businesses. In light of these uncertainties, the Attorney General should clarify the timetable for issuing regulations and his enforcement priorities.

4. The Times For Responding To Access Requests And Look-Back Period Need Clarification.

The Act lays out two potentially contradictory time periods for businesses to respond to consumers' requests for information. Section 1798.130(a)(2) provides businesses with up to 45 days to respond to a verifiable request for information, with an additional 45 days when "reasonably necessary," so long as notice of the extension is provided within the initial 45 day period. Separately, Section 1798.145(g)(1) provides that, "notwithstanding a business'

³⁴ See *id.* § 1798.198(a).

³⁵ *Id.* § 1798.185(a).

³⁶ *Id.* § 1798.185(c).

³⁷ See *id.*

obligations to respond to and honor consumer rights requests pursuant to this title,” the period for responding may be extended “up to 90 additional days where necessary, taking into account the complexity and number of requests.” The Attorney General should clarify whether these provisions should be read independently, such that, where necessary, a business has up to a total of 180 days to respond to verifiable requests, or in conjunction, where the 90 days extension in section 1798.145(g)(1) runs concurrently with the 45-day extension in section 1798.130(a)(2).

A further area that requires clarification concerns requests for information encompassing time periods that precede January 1, 2020. As provided in Section 1798.130(a), disclosures under sections 1798.100-115 and 125 must cover the 12 months prior to receipt of a verifiable consumer request. This would appear to require companies to provide responsive information back to January 1, 2019 – a full year before the CCPA goes into effect and up to 18 months before the Attorney General publishes regulations on verifiable consumer requests and provides other needed clarifications of the CCPA. The Attorney General should clarify that, given that the title is operative on January 1, 2020, a consumer request made in 2020 will only cover personal information collected from January 1, 2020.

5. The Attorney General Should Clarify The Standard Governing Discounts and Incentive Programs.

The CCPA provides inconsistent standards to govern discounts and incentive programs,³⁸ which are of major consumer and commercial importance. Specifically, certain differences related to price or rate, or level or quality of goods and services are permissible if they are “*reasonably related*” to the value of the consumer’s data under Section 125(a)(2), but Section 125(b)(1) requires differences to be “*directly related*” to the value of the data. The Attorney

³⁸ See Cal. Civ. Code § 1798.125.

General should clarify that “directly related to the value of the data” means that there is a reasonable relation between the value of the consumers data to the business, and the different price or level or quality of goods or services offered to the consumer.


IV. CONCLUSION.

CTIA appreciates the opportunity to provide the Attorney General’s Office with these initial comments on key challenges with implementation of the CCPA, and looks forward to continuing to work with you as this rulemaking process proceeds.

Respectfully submitted,

/s/ Gerard Keegan
Gerard Keegan
Vice President, State Legislative Affairs

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th St. NW, Suite 600
Washington, DC 20036

www.ctia.org

February 19, 2019

Message

From: Blenkinsop, Peter [REDACTED]
Sent: 3/8/2019 1:26:50 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments of the International Pharmaceutical & Medical Device Privacy Consortium ("IPMPC")
Attachments: IPMPC Comments to California Department of Justice re CCPA.pdf

Dear Attorney General Becerra,

On behalf of the International Pharmaceutical & Medical Device Privacy Consortium ("IPMPC"), I am pleased to submit these comments on the development of regulations under the California Consumer Privacy Act (CCPA). Further information concerning the IPMPC can be found at <https://www.ipmpc.org>.

Thank you for your consideration.

Sincerely,
Peter Blenkinsop
IPMPC Secretariat

Peter Blenkinsop

IPMPC Secretariat

Drinker Biddle & Reath

1500 K Street, NW, Ste 1100, Washington, DC 20005

Tel: [REDACTED]



IPMPC

International Pharmaceutical &
Medical Device Privacy Consortium

Drinker Biddle & Reath LLP is a Delaware limited liability partnership. The partner responsible for the firm's Princeton office is Dorothy Bolinsky, and the partner responsible for the firm's Florham Park office is Andrew B. Joseph.

This message contains information which may be confidential and privileged. Unless you are the intended addressee (or authorized to receive for the intended addressee), you may not use, copy or disclose to anyone the message or any information contained in the message. If you have received the message in error, please advise the sender at Drinker Biddle & Reath LLP by reply e-mail and delete the message. Thank you very much.



IPMPC

International Pharmaceutical &
Medical Device Privacy Consortium

March 8, 2019

Mr. Xavier Becerra
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

By Email to: PrivacyRegulations@doj.ca.gov

Re: CCPA Regulations

Dear Attorney General Becerra,

The International Pharmaceutical & Medical Device Privacy Consortium (“IPMPC”) welcomes the opportunity to provide comments on the development of regulations under the California Consumer Privacy Act (CCPA).

The IPMPC is comprised of chief privacy officers and other data privacy and security professionals from a number of research-based, global pharmaceutical companies and medical device manufacturers.¹ The IPMPC is the leading voice in the global pharmaceutical and medical device industries to advance innovative privacy solutions to protect patients, enhance healthcare, and support business enablement.²

We welcome the opportunity to provide comments at this preliminary stage of the rulemaking process. We note that the legislature has given the Attorney General broad

¹ IPMPC members may also operate related businesses, including CLIA laboratories.

² More information about IPMPC is available at <https://www.ipmpc.org/>. This filing reflects the position of the IPMPC as an organization and should not be construed to reflect the positions of any individual member.

discretionary authority to adopt regulations “to further the purposes of this title.”³ This may include, but is not limited to, the specific issues enumerated at Civil Code § 1798.185(a). We have focused our comments on the following areas where we believe regulations are needed in order to promote a common understanding of CCPA requirements:

- 1) What qualifies as a “particular consumer or household” for purposes of the definition of “personal information” at Civil Code § 1798.140(o).
- 2) The scope of the medical research provision at Civil Code § 1798.145(c)(1)(C).
- 3) The scope of the HIPAA exemption at Civil Code § 1798.145(c)(1)(A).

I. “Particular Consumer or Household”

The definition of “personal information” at Section 1798.140(o) means “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with *a particular consumer or household*” (emphasis added). It is, therefore, critical for all stakeholders to have a clear understanding of what qualifies as a “particular consumer or household.”

As a preliminary matter, it is important to note that the inclusion of “household” in the definition of “personal information” creates considerable confusion. How, for example, would access rights apply in this context? Would all members of a household be entitled to access the information that a business holds that relates to any member of that household? The application of the law would be clearer if the legislature were to delete the reference to “household.” If this does not occur, however, it will be necessary for the Attorney General to issue rules that clarify how the Act is intended to operate in this context.

It is clear from the fact that the legislature included a definition of “deidentified” information that the legislature did not intend for all information that “describes” or “relates to” a particular individual or household to be considered “personal information,” regardless of the identifiability of such information. To give effect to the apparent legislative intent, it would be prudent to adopt regulations clarifying that (i) “a particular consumer or household” means an identifiable consumer or an identifiable household; (ii) an identifiable consumer is a consumer (as defined in the Act) who can be identified by the business who collects such information, without expending disproportionate efforts or resources, by reference to a name, contact information, or communications device; and (iii) an identifiable household refers to shared users of a personal computer or other personal communications device that can be uniquely identified.

³ California Civil Code § 1798.185(a) and (b).

The IPMPC believes that this proposed clarification protects individual privacy while recognizing that not all individual-level data raises privacy concerns. If information can be associated with a particular consumer or household by name, address, or other contact information, or if the information can be used to communicate with the consumer or household (such as to deliver advertising messages), then the information may trigger privacy interests. Information that does not meet one of these criteria should not be covered as “personal information.”

II. Health Research Exemption

Civil Code § 1798.145(c)(1)(C) states that the CCPA does not apply to “[i]nformation collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.” We understand this exemption to cover health research that is conducted (i) pursuant to the federal Common Rule; or (ii) following ICH E6 GCP standards; or (iii) following FDA human subject protection standards as may be found at 21 C.F.R. Part 50. We would appreciate confirmation of this interpretation.

III. HIPAA Exemption

Civil Code § 1798.145(c)(1)(A) states in relevant part that the CCPA does not apply to “protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations.” We understand the purpose of this exemption is to recognize that collection, use, and disclosure of patient health information is already regulated at the federal level, and, therefore, to exempt this information from the scope of application of the CCPA. We presume that information that is considered de-identified under HIPAA would not be considered “personal information” under the CCPA. Nevertheless, in the unlikely event HIPAA de-identified health information were viewed by the Attorney General as still constituting “personal information” under the CCPA, then we think it is clear that the legislature intended for this information to be exempt from CCPA requirements pursuant to Section 1798.145(c)(1)(A). We would appreciate confirmation of this interpretation as well.

We are also attaching to these comments, our position paper on “Issues Under the CCPA Needing Further Clarification or Amendment.” While some of the issues in the position paper likely

require legislative action, we believe the issues discussed above clearly rest within the Attorney General's rulemaking authority.

We thank you for the opportunity to provide these comments. We applaud your efforts to solicit public input early in the rulemaking process.

Sincerely,

A handwritten signature in black ink, appearing to read "Peter Blenkinsop". The signature is fluid and cursive, with the first name "Peter" and last name "Blenkinsop" clearly distinguishable.

Peter A. Blenkinsop
IPMPC Secretariat



Issues Under the CCPA Needing Further Clarification or Amendment

The International Pharmaceutical & Medical Device Privacy Consortium appreciates the efforts of California lawmakers and the Office of the Attorney General to craft legislation and implementing rules that protect the privacy of California consumers while recognizing the legitimate needs of businesses to collect and use personal information. Clarification of the following areas of the California Consumer Privacy Act (CCPA) is needed to ensure that there are no unintended effects of the law and compliance efforts are focused on those issues that pose the greatest privacy risk.

1. References to “research” should be aligned to existing standards for scientific research activity and should permit research activities undertaken by private businesses to develop new products and services, especially in the area of researching and developing new treatments, diagnostics, medical devices, therapies, and cures for diseases and conditions that affect California residents.
2. The definition of “personal information” should more clearly exclude information that cannot be used without disproportionate efforts to identify the subject of the information. The definition of “de-identified” should be modified in a corresponding fashion. In addition, to more closely align with federal law, the definition of “de-identified” should be modified by adding a new sentence, as follows: “For purposes of this title, ‘de-identified’ shall include information that meets the requirements of 45 C.F.R. 164.514(b) for de-identified information or 164.514(e)(2) for a limited data set.”
3. The definition of “publicly available” information should be revised to include both (i) information that is lawfully made available from federal, state, or local government records; and (ii) information manifestly made public by or on behalf of the consumer.
4. If a business maintains personal information in a pseudonymized form, the business should not be obliged to acquire or maintain additional information in order to identify the individual for the sole purpose of complying with a requirement under the CCPA.
5. A “consumer” should be defined as a California resident who purchases or uses a product or service in a personal capacity. “Consumer” should not include individuals acting in their capacity as employees or as professionals.
6. Businesses should be allowed flexibility to decide what mechanism(s) would be most effective for enabling consumers to exercise their rights, provided that at least one mechanism is provided that is easy-to-use and cost-free.

7. A safe harbor to the private right of action should be included for businesses that have implemented a data security program consistent with recognized industry standards.
8. The CCPA should apply only to personal information collected or disclosed after the effective date of the law. Businesses require adequate time after the promulgation of rules by the Office of the Attorney General to modify their business practices in order to comply.

Message

From: Chris Stewart RRP [REDACTED]
Sent: 3/8/2019 9:14:15 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on California Consumer Privacy Act (CCPA)
Attachments: CA CCPA COmments ARDALetterhead 3.7.19.doc

Please accept the attached comments regarding the implementation of the CCPA. If you have any questions to would like additional information, please contact me at your convenience.



Chris Stewart RRP | Vice President, State Government Affairs
American Resort Development Association (ARDA)

Landmark Center Two
225 E. Robinson Street, Suite 545
Orlando, FL 32801

[REDACTED]
www.arda.org | www.arda-roc.org | www.vacationbetter.org



March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St., Los Angeles, CA 90013

RE: Comments on California Consumer Privacy Act (CCPA)

I am writing on behalf of the American Resort Development Association (ARDA). ARDA is the trade association representing the interests of the timesharing and vacation ownership industry. Founded in 1969, ARDA represents more than 1,000 timeshare development and related service corporations. It is the mission of ARDA to foster and promote the growth of the timeshare and vacation ownership industry and to serve its members through education, public relations and communications, legislative advocacy, membership development and ethics enforcement.

ARDA supports the protection of consumer privacy and reasonable transparency that allows consumers to make meaningful decisions regarding consumers' access and control over their personal information. ARDA appreciates this opportunity to comment on the Attorney General's efforts to promulgate balanced regulations related to implementation of the CCPA.

ARDA's concerns with the legislation primarily focus on the definitions of certain terms, only some of which we are addressing in these comments. The unclear scope for each of these terms permeates through multiple aspects of the CCPA and compounds the confusion for businesses who will be trying to comply with many new requirements under this expansive piece of legislation. Additionally, consumer control and protections of their personal information are exposed to unintentional risks as a result of the lack of clarity in certain defined terms. We will address each of these in turn.

1. "Personal Information"

The broad definition of "personal information" presents challenges to effective compliance and consumer service. The definition far exceeds the current definition of "personal information" under previously existing California law and even goes farther than the definition under the sweeping General Data Protection Regulation ("GDPR") in the European Union. For context, we note that it took over four years to enact the GDPR based on multiple revisions and debate, and even then guidance continues to be written. The CCPA was prepared and approved in significantly less time and has little to no guidance available.

a. "Personal information" should be limited to the individual consumer.

At the core of the CCPA is the protection of an individual's privacy. The use of a broad definition of "personal information" under Section 1798.140(o) will result in unintended consequences for several aspects of the CCPA and may unintentionally erode the protection of an individual's privacy. One concern with the term as defined is that it includes information that "could be reasonably linked, either directly or indirectly, with a particular...household." Thus, any categories or specific data elements may be related to others within a family as well as unrelated individuals living under the same roof.

The ability to respond appropriately to individual requests for access, deletion or even an opt-out becomes a challenge when “household” information is commingled across multiple individuals who may have different privacy preferences. For example, an individual consumer makes a request for deletion of their information related to a purchase contract. There may be more than one person in the household on the contract. The requesting consumer should not have the ability to request deletion of another consumer’s personal information without a reliable form of authorization from the second consumer, consistent with other parts of the CCPA and regulations. However, the business may not be able to delete all of the “household” information related to one individual without potentially deleting the same for another consumer residing in the same household. So that a business does not risk deleting more information than is necessary or deleting any personal information without the proper authorization, the Attorney General should adopt rules limiting the scope of “household” information solely to the requesting consumer, unless the business receives clear, reliable authorization that the request includes other individuals within the same household and each individual clearly agrees to the deletion or other change.

The same can be said for other information, like IP addresses, which by their nature are not capable of being tied to a single individual. This information is only representative of a broader household, a company or even a corner coffee shop’s guest Wi-Fi. The business receiving the request will have difficulty in narrowing the request to the individual given the unspecific nature of the information.

2. “Sell” (and its various forms)

The use of the term “sell” (and its various forms) throughout the legislation creates an undefined path for businesses. As defined in Section 1798.140(t), “sell,” “selling,” “sale,” and “sold” includes “otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or valuable consideration.” The few exceptions to this broad requirement fall short of providing adequate clarity and still requires clear guidance to avoid confusion.

- a. A “sale” must require a transfer from the business, not from the consumer, regardless of whether there is an exchange of valuable consideration.

The regulations adopted by the Attorney General should clarify that the selling of information must involve either the transfer of the personal information from the business to a third party or making the personal information viewable by the third party for money or other valuable consideration (see comment that follows). It should not include merely placing a third party’s advertising in communications to the business’s customers who must then directly contact the third party in order to engage in a transaction or inquiry.

- b. A “sale” should not include a transfer with the consumer’s consent even if there is an exchange of “valuable consideration.”

Similarly, as provided in Section 1798.140(t)(2)(A), the definition should not include where the consumer has provided consent for their personal information to be directly transferred from the business to the third party as part of a real-time hand off, like a call transfer, even if there is an exchange of valuable consideration between the business and the third party. In this instance, the consumer has directed the business to provide their personal information to the third party. The language in this subsection is confusing as it qualifies what appears to be a helpful exception for sharing personal information at the consumer’s direction with “provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title.” It should be

clear that this type of transfer is excluded from the definition of “sell” and the related implications set forth in the CCPA.

c. Clarify “other valuable consideration.”

The use of the vague term “other valuable consideration” causes a significant requirement within the CCPA to be open to confusion for compliance and arbitrary enforcement. Similar to the vagueness doctrine under criminal law, the use of such a vague term fails to provide “sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement.”¹ Accordingly, the Attorney General should clarify what is meant by “other valuable consideration.”

3. “Consumer”

The scope of the term “consumer” under Section 1798.140(g) is unclear and may unintentionally include employees.

The alleged activities that lead the California Legislature to enact the CCPA were focused on the use of consumer information in marketing and political campaign context, not in an employee/employer relationship. However, the broad definition of “consumer” lends itself to potentially include employees. Based upon the feedback the Attorney General has received during the public forums, this is clearly a point of uncertainty and concern for other businesses. To the extent there are any considerations related to the sale of employee information and the California Legislature determines such legislation the will of its constituency, the Legislature may want to take this under advisement for other legislation directed to that specific concern. The CCPA should be amended to clarify that it does not apply to employee personal information.

4. Consumer’s Right to Request and Business’s Obligation to Disclose

a. “Homepage” and placement of the “opt-out” button.

An additional concern relates to the requirement under Section 1798.135(a)(1) to place a link titled “Do Not Sell My Personal Information” on the website’s “homepage.” As defined in Section 1798.140(l), “homepage” includes “any Internet Web page where personal information is collected.” If, for example, a business collects IP addresses for purposes of making the visiting consumer’s experience more convenient (e.g., maintaining a log-in across several Web pages so the consumer is not logged out), this could be considered the collection of personal information. Accordingly, a business would essentially be required to maintain an opt-out button on each and every page of a website.

A more realistic guardrail on the provision of an opt-out “button” is to require it on no more than the front page of the website and only on a specific Web page to the extent that page requires active input of personal information (e.g., filling in contact information for a room reservation) by a consumer.

b. Disclosure only at the consumer’s request.

Section 1798.110(c)(5) appears to require a proactive disclosure of personal information to the granular level for each and every consumer. The preemptive disclosure of information down to the

¹ *Kolender v. Lawson*, 461 U.S. 352 (1983). (Without belaboring the point, we note that the “doctrine” might be slightly different in the administrative law context, but with similar effect.) As noted elsewhere in these comments, there are additional terms in the CCPA that suffer this same deficiency.

specific data elements on a consumer-by-consumer basis does not strike the appropriate balance between consumer notice and business efficiency.

The trigger for a business's obligation to disclose specific elements of personal information should only be the consumer's request for that information. If it is believed that the intent of this law is to require that a business proactively disclose all specific elements of personal information to each and every consumer, the California Legislature and/or the Attorney General should conduct a study to determine the relative cost of such endeavor to companies conducting business in California and the impact on the state's economy.

5. Responding to a Verifiable Consumer Request²

As contemplated by the CCPA, the rights of opt-out, access and deletion added by the legislation create opportunities for third parties to provide services on behalf of consumers. To avoid potential consumer harm and to provide businesses holding personal information clearer direction for compliance, the Attorney General should address two particular areas of concern.

- a. As related to persons authorized to act on behalf of consumers, Sections 1798.135(c) and 1798.145(a) are in conflict.

Section 1798.135(c), as amended, provides:

A consumer may authorize another person solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt-out received from another person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General. (Emphasis added.)

Further, Section 1798.145(a), as amended and in relevant part, directs the Attorney General to "solicit broad public participation and adopt regulations" to, among other things:

(7) Establish(ing) rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130....(Emphasis added.)

In crafting the CCPA, the Legislature identified the sole purpose an authorized agent could represent a consumer, i.e. to opt-out the consumer from a business's sale of their personal information. Only in a list of rulemaking tasks for the Attorney General in Section 1798.145(a) does the Legislature mention a third party acting on behalf of the consumer for other purposes. Accordingly, it is at a minimum unclear whether the CCPA allows a third party to make requests other than an opt-out on a consumer's behalf, requiring a clarifying rule, and at most creates a conflict that should be resolved by an amendment to the CCPA.

- b. For opt-out requests, and to the extent Sections 1798.135(c) and 1798.145(a) are not in conflict, for other requests, the Attorney General must adopt rules for authorized agents.

Pursuant to Sections 1798.135(c) and 1798.140(y), the Attorney General must adopt rules setting forth clear requirements about who a consumer can authorize to submit a request to opt-out of the sale of the consumer's personal information, including among other things, specific requirements for

² Note that Section 1798.145(g) uses the term "*verified* consumer request". This is an undefined term and could simply be a typographical error. However, either the Attorney General or the Legislature, as appropriate, must reconcile this inconsistency.

qualifications of the agent, the form of authorization, and penalties for violations. Further, notwithstanding the conflict identified in ARDA's comments in section 5(a) above, the Legislature must adopt similar rules for authorized agents making access, deletion and any other permitted request on behalf of a consumer.

Since the effective date of the GDPR, phishing and similar scams have targeted both data subjects and data controllers.³ Where these scams or even legitimate requests involve third parties purportedly making such requests on behalf of consumers (either knowingly or unknowingly) places businesses at a disadvantage when attempting to verify the requests. Not only must the business verify the identity of the consumer (to match to the personal information on file), it must also verify both the identity of the agent and the agent's qualification, and the validity of the consumer's authorization, if such is even included. The latter tasks, alone but certainly without further guidance, place an undue burden on businesses and impact a business's response timelines, particularly if such an agent purports to represent multiple consumers.

As part of the definition of "verifiable consumer request," Section 1798.140(y) provides only that the agent must be "registered with the Secretary of State." Most companies doing business in California must be similarly registered, and the Secretary of State does not issue licenses or permits.⁴ This presents a risk to consumers in several ways. First, a general business registration alone is insufficient to provide consumers with protections needed under the CCPA. Even if the extent of the service such an agent may perform is to request an opt-out, the consumer must still place in the custody and care of the agent personal information sufficient enough to be verified by the business holding the consumer's personal information.

Second, these companies can potentially charge unreasonable fees to the unwitting consumer without providing sufficient (or in some cases any) information to the business holding the personal information and misuse the personal information the consumer has provided them in order to perform the opt-out services or, in an access request, misuse the information obtained from the business on the consumer's behalf. While the legislation contains significant penalties against businesses holding personal information and the business's agents for violations of the CCPA, there don't appear to be any financial protections in place to make consumers whole if their agents misappropriate their personal information or fail to carry out their authorized instructions.

Third, the business has only the general business registration of the consumer's agent and some "authorization" of uncertain or inconsistent format to go by when the agent presents a request on behalf of the consumer. This leaves the business open to uncertain risks in denying what could be a legitimate request, taking a lengthy amount of time to validate the identity of the agent or providing access to a consumer's personal information to an unauthorized third party.

The Attorney General should take this opportunity to impose at least the following requirements on any person who intends to make opt-out, access, deletion or any other requests on behalf of any consumer under the CCPA: (1) require registration or licensure with the Attorney General or other appropriate regulatory agency, which should include posting a bond and completing a background check with absence of any criminal convictions; (2) provide a specific authorization form by

³ "Phishing alert: GDPR-themed scam wants you to hand over passwords, credit card details." ZDNet (May 3, 2018)(<https://www.zdnet.com/article/phishing-alert-gdpr-themed-scam-wants-you-to-hand-over-passwords-credit-card-details/>).

⁴ <https://www.sos.ca.gov/business-programs/business-entities/faqs/>

which a consumer may authorize an agent to act on its behalf under the CCPA, which includes listing the registration or license number issued by the Attorney General or other regulatory body for the agent; (3) provide a safe harbor for businesses relying on the approved authorization form; (4) provide additional rules around agents acting on behalf of consumers, including (if the identified sections of the CCPA are found in conflict) prohibiting agents from making personal information access or deletion requests; and (5) provide penalties for violations of the rules.

c. Flexibility for high request periods.

Under normal circumstances, responding to a consumer within 45 days of receiving a verifiable (or verified) request could be a challenge. As was the case immediately following the effective date of the GDPR, it is highly likely businesses will see a deluge of requests, which will test a business's resources, including potentially new processes and systems for complying with the CCPA.⁵ While the CCPA has provided some additional timeframes for "reasonably necessary" and "necessary" extensions, the Attorney General should consider all extensions as "necessary" during at least the first six months following the effective date of the Act without businesses having to proactively notify consumers of those extended timeframes. Alternatively or in addition to the automatic extension, the regulations should permit businesses to disclose upfront (without having to provide individual notices of extension to each requesting consumer or authorized agent) a general notice that delayed responses may be "reasonably necessary" or "necessary" and take additional time, as identified in the CCPA, in times of high demand.

Further Amendments to the CCPA

As ARDA submits these comments, there are pending amendments to the CCPA.⁶ In particular, these amendments would remove a 30-day grace period for curing certain alleged breaches of the CCPA, diminish the ability to seek guidance from the Attorney General on how to comply with the CCPA, and expand consumers' private right of action to all other violations of the CCPA. These amendments do not clarify the terms we or others have identified, but impose greater burdens on businesses attempting to put measures in place to comply with the original legislation. ARDA strongly encourages the Legislature and the Attorney General to instead provide clarity to the already numerous protections the CCPA offers in the best interests of all potentially impacted stakeholders prior to making additional statutory changes.

ARDA again thanks the Attorney General for the opportunity to provide comments through this important rulemaking process.

Respectfully,



Chris Stewart
Vice President, State Affairs
American Resort Development Association

⁵ "Companies under strain from GDPR requests." Financial Times (July 1, 2018) (<https://www.ft.com/content/31d9286a-7bac-11e8-8e67-1e1a0846c475>).

⁶ SB 561 introduced February 22, 2019.

1201 15th Street, NW, Suite 400, Washington, DC 20005 . [REDACTED] . fax 202-289-8544 . www.arda.org
STATE GOVERNMENT AFFAIRS OFFICE
225 E Robinson Street • Suite 545 • Orlando, FL 32801 • [REDACTED] • fax 407.872-0771

Message

From: Jarrell Cook [REDACTED]
Sent: 3/8/2019 6:28:40 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Attachments: CCPA Comments .pdf

Hello,

Attached please find CMTA's comments regarding the pre-rulemaking for select provisions of the CCPA. We appreciate the opportunity and your review.

Please contact us if you have any questions or concerns.



Jarrell Cook

Policy Director

Government Relations

California Manufacturers

& Technology Association

1121 L Street, Suite 700

Sacramento, CA 95814



| www.cmta.net



March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

Re: Pre-Rulemaking Comments on California Consumer Privacy Act Regulations

Dear Attorney General Becerra:

The California Manufacturers & Technology Association (CMTA) is writing to draw your attention to ongoing concerns with the California Consumer Privacy Act (CCPA) that may be addressed through effective rules, guidance, and procedures.

CMTA represents 400 businesses from the entire manufacturing spectrum – including large, medium, and small manufacturers – generating more than \$230 billion every year and employing more than 1.2 million Californians. A critical area for growth in the manufacturing industry is in the creation and use of connected devices – the network of physical objects embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data commonly described as 'The Internet of Things.'

The Internet of Things is poised to radically transform society. Rapid growth in agriculture, urban development, medicine, transportation, telecommunications, and other sectors will all depend on thoughtful policy that balances privacy concerns with rules that still enable this emerging technology to function. As you promulgate regulations that provide guidance and procedures to comply with consumers' exercise of their rights under the CCPA, the following is a non-exhaustive list of key areas that would provide clarity to manufacturers, while still aligning the operational needs of connected devices with the purpose of the act:

I. Device to Device Communication

Interoperability is at the heart of what makes connected devices valuable; an array of devices with advanced functions that can seamlessly interact is what the Internet of Things promises. For many connected devices, that interoperability is achieved through the automated transmission and receipt of unique device identifiers. Manufacturers have built the both networking and security infrastructure necessary for these devices to function properly around devices possessing strong, unique, and immutable identifiers.

Unique persistent identifiers alone are themselves newly considered personal information under the CCPA. This raises concerns regarding device-to-device communications. In the ordinary course of operation, a connected device may be continuously and persistently transmitting and receiving device IDs. For example, an autonomous vehicle driving through a city may innocuously interact with countless consumer devices, smart traffic lights, and other safety equipment to successfully navigate to its endpoint.

Under this new framework, it is unclear whether a manufacturer of a connected device, 'A' that communicates with second connected, 'B' has any obligations to the owner of Device B if Device A receives the device ID of B.

If the receipt of such an ID is considered “collection” for the purposes of the statute, then it would at least require individualized notice for each device, even where there is no direct relationship to the consumer, which is impractical-to-impossible.

Recommendation: Clarify that the automated transmission and receipt of unique identifiers, such as device IDs, between connected devices that is necessary for their operation or function is not considered a “collection” under the CCPA.

II. The Definition of Household

The CCPA further expands the definition of personal information to include “household” data. But it does not clarify what “household” means. An expansive interpretation of the term “household” mean data generated by any individual in the home – including data generated by transient occupants (roommates, guests, etc.). This would create an unworkable standard.

Connected devices, such as appliances or shared electronics, can generate data for any number of persons that are in a household. Guests in the home for only a few minutes that use a smart refrigerator, for example, would be able to create a set of obligations for manufacturers under this reading of the CCPA. Further, the resident would be able to obligate the manufacturer to provide information about his or her guests or roommates generated from their use of these devices.

An even more complicated scenario occurs when ownership or occupancy of a home changes, but the smart device is attached to the home. Does the current owner or occupant now possess a right to all the data a manufacturer has about the household, including the data generated by the former resident? For many devices, the manufacturer has no knowledge or control over a device that would permit them to limit their obligation to or liability from consumers.

Recommendation: Clarify that data generated by a “household” only applies to that generated by a device intended to collect data of the household as a single entity – such as smart meters, thermostats, etc. – and not the data of individuals within.

III. The Submission and Verification of a Consumer Request

The CCPA requires that businesses take steps to verify a consumer’s identity before complying with a request to disclose or delete that consumer’s data. Many connected devices are used by multiple consumers over the course of their life; smart appliances and smart cars, for example, transfer possession without any notification to the manufacturer from either the old or new owner. This creates significantly burdensome compliance issues for manufacturers.

Recommendation: The CCPA allows for manufacturers to comply with requests submitted through a “password protected account.” First, recommend interpreting this passage as intending to require the creation of a secure, user-created account, and, thus, permit any legitimate means of authentication. Passwords are not necessarily the most secure method of security and manufacturers should not be required to use regressive technology where more secure standards exist.

Second, in the absence of a protected account, the procedure for compliance with the duty to verify a consumer’s request should be through registration of the device with the manufacturer (along with the creation of process to re-register the device to a new owner in the event of a sale or transfer). The burden should be on the consumer to take the proactive step to create an account or register with a manufacturer in order to exercise the rights they have over their data. Manufacturers would only be obligated to respond to submissions for information and requests for delete from registered users. This would significantly reduce the possibility of erroneous or fraudulently induced disclosures. And the burden is appropriately balanced – manufacturers should not be expected to hunt down consumers to verify their identity.

In addition to these device-specific issues, manufacturers share the workability concerns facing every business operating in California and encourage you to consider rules that would address those general issues as well.

Sincerely,

A handwritten signature in black ink, appearing to read "Jarrell Cook". The signature is fluid and cursive, with the first name "Jarrell" written in a larger, more prominent script than the last name "Cook".

Jarrell Cook
Policy Director, Government Relations
California Manufacturers & Technology Association



Message

From: Hartwell, Robert L. [REDACTED]
Sent: 3/8/2019 2:11:17 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Attachments: Trade Association Comments to California AG.pdf

Please find attached comments on the CCPA on behalf of the American Association of Advertising Agencies (4A's), American Advertising Federation ("AAF"), Association of National Advertisers ("ANA"), Interactive Advertising Bureau ("IAB"), and Network Advertising Initiative ("NAI").

Thank you.

Rob L. Hartwell, Esq. | Venable LLP

[REDACTED]
600 Massachusetts Avenue, NW, Washington, DC 20001

[REDACTED] www.Venable.com

This electronic mail transmission may contain confidential or privileged information. If you believe you have received this message in error, please notify the sender by reply transmission and delete the message without copying or disclosing it.



March 8, 2019

The Honorable Xavier Becerra
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Submitted via privacyregulations@doj.ca.gov

RE: California Consumer Privacy Act Regulation

Dear Attorney General Becerra:

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies in California and across the country, from small businesses, to household brands, across every segment of the advertising industry, including a significant number of California businesses. Our combined membership is responsible for more than 85 percent of the U.S. advertising spend. Locally, our members help generate some \$767.7 billion dollars for the California economy and support more than 2 million jobs in the state.

Consumer trust is vital to our members' ability to successfully operate in the marketplace, and they take that responsibility seriously. A prime example of this commitment is through the Digital Advertising Alliance ("DAA") YourAdChoices Program. We helped create the DAA to establish a self-regulatory code for all companies that collect or use data for interest-based advertising, based on practices recommended by the Federal Trade Commission ("FTC") in its 2009 report on online behavioral advertising.¹ The effectiveness of the Self-Regulatory Program also has been recognized by the United States government. At a 2012 White House event, Obama Administration officials including the then-FTC Chairman and Secretary of Commerce publicly praised the DAA's cross-industry initiative. The DAA approach has also garnered kudos from the leadership at the FTC under recent administrations for the program's pioneering privacy work.²

We agree that privacy deserves strong meaningful protections in the marketplace, while also allowing for innovative new uses of data to continue to grow the data-driven economy. We appreciate the opportunity to comment on the California Consumer Privacy Act ("CCPA" or "the Act") and its implementation, and to work with the Attorney General ("AG") on these matters. While our members support the CCPA's intent to provide consumers privacy protections, consumers and businesses would benefit from clarification concerning certain provisions of the

¹ DAA, *Self-Regulatory Principles for Online Behavioral Advertising* (Jul. 2009); FTC, *FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising* (Feb. 2009).

² The White House recognized the Self-Regulatory Program as "an example of the value of industry leadership as a critical part of privacy protection going forward." The DAA also garnered kudos from then-FTC Commissioner Maureen Ohlhausen who stated that the DAA "is one of the great success stories in the [privacy] space." In its cross-device tracking report, the FTC staff also praised the DAA for having "taken steps to keep up with evolving technologies and provide important guidance to [its] members and the public. [Its] work has improved the level of consumer protection in the marketplace."



Act. Below we explain the importance of data to consumers and the broader economy. We then suggest and discuss five key areas within the CCPA on which the AG should focus his attention during this rulemaking process. We note that these are just a few of the important aspects of the CCPA, but that they are not the totality of the issues we and our members wish to discuss. Additional comments will be filed by some of the individual trade associations that will focus on some of those other important concerns.

I. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth

Today, the U.S. economy is increasingly fueled by the free flow of data. One driving force in this ecosystem is data-driven advertising. Advertising has helped power the growth of the Internet for decades by delivering innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet's largest players.

As a result of this advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.³ Calculating against those figures, the interactive marketing industry contributed \$1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.⁴

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to create their own platforms to reach millions of other Internet users. Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored experience. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. Indeed, as the FTC noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.⁵ It is in this spirit—

³ John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017) <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>.

⁴ *Id.*

⁵ Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018) https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.



preserving the ad supported digital and offline media marketplace while helping to design privacy safeguards—that we provide these comments.

II. Improve Consumer Privacy by Approving Granular Choice, Clarifying Definitions, and Updating Required Language

This section discusses different avenues through which the AG can help businesses to more effectively and efficiently provide consumers with their rights under the CCPA, including through the use of well-regarded tools already in the marketplace.

a. Grant Consumers the Ability to Delete or Opt Out of the Use of Some and/or All of Their Personal Information

The CCPA should allow consumers to express their rights to delete or opt out for a subset of data at their election if a company is capable of providing and elects to offer such choices to consumers. This option would provide full control over covered personal information, and help ensure that consumers maximize their rights. We suggest that the AG issue a rule that allows, but does not require, businesses to provide consumers with this type of flexible choice options regarding deletion or opt-out requests.

The CCPA creates the right for consumers to opt out all of their personal information from sale or delete all their data. The law does not, however, recognize that a consumer may want more selective choices based on how they interact with a particular business that is able to offer those choices. The CCPA's blanket choice limits consumers from fully expressing their preferences, could lead to requests that do not accurately reflect consumer wishes, and create confusion and frustration.


To solve this issue we ask the AG to clarify that consumers may be provided the choice of subsets of data that they want to effectuate their rights against, while still having the option to apply their rights against all covered data if a business is able and elects to offer various levels of choice. This will provide consumers with more valuable and personalized choices. The AG can issue such a rule under the power to promulgate rules “[t]o facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information.” The AG can also clarify the deletion rights under the authority to issue rules that “further the purposes of [the] title.” Providing flexible choice options to consumers promotes their privacy decisions and empowers them to better control how their data is used.

b. Enable Existing Privacy Controls to Continue and Provide Flexibility for Effectuating Rights Requests in a Manner that Provides for Consumer Privacy

The AG should clarify the CCPA does not require businesses to identify pseudonymized data. Pseudonymized data does not typically contain identifiable information (e.g., names and email addresses). A consumer's request to effectuate their rights will likely be based on this type of identifiable information, data that businesses will not have in their pseudonymized data sets. If the AG does not clarify that such data does not need to be identified, businesses may feel



compelled to link the identifiable and non-identifiable pseudonymized data, which lowers consumer privacy protections in the marketplace. Such a reading is the antithesis of the CCPA's goals, and may also render ineffective the CCPA section that states: "This title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information."⁶

We ask the AG for a clarification to the law that makes clear that businesses should not identify non-identifiable pseudonymized data in order to complete a consumer request. The AG should also recognize that businesses are able to use flexible tools to answer consumer requests while maintaining existing privacy protections. Such a clarification is needed to avoid a poor result where pseudonymous data, to the extent it is considered to be personal information under the Act, is made identifiable if there is no ability to use a flexible approach. One potential tool that a business can use to effectuate consumer rights if the AG allows for flexible tools is the DAA YourAdChoices Icon  and consumer choice program for the data the program covers. The AG can issue rules on these topics under the powers to "[e]stablish... rules and procedures... [f]or the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information," as well as based on the authority to promulgate rules that further the purpose of the CCPA.⁷ By looking to tools that consumers know and businesses adopt in the marketplace, and allowing companies the chance to use a variety of opt-out tools, as opposed to one tool, the AG can prevent the potential identification of pseudonymized data covered by the Act, and further the Act's purposes of improving privacy controls for consumers.⁸

c. Clarify Requirements for the Language of the "Do Not Sell My Data" Link

We ask the AG to provide clarification and flexibility with regard to the required language in the "Do Not Sell My Data" link required under the Act. The CCPA requires businesses to "provide a clear and conspicuous link on the business's Internet homepage, titled 'Do Not Sell My Personal Information,'" to a page that enables a consumer to opt-out of the sale of the consumer's personal information.⁹ However, consumers have a different understanding of the term "sell" than the idiosyncratic definition in the CCPA.¹⁰ The delta between consumer

⁶ Cal. Civ. Code § 1798.145(i).

⁷ Cal. Civ. Code § 1798.185(a)(4)(C); §§ 1798.185(a), (b).

⁸ Consumer awareness and understanding of the DAA program continues to increase, and a 2016 study showed more than three in five consumers (61 percent) recognized and understood what the YourAdChoices Icon represents. DAA, *Consumers' recognition of the AdChoices Icon -- and understanding of how it gives choice for ads based on their interests -- continues to rise* (Sep. 29, 2016) <https://digitaladvertisingalliance.org/blog/icon-you-see-yeah-you-know-me-0>.

⁹ Cal. Civ. Code § 1798.135(a)(1).

¹⁰ Cal. Civ. Code § 1798.140(t)(1) (defining "sell" as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or third party for monetary or other valuable consideration").



understanding and the CCPA's required language could cause consumers to make requests that they do not understand, and ultimately lose access to goods and services they desire.

The AG should issue a rule stating that businesses do not need to use the term “sell” in the opt-out links mandated by the CCPA. Instead, the AG should allow for the use of different language that more accurately describes what the consumer will be able to do following the link. The AG has authority to issue these rules pursuant to the ability to “[e]stablish... rules and procedures... [f]or the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.”¹¹ More accurately presenting consumers with their rights will increase their awareness of those rights and promote their use.

III. Clarify Required Notices & Information for Consumers, including Financial Incentive Offerings

This section discusses regulatory approaches that the AG could adopt in order for consumers to receive all notices and information they are required to receive, and to enable businesses to effectively provide consumers with that information.

a. Protect Customer Loyalty Programs

We ask the AG to issue a rule that will protect customer loyalty programs that consumers want and enjoy. The CCPA contains prohibitions against price and service discrimination against consumers that exercise their CCPA rights. The Act creates these prohibitions, however, through imprecise language that could prohibit traditional loyalty discount programs.¹² The CCPA is also contradictory on this topic. One section of the Act states that loyalty programs must be “reasonably related” to the value provided to the consumer by their data, but another section provides that these programs must be “directly related” to the value provided to the consumer by their data.¹³ This confusion leaves businesses unable to determine which standard applies, and unable to determine how to provide discounts and programs to consumers.

Consumers that request deletion or opt-out from data practices that are required in order for them to participate in a loyalty program will no longer be able to participate fully. As a result, such consumers will by definition be treated differently from consumers that participate in a loyalty program. This differential treatment could unintentionally violate the ambiguous wording in the Act, which only allows these differences when the activity is “reasonably related”

¹¹ Cal. Civ. Code § 1798.185(a)(4)(C).

¹² The CCPA states: “A business shall not discriminate against a consumer because the consumer exercised any of the consumer’s rights under this title, including... by: ... [c]harging different prices or rates for goods or services, including through the use of discounts or other benefits imposing penalties.... Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer’s data.” Cal. Civ. Code §§ 1798.125(a)(1)-(2).

¹³ Compare Cal. Civ. Code § 1798.125(a)(2) (“reasonably related”) with Cal. Civ. Code § 1798.125(b)(1) (“directly related”).



or “directly related” to the value provided to the consumer. Therefore, in an abundance of caution, businesses may choose to discontinue these programs in California.

We therefore ask the AG to permit a business to offer loyalty-based discount programs that consumers’ value and expect, without the program violating the CCPA. Specifically, the terms “reasonably related” and “directly related” to the value provided to consumers by their data should be interpreted to include the collection, use, and sharing of any data that is needed to provide a loyalty discount program.¹⁴

b. Ensure that the Act does Not Require Customized Privacy Policies

We urge the AG to clarify that a business is not required to provide consumers with a list of the specific pieces of information it collects about a specific consumer in the privacy policy posted on the business’s website. The CCPA requires a business’ privacy policy to disclose to a consumer the “specific pieces of personal information the business has collected about that consumer.”¹⁵ However, this section of the law focuses on the consumer’s right of access, which could be interpreted as applying only to that right. The Act currently creates uncertainty because it could also be interpreted to require each privacy policy to list such data for the consumer currently reading the policy. Such a requirement would be impossible to comply with from a technical standpoint, especially for in-store disclosures. It also creates a higher likelihood of inadvertent disclosures of a specific consumer’s information to the wrong recipients. This would ultimately lower the level of consumer privacy, not enhance it.¹⁶

We suggest that the AG clarify that businesses need only provide specific pieces of information to effectuate a consumer access request, not through more generally applicable privacy policies, to comply with the CCPA. The AG can issue this rule under the authority to “[e]stablish rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer’s...ability to obtain information...”¹⁷ Explaining where and how

¹⁴ The AG has authority to issue regulations to “further the purposes of [the] title.” Cal. Civ. Code §§ 1798.185(a), (b). The clarification furthers the purposes of the title because it harmonizes the Act to be internally consistent. Additionally, this clarification will allow loyalty programs to continue for consumers that wish to participate in them.

¹⁵ Cal. Civ. Code § 1798.110(c) (“A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130: (5) The specific pieces of personal information the business has collected about that consumer.”); Cal. Civ. Code § 1798.130(a)(5)(B) (“In order to comply with [Section]... 1798.110... a business shall, in a form that is reasonably accessible to consumers... [d]isclose... in its online privacy policy... [f]or purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.”).

¹⁶ Furthermore, in a survey of 1,039 California adults conducted by the DAA via SurveyMonkey from January 29-30, 2019, over 87% of individuals surveyed indicated they would prefer to receive generic information from a business based on broad interest and demographic categories rather than detailed information based on the individual’s specific activities, identity, and interests. DAA, *California Perspectives on Privacy Issues* (Jan. 2019), available at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/DAA_CA_privacy_survey_January_2019.pdf.

¹⁷ Cal. Civ. Code § 1798.185(a)(7).



“specific pieces of information” should be delivered to consumers facilitates the consumer’s ability to exercise rights under the law, and also drives proper implementation of the CCPA by businesses without subtracting from the Act’s overall purpose.

c. Clarify the Requirements for “Explicit Notice”

The Act prohibits a business from selling consumer personal information that it did not receive directly from the consumer, unless the consumer has received “explicit notice” and is provided an opportunity to exercise the right to opt-out of that sale.¹⁸ In general, third parties do not have a direct relationship with the consumer, and therefore have no way to effectively provide this notice. Therefore, this requirement could shut off the ability of third parties to participate in the digital marketing ecosystem, undermining competition in the marketplace and lowering the availability of goods and services to consumers. We urge the AG to state that a third party may rely on contractual assurances from their partners with a consumer touchpoint to provide the CCPA-required “explicit notice” as one method of meeting these requirements.

To avoid the unintended consequence of stopping third parties from participation in the market, we urge the AG to promulgate a rule that states that businesses can rely on contractual assurances to satisfy the CCPA’s “explicit notice” requirement. This would involve a business that provides data to a third party representing, and the third party relying on those representations, that the consumer was provided “explicit notice” at the time of collection. The AG may issue this rule pursuant to the ability to issue rules to “facilitate a consumer’s or the consumer’s authorized agent’s ability to obtain information pursuant to Section 1798.130.”¹⁹ This rule will allow the direct consumer touchpoint to provide consumers with the CCPA’s required notices, and allow competition and consumer benefits to continue to flow from third-party data use.

IV. Clarify that the CCPA Does Not Apply to Data Collected Prior to January 1, 2020

We urge the AG to interpret the CCPA’s coverage to begin on its enforcement date of January 1, 2020, and that data collected prior to that date is not covered by the Act. The CCPA requires businesses to provide information to consumers about data practices from “the 12-month period preceding the business’s receipt of the verifiable consumer request...”²⁰ However, it does not state whether data collected prior to the effective date must be included in the initial 12-month period starting on January 1, 2020. Should such data be included in the required data set, companies are effectively under a 12-month retention period with no direct statutory requirement to do so or guidance for how to follow the law.

The AG should clarify this point to make clear that the CCPA does not create a data retention requirement for companies. The AG may regulate this issue based on the authority to

¹⁸ Cal. Civ. Code § 1798.115(d).

¹⁹ Cal. Civ. Code § 1798.185(a)(7).

²⁰ Cal. Civ. Code § 1798.130(a)(2).



adopt rules to “further the purposes of [the] title.”²¹ This clarification promotes the purpose of the CCPA as it allows companies to continue to delete and otherwise dispose of information in a privacy-responsible manner.

V. Provide a Flexible Framework for Verifying and Responding to Consumer Requests

The AG should issue a rule that makes clear that non-personally identifiable pseudonymous data is not subject to the access, deletion, or opt out rights under the law to protect consumer privacy, and provide that businesses can use commercially reasonable methods to verify consumer requests. The CCPA uses the term “verifiable consumer request” as the trigger for businesses to act on and effectuate the rights consumers maintain under the Act. However, the CCPA fails to provide businesses with direction for how to verify a consumer’s request, or how to verify that a request by a third party is authorized by the consumer in question. This is because information businesses maintain for a variety of purposes is pseudonymized and not identifiable.

Digital advertisers generally use pseudonymized data tied to unique identifiers. This pseudonymized data is not tied to identifying information. As a result, those companies will have difficulty verifying a consumer’s request, and matching data that relates the consumer to it. Under the CCPA it will be very difficult if a business cannot ask for more information, or it will require pseudonymized data to be made identifiable and therefore deprecate consumer privacy.²² This problem is also present when companies need to verify third parties submitting requests on behalf of unknown consumers.²³

We suggest that the AG clarify that pseudonymous data is not subject to a consumer access, deletion, or opt out request under the law so that such data can remain in a non-identifiable form. We also ask for a rule that makes clear that a business can use commercially reasonable methods to verify a consumer request, and that if such methods fail the request is not verifiable. The AG can issue these clarifying rules under the authority to establish “rules and procedures... to facilitate a consumer’s... ability to obtain information pursuant to Section 1798.130....”²⁴ The AG can also put forth this interpretation through the authority found in the definition of a “verifiable consumer request.”²⁵

²¹ Cal. Civ. Code §§ 1798.185(a), (b).

²² The only approved method under the CCPA for confirming consumer identities assumes the consumer maintains an account with the entity to which the request is directed. Cal. Civ. Code § 1798.185(a)(7).

²³ Cal. Civ. Code §§ 1798.135(a)(1), (c), 140(y).

²⁴ Cal. Civ. Code § 1798.185(a)(7).

²⁵ Cal. Civ. Code § 1798.140(y) (A verifiable consumer request is “a request that...the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information.”).



VI. Clarify the Categories of Personal Information and Other Definitions in the CCPA

This section discusses various concerns and inconsistencies within the CCPA's definitions that we suggest the AG clarify in order to ensure that businesses can comply with the law, and consumers receive the full benefit of the law's newly-granted rights.

a. Clarify the Definition of “Publicly Available”

The definition of “publicly available”²⁶ in the CCPA is vague and problematic. Specifically, it states that “[i]nformation is not ‘publicly available’ if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.”²⁷ This definition is problematic because many government reports and data sets are publicly released without informing the public about the original purpose of the dataset. This creates ambiguity for businesses regarding how to treat information that is publicly available. We ask the AG to issue a rule to make clear that businesses may use data made public by the government.

For example, U.S. census data is often used for a variety of valid and socially valuable purposes by the private sector, purposes that go beyond the Constitutional mandate to count the number of individuals living in the United States. To limit the use of publicly available information solely for the purposes for which the government collected the information for is to rewrite the traditional understanding of how the private sector can appropriately utilize public data.

The definition of “publicly available” information should be interpreted to allow for the free use of data provided by the government to the public, unless there are other governmental, legal, or regulatory limits placed on a specific dataset. The AG is able to interpret the definition in this manner pursuant to the authority to adopt rules that further the purposes of the CCPA.²⁸ Clarifying the fact that publicly available information includes information made public by the government for any purpose, unless other laws directly prohibit a use case, furthers the intent of the CCPA by assuaging consumer confusion and streamlining responses to consumer requests.

b. Clarify the Concept of “Household” in the Definition of “Personal Information”

The CCPA creates the ability to access personal information about a consumer,²⁹ however it includes within its definition of “personal information” information that relates to the “household.”³⁰ The Act does not contain a corresponding definition of “household” to make

²⁶ Cal. Civ. Code § 1798.140(o)(2).

²⁷ *Id.*

²⁸ Cal. Civ. Code §§ 1798.185(a), (b).

²⁹ Consumers have “the right to request that a business that collects personal information about the consumer disclose to the consumer...the categories [and]... specific pieces of personal information it has collected about that consumer.” Cal. Civ. Code § 1798.110(a).

³⁰ Cal. Civ. Code § 140(o)(1).



clear what constitutes a household, which could lead to inadvertent disclosures of personal information to unauthorized individuals. This means that a member of a household (regardless of whether he or she is merely a roommate) or a family member (regardless of whether he or she is an abusive spouse), could potentially access personal information about another member of the household.³¹ This contravenes the stated purpose of the law, to protect individuals' privacy.

We ask the AG to clarify through a rule that the term "household" relates to information about the requesting consumer, not information about others in the household unless the other individuals provided authorization to the requesting consumer to access the information. The AG has authority to issue this rule under the authority to "[e]stablish rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's...ability to obtain information..."³² This would allow for completion of consumer requests in a more privacy-protective manner.

c. Clarify the Definition of "Deidentified" and "Aggregate Consumer Information"

We suggest that the AG should promulgate a rule that clarifies that "deidentified information" and "aggregate consumer information" are not included in the definition of "personal information." The unclear language and structure in the Act could lead to interpretations that create unintended consequences by bringing deidentified information and aggregate consumer information within the scope of the CCPA.

The CCPA defines personal information as "information that... is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."³³ The law seems to exempt deidentified and aggregate consumer information from this definition when it defines them separately, but the law does not explicitly exempt them from it.³⁴ This could lead one to wrongly interpret the Act to mean that deidentified information or aggregate information are also personal information.

The CCPA does create an exception for deidentified and aggregate consumer information. That exception states, "The obligations imposed on businesses by this title shall not restrict a business's ability to... (5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information."³⁵ However, that exception is vague and lacks the specific statement that deidentified and aggregate consumer information is not covered.

The unintentional result of these two issues could lead to consumer exercising rights to request this type of data, even though those rights attach to personal information under the CCPA. To avoid this result, we suggest that the AG clarify through a rule that "deidentified" information and "aggregate consumer information," are not "personal information" and are

³¹ Cal. Civ. Code § 1798.110.

³² Cal. Civ. Code § 1798.185(a)(7).

³³ Cal. Civ. Code § 1798.140(o)(1).

³⁴ Cal. Civ. Code § 1798.140(h); 1798.140(a).

³⁵ Cal. Civ. Code § 1798.145(a)(5).



outside the scope of the rights related to it. The AG has authority to issue this rule under the ability to issue regulations to “further the purposes of [the CCPA].”³⁶ This rule ensures that the CCPA remains focused on protecting consumer privacy and personal information, and that it does not unintentionally impact activity using other types of information.

* * *

We appreciate the opportunity to provide comments on implementation of the CCPA and remain ready to work with you to improve the CCPA’s privacy protections.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
[REDACTED]

Christopher Oswald
Senior Vice President, Government
Relations
Association of National Advertisers
[REDACTED]

Clark Rector
Executive Vice President-Government
Affairs
American Advertising Federation
[REDACTED]

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
[REDACTED]

Alison Pepper
Senior Vice President
American Association of Advertising
Agencies, 4A's
[REDACTED]

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
[REDACTED]

cc: Michael Signorelli, Venable LLP
Rob Hartwell, Venable LLP

³⁶ Cal. Civ. Code §§ 1798.185(a), (b).

Message

From: Douglas Peddicord [REDACTED]
Sent: 3/8/2019 1:13:32 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Karen Noonan [REDACTED]
Subject: Comments on CCPA
Attachments: ACRO CCPA.docx

Attached are comments from the Association of Clinical Research Organizations (ACRO).

Thank you for the opportunity to submit. Please contact me if you have any questions.

Douglas Peddicord, Ph.D.

Executive Director

E [REDACTED]

ACRO

Association of Clinical Research Organizations

601 New Jersey Ave, NW

Suite 350

Washington, DC 20001



www.acrohealth.org

March 8, 2019

California Department of Justice
300 S. Spring Street
Los Angeles, CA 90013
Attn: Privacy Regulations Coordinator

Re: California Consumer Privacy Act
Civ. TITLE 1.81.5 [1798.100-1798.199]

Introduction

The Association of Clinical Research Organizations (ACRO) represents the world's leading clinical research and technology organizations. Our members provide a wide range of specialized services across the entire spectrum of development for new drugs, biologics and medical devices, from pre-clinical, proof of concept and first-in-man studies through post-approval and pharmacovigilance research. In 2018, ACRO member companies managed or otherwise supported a majority of all FDA-regulated clinical investigations worldwide.

With more than 130,000 employees engaged in research activities in every U.S. state and 114 countries around the world, the member companies of ACRO advance clinical outsourcing to improve the quality, efficiency and safety of biomedical research.

In addition to their work in conducting and facilitating clinical trials, the companies of ACRO regularly use limited data sets and de-identified data (as defined by HIPAA) in the course of post-approval work, including safety surveillance and epidemiology studies, patient registry and health outcomes analyses, comparative effectiveness research (CER), and other information-based research. ACRO members also deploy data analytics tools that are derived from de-identified data to support biopharmaceutical commercialization, pricing and market access decisions, and consult to biopharmaceutical companies, payers and providers in regard to value-based contracts.

ACRO is concerned about the potential of the California Consumer Privacy Act (CCPA) to negatively impact the crucial biomedical and health data research that drives improvements in medical care and the health of individuals and populations. We will focus our comments on two issues: 1) the exemption for clinical trial data in section 1798.145, and 2) the definition of "deidentified" in section 1798.140.

The Exemption For Clinical Trial Data Is Too Narrow

Section 1798.145(a)(1)(C) exempts from the requirements of the CCPA information that is collected as part of a clinical trial that is subject to the Common Rule, Good Clinical Practice guidelines (ICH-GCP) or the human subjects protection requirements of the US FDA. The problem is that clinical

trials – which, by definition involve interventional investigation of drugs, biologics, devices and procedures – constitute only a small subset of the biomedical and health data research that is crucial to medical progress. As noted in the list above of research activities undertaken by ACRO member companies, information from many sources other than clinical trials is used in FDA-regulated research. Information from electronic health records fuels comparative effectiveness research and health outcomes studies; adverse event reports and patient-reported outcomes facilitate ongoing evaluation of approved drugs, biologics and devices; information from patient registries is utilized for hypothesis generation, clinical trial design and patient-finding; limited data sets drive epidemiologic and safety studies; monitoring of individual patient information may be required by the FDA as a part of a REMS (risk evaluation and mitigation strategy) safety program; de-identified health information supports the development of the new data analytics that are essential to fulfilling the promise of “big data” in healthcare – the list could go on and on.

All of these studies are conducted in accordance with current federal law, and super-imposing the requirements of the CCPA could have a disastrous effect on the conduct of such research, not only in California, but in the nation as a whole.

ACRO believes that the intent of 1798.145(a)(1)(C) should be re-examined, and that the exemption of biomedical and health data research should be significantly broadened. At a minimum, we suggest that 1798.145(a)(1)(C) be extended as follows: “...or pursuant to human subject protection requirements of the United States Food and Drug Administration. **In addition, information that is individually identifiable health information, as defined at 45 CFR 160.103, and is used in research, as defined at 45 CFR 164.501.**”

The Definition Of Deidentified Conflicts With HIPAA And Will Have Significant Negative Effect

The HIPAA Privacy Rule distinguishes between the use of protected health information (PHI) which identifies an individual, and de-identified information for which “there is no reasonable basis to believe that the information can be used to identify an individual” [45 CFR 164.514 (a)].

HIPAA provides for “safe harbor” and “statistician” methods of de-identification, and since 2002 de-identified health data has facilitated important research while also protecting individual privacy. [Importantly, while successful re-identification attacks against a variety of data sets have been reported, the literature does not describe any successful re-identification of a data set de-identified to the standards established at 45 CFR 164.514 (a)-(c).]

By contrast to the firmly established definition of “de-identified” under federal law, the CCPA roots its definition of “deidentified” in safeguards and business processes aimed at reidentification. In other words, rather than considering the legitimate uses of de-identified data, the CCPA rests the very definition of deidentified on the prevention of reidentification. This approach conflicts not only with HIPAA, but with the GDPR (General Data Protection Regulation) and other privacy laws.

ACRO suggests that a straightforward ban on reidentification, perhaps with penalties for reidentification attempts, might more effectively protect individual privacy, without hobbling the use of de-identified data for important biomedical and health research.

We recommend that the CCPA definition of “deidentified” be harmonized with the definition of “de-identified” health data at 45 CFR 164.514 (a).

Conclusion

Representing companies whose lifeblood is the collection and analysis of health information to test the safety and efficacy of new drugs and new treatments for patients, ACRO thanks the Department of Justice for the opportunity to provide these comments on the California Consumer Privacy Act. We look forward to working with the Attorney General as regulations to implement the law are crafted.

Respectfully submitted,

Douglas Peddicord, Ph.D.
Executive Director

Message

From: Ann Waldo [REDACTED]
Sent: 3/8/2019 12:57:31 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Attachments: WLO Comments to CA AG re CCPA 3.8.2019.docx

My comments are attached.

Thank you,

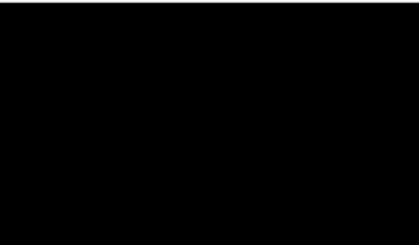
Ann Waldo

Ann B. Waldo, JD, CIPP

Waldo Law Offices, PLLC

601 New Jersey Avenue NW, Suite 350

Washington, DC 20001



This email was sent by an attorney and may contain confidential or privileged information. If you think you may have received this email in error, please email the sender or call 202-464-9357.



WALDO LAW OFFICES PLLC

1990 K Street, NW | Suite 401
Washington, DC 20006
Tel: [REDACTED]

March 8, 2019

California Department of Justice
300 S. Spring St.
Los Angeles, CA 90013
ATTN: Privacy Regulations Coordinator

Re: California Consumer Privacy Act

Dear Sir/Madame:

I appreciate the opportunity to submit comments regarding the California Consumer Privacy Act (CCPA). I'd like to express three concerns related to health care entities and biomedical research. From my perspective:

- (1) The exemption for HIPAA Business Associates in section 1798.145(c) needs to be tweaked;
- (2) The exemption for biomedical research is far too narrow to encompass the myriad types of research that are taking place currently -- and that need to take place in order to bring about medical advances; and
- (3) The definition of de-identification is so narrow that it would hamper important biomedical research involving de-identified data.

My background - I'm an attorney with a boutique law practice in Washington, DC focusing on HIPAA and digital health privacy. I've been practicing privacy law full-time for 15 years and part-time for more. In addition to focusing on my clients' needs, I have long been deeply committed to the public policy priorities of improving patients' rights to access and use their medical records, healthcare technology innovation, and medical advancements through science and research. My views about privacy, compliance, and appropriate, rational regulation have also been shaped by previous jobs as Chief Privacy Officer of a global technology company, Chief Privacy Officer of a global pharmaceutical company, and stints in infectious disease public policy, consumer protection, and e-commerce law. It's from this perspective that I'd like to voice my concerns about CCPA's potential effects on healthcare and medical progress.

- (1) The exemption for Business Associates in section 1798.145(c).

Section 1798.145(c)(1)(A) exempts from CCPA both Medical Information subject to the CMIA (MI) and Protected Health Information governed by HIPAA (PHI) collected by a HIPAA Covered Entity or Business Associate. *In other words, the scope of the exemption under subsection (A) applies only to the extent of the MI or PHI.* Under (A), if a Covered Entity or

Business Associate has patient data that is not PHI as a matter of law, it would be subject to the CCPA. However, in the case of Covered Entities only, a helpful additional exemption applies – subsection (B) provides that if a provider governed by the CMIA or a Covered Entity subject to HIPAA maintains patient information in the same manner as it maintains its MI or PHI, that additional non-PHI patient information is outside the CCPA. That is completely appropriate, for expecting a Covered Entity to adopt an entirely different regulatory compliance framework for what might be a sliver of patient data outside HIPAA, when they are treating such in accordance with HIPAA, would be brutally complex, unworkable, and expensive.

My concern is that subsection (B) does not extend to Business Associates. They need the exemption for patient information that they maintain in accordance with HIPAA for the exact reasons that Covered Entities do – it would be mind-bogglingly difficult and expensive to treat certain patient data (likely a very small fraction of all the patient data they hold) under an entirely different legal framework than other patient data. Actually, I think Business Associates need this exemption even more than Covered Entities do, for they frequently lack the ability to even know if the patient data they hold is or is not subject to HIPAA. Compliance with divergent regimes would thus not even be possible in many cases – and painfully and unnecessarily expensive in others.

Here's the reason the current law will be so exceptionally difficult for Business Associates: With regard to its patient data, a Covered Entity is almost always covered 100% by HIPAA or 100% outside HIPAA, for if a provider accepts insurance on even one patient, then *all* of its patient data becomes subject to HIPAA. So the useful and appropriate existing provision in subsection (B) that exempts Covered Entities that maintain patient data as though it were subject to HIPAA will rarely be triggered in the normal patient care context (although it could be useful with regard to some research data.) In contrast, it is extremely commonplace that Business Associates – even ones that provide services only to healthcare entities – maintain both PHI and non-PHI patient data on behalf of their provider customers.

For example, consider a Business Associate that is a large IT provider or cloud storage provider serving medical practices. Let's say 95% of its customers are garden-variety HIPAA Covered Entities providers, 2% are concierge providers that don't accept insurance and thus are outside HIPAA, and 3% are stand-alone clinical trial sites outside HIPAA. Of the 95% Covered Entities, 6% have made the HIPAA election to "hybridize," meaning that their non-PHI patient data *is not* inside HIPAA, while 94% of the 95% have not done so, meaning that their non-PHI patient data *is* inside HIPAA. The most conscientious of Business Associates in this situation cannot possibly know which of its customers' data is subject to HIPAA and which is not. The only rational compliance approach is to treat all of customers' data as subject to HIPAA.

This is not theoretical. Personally, I've helped Business Associates implement exactly this approach – they deliberately and thoughtfully define the expand the scope of their HIPAA policies and procedures, training, Risk Analyses, Compliance Gap Assessments, breach response plans, etc. to cover all of their customers' data, not just the subset (usually overwhelmingly large) that is PHI. That's the only workable approach for the company, which simply couldn't know about the legal status of each customer, and wouldn't want to implement divergent internal systems even if they could do so. It's also good for protecting patients' privacy by casting the net of safeguards a bit wider than what the law would actually require.

I could elaborate further on the practical problems and considerable wasteful expense that would be imposed by the current-law approach of not including Business Associations in the subsection (B) exemption, but I'd like to simply propose a remedy – I'd recommend changing section 1798.145(c)(1)(B) as follows:

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity **or business associate** governed by [HIPAA], to the extent that the provider or covered entity **or business associate** maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

On a related note, some commentators have expressed concern that “patient information” in the above sentence is undefined. That’s a fair point. I’d thus suggest that clarity and compliance would be advanced if “patient information” were tied to the longstanding and well-understood definition of “individually identifiable health information” under HIPAA. (PHI is a subset of “individually identifiable health information” – see the definitions in 45 CFR 164.103.)

Accordingly, I’d recommend adding the following to the end of the paragraph above:

For purposes of this section, “patient information” means “individually identifiable health information,” as defined by 45 CFR 160.103.

(2) The exemption for clinical trial data in section 1798.145(a)(1)(C).

Section 1798.145(a)(1)(C) exempts information that is collected as part of a clinical trial and is subject to the federal Common Rule, Good Clinical Practices (GCP) guidelines, or FDA human subject protections. That is regrettably narrow. Some clinical trials take place that are not subject to any of the three regulatory regimens cited (Common Rule, GCP, or FDA). For example, a surgeon in private practice that doesn’t receive any federal funding might responsibly and carefully undertake a trial to test the efficacy of a modifying a particular surgical technique; that would not be subject to any of those three regulations.¹

Of far greater significance and magnitude, though, is that this exemption fails to include the vast array of biomedical research that does not involve clinical trials at all. Massive research is done involving healthcare data - without any clinical interventions at all. Examples are too numerous to list – observational studies, comparative effectiveness studies (conducted both by governments

¹¹¹ The fact that some clinical trials are conducted entirely outside the purview of federal regulation is not without controversy. If the California legislature believes, as some ethicists do, that such private clinical trials not regulated by the Common Rule, GCP, or FDA merit additional scrutiny and control, and any existing California-specific regulation of such is inadequate, then the legislature could consider additional state regulation of private research. The focus should be on protecting the research-related rights and interests of the trial participants, considering matters like external ethical review of the trial protocol and documents, informed consent, the right to withdraw from the trial, etc. But applying a sweeping consumer-oriented law like the CCPA to such clinical trials would be an exceedingly poor fit. The CCPA’s access and deletion rights alone would destroy the ability to conduct a double-blind trial, which is the gold standard for scientific validity.

and private researchers), health outcomes studies, pharmaceutical surveillance studies, opioid prevention and outcomes studies, Risk Evaluation and Mitigation Studies *mandated by the FDA*, etc. Such data may include fully identifiable Protected Health Information, a Limited Data Set as defined by 45 CFR 164.514(e), other pseudonymized data, and/or de-identified data. None of these data-based studies are clinical trials, and yet their worth is invaluable. Subjecting them to the CCPA regimen would, at the very least, chill, burden, and delay such vital research.

The clinical trial exemption thus needs to be dramatically broadened. I'd recommend consulting experts at the American Medical Informatics Association (AMIA), the Association of Clinical Research Organizations (ACRO), and the American Health Information Management Association (AHIMA) regarding the precise language to be used. As a working start, you could consider the following to include the data-based research (a broadening of clinical trial language would be still be needed):

1798.145(c)(1)(C). *Make the existing language a new subsection (i), and then add:*
(ii) Individually identifiable health information, as defined by 45 CFR 160.103, involved in research, as defined in 45 CFR 164.501.

(3) The narrow definition of “deidentified” under section 1798.140(h).

Numerous commentators are criticizing the extremely broad definition of “personal information” and the exceptionally narrow definitions of “deidentified” and “pseudonymize” in section 1798.140 (as well as the lack of harmonization between these definitions). There are also grave concerns about the damage resulting to the healthcare ecosphere and biomedical research of having a state-specific definition of “deidentified” that varies dramatically from the well-understood, established HIPAA standard of “de-identification.” I share those serious concerns, although I won't elaborate on them here.

What I do want to point out, in particular, is that the extremely narrow CCPA definition of “deidentified” is not only inconsistent with such definitions in HIPAA, GDPR, and other privacy laws, it also doesn't comport with the real world. This definition would ban vast swaths of appropriate and valuable uses and disclosures of de-identified healthcare data that currently take place. This would occur because data can meet the CCPA definition of “deidentified” data only if also subject to four highly specific provisos involving technical safeguards to prohibit reidentification, business processes to specifically prohibit reidentification, business processes to prevent inadvertent release of deidentified data, and no attempts to reidentify the data. It's true that in the research or business context where deidentified data is to be appropriately shared, these four provisos may often constitute best practices – *i.e.*, valuable controls to put on the downstream recipient of the de-identified data. For example, Data Use Agreements containing some (though not all) of those provisos are commonplace among biomedical researchers. Furthermore, there are cases where Data Use Agreements banning attempts to re-identify de-identified data, and imposing the same ban on downstream recipients, are mandated by law, such as when a Limited Data Set is shared under HIPAA for research or public health, or sometimes when de-identified data is disclosed under a litigation settlement.

However, this definition would have the odd, and no doubt unintended, effect of providing that properly de-identified data wouldn't be “deidentified” data at all if such provisos have not been

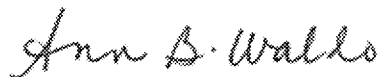
imposed. As written, the statute would mean, for example, that de-identified data could never be released to the public under any circumstances (since obviously, the public can't agree to those provisos). Even numerous data releases currently done by federal, state, and local governments would purportedly be banned, such as hospital discharge data sets released by most states, including California. Countless FOIA data requests would purportedly be blocked as well. This area clearly needs additional work. I believe that far and away the best approach would be to simply harmonize the CCPA definition of "deidentified" with the HIPAA definition of "de-identified." Any divergence in these definitions creates a huge risk of imposing massive financial burdens on the healthcare ecosystem and terrible setbacks to medical research advances.

If the California legislature wants to do something productive and consumer-protective in the realm of protecting de-identified data from re-identification attacks, there are steps that could be thoughtfully and carefully considered. For example, the wisdom of publicly releasing individual-level hospital discharge sets that are as specific and granular as they currently are could be re-evaluated, especially since hospital discharge sets are frequently the most essential data set used in re-identification attacks. Expert statisticians who specialize in statistical disclosure science should be consulted to evaluate the risks of re-identification inherent in the current practice of liberal releases of hospital discharge data sets, while public health experts and scientists should weigh in on the scientific value of having such data remain publicly available. If the decision is made to continue to release the highly granular hospital data, requiring recipients to agree to more rigorous Data Use Agreements banning re-identification seems appropriate.

In addition, it may be time to impose a ban on re-identification and attempted re-identification of de-identified health data, with any appropriate exceptions carefully drawn. A related approach would be to statutorily provide that a commercial attempt to re-identify de-identified biomedical data in order to sell or use the resulting re-identified data, or to buy, sell, or use such re-identified data, is an unfair business practice subject to treble damages and private rights of action. The point is that carefully tailored new measures could be imposed that would create meaningful new protections to safeguard individuals from harm caused by re-identification attacks on de-identified data about them. But defining "deidentified" data in a way that diverges from HIPAA and includes strict provisos that aren't generally used in practice and that sometimes could not even be used at all without banning all important public data disclosures is not a wise approach.

Thank you for the opportunity to express these concerns. I appreciate the hard work involved on the part of the Attorney General staff in crafting appropriate regulations. I'd be more than happy to follow up if I can be of help.

With kind regards,

A handwritten signature in cursive script that reads "Ann B. Waldo". The ink is dark and the signature is fluid, with a large initial 'A' and a clear 'W'.

Ann B. Waldo

Message

From: Kammerer, Susan [REDACTED]
Sent: 3/8/2019 12:19:37 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Merz, Jeremy [REDACTED]
Subject: Comments on CCPA
Attachments: 19-03-8 - CA CCPA Regulations - APCIA Comments - Final.pdf

To Whom it May Concern:

Thank you for the opportunity to provide comments on the CCPA rulemaking process. Please see APCIA's attached comments.

Thank you,

Susan Kammerer

American Property Casualty Insurance Association

1415 L Street, Suite 670

Sacramento, CA 95814

[REDACTED]

Please Note - My Email address has changed effective January 21, 2019 to: [REDACTED]





March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

VIA Electronic Mail: PrivacyRegulations@doj.ca.gov

To Whom It May Concern:

The American Property Casualty Insurance Association (APCIA) is pleased to provide input on the regulatory implementation of the California Consumer Privacy Act (CCPA). APCIA is the preeminent national trade association representing property and casualty insurers doing business locally, nationally, and globally. Representing nearly 60 percent of the U.S. property casualty insurance market, APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers. APCIA represents the broadest cross-section of home, auto, and business insurers of all sizes, structures, and regions of any national trade association.

Consumer privacy and security are priority issues for the insurance industry and insurers devote considerable resources to protect data, information systems, and consumer trust. The insurance industry has been subject to the Gramm-Leach-Bliley Act (GLBA) and implementing privacy regulations in all 50 states and the District of Columbia for over two decades. In California, compliance obligations specific to insurers are found in Cal. Fin. Code §§4050, et seq.; Calif. Ins. Code §791 et seq.; and, Calif. Code Regs. tit. 10, §§2689.1 et seq. The insurance specific statutes seem to have been overlooked from the Calif. Civ. Code §1798.145(e) list of exemptions and, as such, create many challenges and questions for insurance compliance.

Regardless of statutory and regulatory obligations, insurers appreciate the significant responsibility we have to respect consumer privacy and data security while balancing practical day-to-day business applications. A review of the CCPA and existing privacy requirements raises significant concerns that create unnecessary obstacles to this objective and may have the unintended consequence of harming consumers. We respectfully request the California Attorney General clarify the following issues through the rulemaking process.

Scope

Consumer

The definition of “consumer” should be tailored to meet the CCPA’s objective to protect consumer privacy. Currently, as defined in the CCPA, a consumer is broad enough to include any natural person who is a California resident pursuant to identified regulations. “Consumer,” therefore, could include an individual acting in his or her commercial or employment capacity – not only his/her personal capacity – such as an insurance agent, shareholder, vendor, or commercial insured. The Attorney General’s office should clarify that information derived in the context of employment or business transactions is not within the scope of this regulation. This is particularly concerning given the breadth of the definition of “personal information.” Consider, for example, commercial insurance policies where the insurer may need to have personal information of individuals working at a business to process a corporate executive or professional liability policy, employee information for workers’ compensation, processing of a commercial auto or commercial general liability claim, or personal information about an individual principal to issue a commercial surety or fidelity bond, etc. Implementing and complying with the CCPA opt-out and disclosure obligations in this law could unnecessarily stall or even prevent a commercial transaction from moving forward. Considering the statutory obligations and legislative purpose, APCIA does not believe a broad interpretation is the intent of the CCPA and would recommend this ambiguity could be clarified by identifying through regulation who is or is not a “consumer.”

Personal Information

APCIA’s concern with the definition of “personal information” is primarily related to information “capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.” The list could be exhaustive in this context, to include even pseudonymized information, and as such reasonable parameters around how far the list can extend would be helpful. In addition, the household information could be so tangential that there is no ability to associate a single individual with the information, yet it is considered “personal information” under a strict reading. The California Attorney General should provide certainty that there must be a connection to an individual in the household to be identified as “personal information.”

We also question how an Internet Protocol Address (IP Address) can be considered “personal information” or a “unique identifier.” Clarification as to the circumstances the IP Address is capable of being associated with a particular consumer such that it would be considered “personal information” or a “unique identifier” would be helpful. Given the sharing restrictions and notification obligations considering an IP Address personal information could actually harm consumers rather than provide any consumer benefit.

Sale

We urge the Attorney General to reasonably define through regulation or provide guidance as to what does or does not constitute “other valuable consideration.” From a property/casualty insurance perspective, this is particularly important in the context of fraud prevention, claims handling, underwriting, and other necessary business functions. APCIA questions whether the following scenarios, which APCIA believes are outside the spirit of the CCPA, would be interpreted as a “sale” based upon a strict reading of the CCPA.

- An insurer includes a term in a contract that allows a vendor or third-party service provider to use personal information for any purpose outside of the contract's main purpose, but the inclusion of this term does not affect the price of the contract. Is that term considered "valuable consideration?"
- An insurer gives permission to a third-party service provider, who requires personal information in order to perform a necessary business function, to de-identify and aggregate the personal information and then use the de-identified, aggregated data for the provider's own purposes.
- Insurers participate in contributory databases for the purposes of sharing claims information to prevent fraud. This is a critical function that benefits not only consumers but society. The CCPA should not create uncertainty or unintended consequences that allow an individual to opt-out of sharing to avoid detection or have early notification to circumvent a fraud investigation. This sharing can also assist in underwriting where the insurer would not want to rely solely on the consumer to identify a prior claims history, for example.

The "business purpose" exceptions in Cal. Civ. Code §1798.140 (t)(2)(C) should be clarified regarding the disclosure obligations and what is "necessary to perform the business purpose." For instance, in the context of a contributory database, the service provider is further selling/using the personal information, but without that additional sale/use the service would be useless to the insurer. These contributory databases are critical to the business of insurance for a variety of reasons, such as fraud detection and actuarially sound decision making. Again, APCIA believes in the spirit of the CCPA this activity would be "necessary to perform the business," but clarification would be welcome.

Additionally, there are questions about the exchange of information with business partners to obtain information fundamental to conducting business operations such as ratemaking. It should be clear that a person cannot opt-out of activity that is fundamental to providing the services requested. Permitting such an opt-out would be untenable. If a consumer may opt-out of processing information integral to providing a service for which he or she wishes to contract, the covered entity should be able to deny service. The regulations should make clear the types of data and transactions that require opt-out. One way to accomplish this is with a clear and definitive regulatory statement that consumers cannot opt-out of activity that is necessary to perform actions requested by a consumer.

Privileged Information

The CCPA would benefit from implementing regulations that clarify and add certainty for protections of confidential and privileged information. Currently, the only protection is a limited exemption tied to an "evidentiary privilege" under California law. This is extremely narrow and creates a high burden to meet with multiple complex legal issues. The exemption does not account for information of a sensitive or confidential nature. There also has to be a California evidentiary rule that is applicable negating the possibility of cross border litigation needs and suggests that a proceeding must already be in place. Hence, an individual that might be contemplating litigation, or even fraud, is able to obtain information from the business to prepare their case. The California legislature has already recognized that such disclosures are not in the public interest. Cal. Ins. Code §791.01 et seq., the Insurance Information Privacy Protection Act, has a privilege exemption that applies when there is reasonable anticipation that a claim or criminal proceeding will be filed.

We respectfully urge the Attorney General to identify that the evidentiary exemption applies when there is a reasonable anticipation of litigation and the information is sensitive or confidential.

Look Back Period

Business are actively determining how to comply with the CCPA. The legislature recognized that this will take time when they identified the operative effective date as January 1, 2020 and stated that the Attorney General cannot bring any actions until 6 months after this date or the Attorney General has finalized the rulemaking process, whichever is sooner. To that end, APCIA recommends that the look back period should apply from the effective date of the CCPA, so it will not include processing activities that took place prior to January 1, 2020.

Notice

A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. Regulations should clarify that the business with the direct relationship with the consumer should provide this notice. Otherwise, APCIA believes there are potential unintended consequences that will only serve to confuse and frustrate consumers. For instance, consumers may receive multiple notifications for a single transaction. Additionally, businesses should be provided flexibility to meet this notification obligation, such as by posting the notice on a website and directing consumers to the website to review the notice. Given the broad scope of recipients it may be difficult to identify all individuals in an efficient and timely manner.

Production of Personal Information

Cal. Civ. Code §1798.100(a) states that a “consumer shall have the right to request that a business that collects a consumer’s personal information disclose to that consumer the categories and specific pieces of information the business has collected.”

Cal Civ. Code §1798.100(d) states that upon receipt of a verifiable consumer request for the personal information, the business is required to “promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section, [which may] be delivered by mail or electronically, and if provided electronically, the information shall be in a portable. . .format.”

Cal. Civ. Code §§1798.110 and 1798.115 provide a consumer the “right to request that a business that collects personal information about the consumer disclose to the consumer the following:

- Categories of personal information collected about the particular consumer
- Categories of sources from which the personal information is collected
- Business purpose for collecting the personal information
- Categories of third parties with whom the personal information is shared
- Specific pieces of personal information the company has collected about the consumer
- Categories of personal information the company has disclosed for a business purpose

All three sections are subject to Cal. Civ. Code§ 1798.130, which requires that the information be disclosed in a readily useable format upon receipt of a verifiable consumer request. How is a business to determine under which section the verifiable consumer request has been made? What are the practicable

distinctions between these sections? If a business discloses the “incorrect” information, would a business be liable for failure to distinguish between these similar portions of the statute? Clarification on the responsibilities of businesses in responding to verifiable consumer requests is necessary for businesses to comply properly with CCPA’s requirements.

We strongly oppose including a private right of action into the CCPA for a variety of reasons, but the lack of clarity and “gotcha” type of scenario identified above is an example.

Enforcement

The complexity and lack of clarity associated with the CCPA demonstrate the need for the Attorney General to consider building in a consultation provision whereby businesses are allowed a period of time to bring unintentional violations into compliance. Under Cal. Civ. Code §1798.155(b), a business is permitted thirty days to cure an alleged violation after being informed of alleged noncompliance. California Senate Bill 561 seeks to remove the aforementioned cure provision, to which APCIA objects, particularly given the complexity of implementing CCPA while it is still being finalized during the rule-making period.

APCIA appreciates the opportunity to provide feedback. Please, let us know if you have any questions or would like additional information.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Jeremy Merz". The signature is fluid and cursive, with a large, stylized 'J' and 'M'.

Jeremy Merz

Vice President State Affairs, Western Region
American Property Casualty Insurance Association
1415 L Street, Suite 670, Sacramento, CA 95814
P: [REDACTED]

Message

From: Hartwell, Robert L. [REDACTED]
Sent: 3/8/2019 12:08:56 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Attachments: IAB comments to California AG.pdf

Please find attached comments on the CCPA on behalf of the Interactive Advertising Bureau ("IAB").

Rob L. Hartwell, Esq. | Venable LLP

[REDACTED]
600 Massachusetts Avenue, NW, Washington, DC 20001

[REDACTED] www.Venable.com

This electronic mail transmission may contain confidential or privileged information. If
you believe you have received this message in error, please notify the sender by reply
transmission and delete the message without copying or disclosing it.

March 8, 2019

The Honorable Xavier Becerra
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Submitted via privacyregulations@doj.ca.gov

RE: California Consumer Privacy Act Regulation

The Interactive Advertising Bureau (“IAB”) provides these comments in advance of the rulemaking by the California Attorney General (“AG”) on the California Consumer Privacy Act (“CCPA”).

Founded in 1996 and headquartered in New York City, the IAB (www.iab.com) represents over 650 leading media and technology companies that are responsible for selling, delivering, and optimizing digital advertising or marketing campaigns. Together, our members account for the vast majority of online advertising in the United States. In California, we contribute \$168 billion to the state gross domestic product and support over 478,000 full-time jobs in the state.¹ Working with our member companies, the IAB develops technical standards and best practices and fields critical research on interactive advertising, while also educating brands, agencies, and the wider business community on the importance of digital marketing. The organization is committed to professional development and elevating the knowledge, skills, expertise, and diversity of the workforce across the industry. Through the work of our public policy office, the IAB advocates for our members and promotes the value of the interactive advertising industry to policymakers and legislators across the country.

The free flow of data online enables the continued economic success of the Internet, creating substantial consumer benefit. Online data-driven advertising has powered the growth of the Internet for decades by funding innovative tools and services for consumers and businesses to use to connect and communicate. Data-driven advertising supports and subsidizes the online content and services consumers expect and rely on, including video, news, music, and much more, at little or no cost to the consumer. Companies also collect data for various operational purposes, such as ad delivery and reporting, fraud prevention, network enhancement, and customization. These uses are necessary for a seamless cross-channel, cross-device consumer experience and a functioning digital economy.

As a result of this advertising-based model, the Internet economy in the United States has rapidly grown to deliver widespread consumer and economic benefits. According to a recent study conducted for the IAB by Harvard Business School Professor John Deighton, the U.S. ad-supported Internet created 10.4 million jobs in 2016, and the data-driven ad industry contributed \$1.121 trillion to the U.S. economy that year, doubling its contribution over just four years and accounting for 6 percent of U.S. gross domestic product. Consumers have enthusiastically

¹John Deighton, *The Economic Impact of California’s Advertising-Supported Internet Ecosystem* (2017), available at <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>.

embraced the ad-supported model, and they have actively enjoyed the free content and services it enables. They are increasingly aware that online products and services are enabled by data collected about their interactions and behavior on the web and in mobile applications, and they support that exchange of value. A Zogby survey commissioned by the Digital Advertising Alliance (“DAA”) found that consumers assigned a value of nearly \$1,200 a year to common ad-supported services.² A large majority of surveyed consumers (85 percent) stated they like the ad-supported model, and 75 percent indicated that they would greatly decrease their engagement with the Internet were a different model to take its place.³ It is important that the CCPA and the AG’s rules thereunder do not create an environment that harms the democratization of access to ad-supported goods and services consumers want, such as by creating an environment where paywalls and subscription-based models bar access to those unable to afford to pay.

Legislative and regulatory efforts to empower consumers by giving them increased control over their online data must take into account consumers’ support for the ad-driven Internet model. To that end, in order to assist the AG in developing regulations implementing the CCPA, we provide these comments. IAB broadly supports the purpose and intent of the CCPA—to enhance consumer privacy by giving consumers transparency and choice regarding the use of their personal information. However, a number of provisions in the law are unclear, and some will detract from current effective consumer privacy practices in the marketplace. Myriad research papers, surveys, and reports that we, our members, and sister trades have developed reveal and explain the value of data within the economy, especially in California.⁴ This body of research makes clear that the free flow of data, coupled with appropriate privacy protections, is the economic engine that fuels the data-driven economy providing consumers with benefit. As a result, the AG’s regulation(s) interpreting the CCPA should clarify the law’s terms and remedy its unintended results of reducing consumer choice and privacy rather than expanding it, as the law intended. Below we discuss specific provisions of the CCPA that require the AG’s clarification, and how such changes are supported by the regulatory authority provided to the AG in the CCPA.⁵

² Zogby Analytics, *Public Opinion Survey on Value of the Ad-Supported Internet* (May 2016), available at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/ZogbyAnalyticsConsumerValueStudy2016.pdf

³ *Id.*

⁴ Please find the following pieces of research: Howard Beales, *The Value of Behavioral Targeting* (2010), available at https://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf; Ari Goldfarb & Catherine Tucker, *Privacy Regulation and Online Advertising* (2011), available at https://econpapers.repec.org/article/inmormnsc/v_3a57_3ay_3a2011_3ai_3a1_3ap_3a57-71.htm; Howard Beales & Jeffrey Eisenach, *An Empirical Analysis of the Value of Information Sharing in the Market for Online Content* (2014), available at <http://www.aboutads.info/resource/fullvalueinfostudy.pdf>; Yan *et al.*, *How much can Behavioral Targeting Help Online Advertising?* (2009), available at <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.215.1473&rep=rep1&type=pdf>; Zogby Analytics, *Public Opinion Survey on Value of the Ad-Supported Internet* (May 2016), available at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/ZogbyAnalyticsConsumerValueStudy2016.pdf; John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017), available at <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>; Zogby.

⁵ See Cal. Civ. Code § 1798.185.

I. Clarify that Data is Personal Information Only When Individuals Act in their Consumer Capacities

The definition of the terms “personal information” and “consumer” in the CCPA appear to cover employee data.⁶ Such a reading of the law could be disruptive of employer-employee relationships and expose proprietary business records to risk. The AG should clarify that the CCPA applies to personal information only when individuals act in their consumer capacities.

Personal information under the CCPA includes “[p]rofessional or employment-related information” if such information is capable of being associated with a consumer.⁷ “Consumer” is defined as “a natural person who is a California resident... however identified.”⁸ These terms could encompass information held in a business-to-business context pertaining to an individual’s status or actions as an employee of a company, not as a “consumer” as the term is traditionally understood. For instance, if personal information includes “professional or employment-related information” that is associated with a California resident in an employee or independent contractor rather than a consumer context, all business contact data and anything “capable of being associated with” such data could be included within the scope of the CCPA’s access, deletion, and opt-out rights. Such an interpretation would risk exposing proprietary business information to a third party access request, pose supply chain disruptions for businesses, and harm employee relationships with employers.

We suggest that the AG issue a rule declaring that “[p]rofessional or employment-related information” excludes information about California residents when they are acting in an employment or business context. The AG may issue such a clarification pursuant to his ability to adopt rules to “updat[e] as needed additional categories of personal information.”⁹ Publishing a rule to clarify that the phrase “[p]rofessional or employment-related information” relates to an individual acting in the capacity of a consumer (as that term is generally understood) and excludes information about an individual acting in the capacity of an employee or in a business context and related business information updates an additional category of personal information by clarifying the types of employment information covered by Section 1798.140(o)(1)(I) of the CCPA, and addresses an obstacle to implementation of the CCPA which the AG is directed to address. Information about business-to-business contacts and transactions is used by businesses for legally required record-keeping, auditing, and research purposes, and should not be included in the definition of personal information pertaining to the consumer.

II. Empower Consumers to Delete or Opt Out from the Sale of Part and All of their Personal Information

While the CCPA enables consumers to delete or opt out from businesses’ sale of their data, it gives consumers no ability to select which data points they would like to delete or restrict from sale. This approach fails to give consumers full control over their data and could limit consumers from accessing particular benefits associated with data use and sale. We therefore

⁶ Employee, in this context, should be understood broadly to include direct employees, contractors, contingent workers, and other employee-employer relationships.

⁷ Cal. Civ. Code § 1798.140(o)(1)(I).

⁸ Cal. Civ. Code § 1798.140(g).

⁹ Cal. Civ. Code § 1798.185(a)(1).

ask the AG to issue a rule recognizing that in addition to all of related personal information, companies can choose to offer consumers the opportunity to delete or opt out from the sale of part of their personal information under the CCPA if the business elects to offer and is capable of offering such granular choices.

The CCPA gives consumers the right to completely opt out of the sale of their data, or fully delete their data from businesses' files.¹⁰ The law, however, does not acknowledge that a consumer may wish to delete or opt out of the sale of only a portion of the personal information a business may maintain about them. Such binary, all-or-nothing choices do not empower consumers to express their true preferences or tailor their requests. Requiring all-or-nothing consumer choices could also deprive consumers of select benefits associated with data sale. The lack of consumer choice in the CCPA surrounding the exact data points they can delete or restrict from sale has the potential to engender consumer confusion and frustration, and allowing companies the option to offer more tailored choices to consumers if they choose to do so would help ease this potential confusion.

We suggest that the AG clarify that businesses are allowed to offer more granular choices to consumers about the types of "sales" they want to opt out of, or the types of data they want deleted, not just provide an all-or-nothing option. This would provide consumers with more valuable and personalized choices that reflect their actual preferences. The AG has authority to clarify this issue pursuant to his directive to establish rules "[t]o facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information."¹¹ The AG also has authority to interpret and clarify the CCPA's deletion right pursuant to the regulatory authority to issue rules that "further the purposes of [the] title".¹² By providing the option for companies to enable more tailored consumer choices, and create an environment that reflects actual consumer expectations, the AG will promote more effective privacy choices for consumers when they interact with businesses that decide to offer such choices to their customers.

III. Protect Existing Privacy Controls and Enable Flexibility for Effectuating Rights Requests to Promote Privacy Protections for Consumers


We ask the AG to clarify that businesses are not required to identify data that has been pseudonymized. Pseudonymized data sets do not include identifiable information like name, postal address, or email. This type of identifiable information is the type of data that would likely be included in a consumer's request, which is not associated with pseudonymized data sets. Without the requested clarification, the CCPA could be read to compel businesses to link identifiable and non-identifiable information, thereby destroying a common consumer privacy protection. This result is counter to the privacy protective goals of the CCPA, and would also run counter to the CCPA provision that states: "This title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information."¹³

¹⁰ Cal. Civ. Code §§ 1798.100, 105, 110, 115, 120.

¹¹ Cal. Civ. Code § 1798.185(a)(4)(A).

¹² Cal. Civ. Code §§ 1798.185(a), (b).

¹³ Cal. Civ. Code § 1798.145(i).

We ask the AG to clarify that companies are not required to identify non-identifiable pseudonymized data, and that they can use flexible tools to provide rights to consumers to protect certain consumer privacy practices. This interpretation is necessary because without it many businesses may be required to make pseudonymous data, to the extent it is personal information under the CCPA, identifiable if they do not have this flexibility. The CCPA suggests this result should not be the case.¹⁴ One such tool to effectuate rights that companies could use if provided with this flexibility is the DAA YourAdChoices Icon  and consumer choice program for data that this program covers.¹⁵ The AG has authority to issue these rules pursuant to his ability to “[e]stablish... rules and procedures... [f]or the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information,” as well as under his authority to issue rules that further the purpose of the CCPA.¹⁶ The AG should leverage existing tools that have wide consumer recognition to achieve this goal, and allow companies to choose to offer different opt-out choices, as opposed to a single choice, to prevent the reidentification of covered pseudonymized data, and further the law’s goal of providing consumers with privacy controls.¹⁷

IV. Allow Businesses to Reference Privacy Policies to Comply with the Requirement to Provide Consumers with Information “At or Before the Point of Collection”

We request that the AG issue a rule allowing businesses to reference their privacy policies in order to comply with the CCPA requirement to give consumers information about data practices at or before the point of data collection. The CCPA requires “a business that collects a consumer’s personal information” to, “at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used.”¹⁸ The law does not explicitly state the methods by which businesses must give such notice or allow businesses to give consumers the required information at a later point in time. Additionally, online businesses may have difficulty providing this information if they do not collect information directly from consumers but instead collect it through interactions and commercial relationships with other parties, such as third party advertising companies that support first party publishers’ websites and digital properties.

We ask that the AG clarify that businesses may fulfil this requirement by pointing consumers to online privacy policies to access the required information. We also ask the AG to

¹⁴ See Cal. Civ. Code § 1798.145(i).

¹⁵ The White House recognized the DAA Self-Regulatory Program as “an example of the value of industry leadership as a critical part of privacy protection going forward.” The DAA also garnered kudos from then-Acting FTC Chairman Maureen Ohlhausen who stated that the DAA “is one of the great success stories in the [privacy] space.” In its cross-device tracking report, the FTC staff also praised the DAA for having “taken steps to keep up with evolving technologies and provide important guidance to [its] members and the public. [Its] work has improved the level of consumer protection in the marketplace.”

¹⁶ Cal. Civ. Code § 1798.185(a)(4)(C); §§ 1798.185(a), (b).

¹⁷ Consumer awareness and understanding of the program continues to increase, and a 2016 study showed more than three in five consumers (61 percent) recognized and understood what the YourAdChoices Icon represents. DAA, *Consumers' recognition of the AdChoices Icon -- and understanding of how it gives choice for ads based on their interests -- continues to rise* (Sep. 29, 2016) <https://digitaladvertisingalliance.org/blog/icon-you-see-yeah-you-know-me-0>.

¹⁸ Cal. Civ. Code § 1798.100(b).

issue a rule acknowledging that businesses which collect consumer information from other businesses may satisfy the CCPA requirement by disclosing this information in their online privacy policies. The AG has authority to issue these rules pursuant to his ability to establish rules to “facilitate a consumer’s or the consumer’s authorized agent’s ability to obtain information pursuant to Section 1798.130...” and “to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer.”¹⁹ These rules would facilitate the consumer’s ability to obtain and understand information by providing the required data in an easily accessible, readily available format. Furthermore, these rules would be consistent with other laws, such as California’s Shine the Light law and the California Online Privacy Protection Act, which require businesses to provide particular disclosures to consumers.²⁰

V. Clarify the Household Concept

IAB requests that the AG issue a rule clarifying the term “household” in the law. The CCPA gives consumers the right to access their personal information,²¹ and the law’s definition of personal information includes “household” data.²² However, the law does not define the term “household,” and the CCPA provides no guidance on what constitutes a “household” under the law. For example, it is unclear whether a “household” includes living arrangements involving roommates, college dormitories, or other individuals who may live in a particular home at different points in time potentially with no familial relationship between them. As such, the CCPA’s indefinite language could be interpreted to require a business to disclose information about a consumer within a “household” to another consumer in the household when responding to a consumer access request. This possibility creates privacy concerns, because a business might provide a consumer’s personal information to a household member who should not have access to such data, creating the potential for a data leakage facilitated by a legal obligation.

IAB suggests the AG clarify the definition of “household” to mean information known about the consumer making the request and information about others in the household only if the individual making the request is an authorized representative of such other persons. The AG has authority to issue this clarification pursuant to his authority to “[e]stablish rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer’s...ability to obtain information...”²³ The AG should exercise this authority and create regulations to explain the type of household data that should be provided to a consumer without creating additional privacy concerns.

VI. Provide Flexibility for Verifying and Executing Consumer Requests

IAB asks the AG to issue a rule to clarify that: (a) a business may use commercially reasonable methods to verify a consumer’s request, and (b) if data is maintained in a pseudonymous manner, businesses have no obligation to identify such data to effectuate the

¹⁹ Cal. Civ. Code §§ 1798.185(a)(6), (7).

²⁰ Cal. Civ. Code § 1798.83; Cal. Bus. & Prof. Code §§ 22575 - 22579.

²¹ Consumers have “the right to request that a business that collects personal information about the consumer disclose to the consumer...the categories [and]... specific pieces of personal information it has collected about that consumer.” Cal. Civ. Code § 1798.110(a).

²² Cal. Civ. Code §§ 1798.110; 140(o)(1).

²³ Cal. Civ. Code § 1798.185(a)(7).

consumer rights under the law. The CCPA relies on the concept of a “verifiable consumer request” to trigger businesses to act on any of the rights granted to consumers. However, businesses will have difficulty verifying a consumer’s request in incidences where the information businesses maintain is not directly identifiable to an individual consumer. Digital advertisers often collect and pseudonymize data, associating it with a unique identifier, as a privacy protective practice. The pseudonymized information is thereafter not tied to a consumer’s name or other identifying information. As a result, verifying a consumer’s request, and associating non-identifiable information with a consumer, could be technologically difficult under the CCPA without the business’s ability to request additional information from the consumer or require that pseudonymized data be made identifiable, thereby undermining consumer privacy.²⁴ A similar problem exists for verifying authorized representatives who may submit CCPA requests on behalf of consumers.²⁵ One possible path for solving this difficult issue will be for companies to store all information in an identifiable form, thereby reducing privacy protections for Californians in direct competition with the CCPA’s stated goals.

We ask the AG to issue a rule stating that a business may use commercially reasonable methods to verify a consumer request, and if such methods fail that the request is not a verifiable consumer request. The AG can issue these clarifications pursuant to his authority to establish “rules and procedures... to facilitate a consumer’s... ability to obtain information pursuant to Section 1798.130...”²⁶ The AG can also make this interpretation pursuant to his specific authority to adopt rules related to verifiable consumer requests as articulated in the CCPA’s definition of a “verifiable consumer request.”²⁷

VII. Clarify “Explicit Notice”

In order for third parties to sell a consumer’s personal information under the CCPA, third parties must ensure that consumers received “explicit notice” of the sale and an opportunity to opt out.²⁸ However, third parties typically do not directly interface with consumers in a way that would allow them to provide such explicit notice directly. We therefore ask the AG to clarify via regulation that third parties have the choice to rely on contractual, written, or other assurances from businesses selling data to the third party that the CCPA-required “explicit notice” has been provided as one method of providing “explicit notice.”

The CCPA’s “explicit notice” requirement is not clearly defined. Third parties, generally defined by the CCPA as entities who do not fit the description of a business or a service provider,²⁹ may not be able to provide consumers with explicit notice because they usually have no direct contact with the consumer. As a result, third parties may be prohibited from selling

²⁴ The only approved method under the CCPA for confirming consumer identities assumes the consumer maintains an account with the entity to which the request is directed. Cal. Civ. Code § 1798.185(a)(7).

²⁵ Cal. Civ. Code §§ 1798.135(a)(1), (c), 140(y).

²⁶ Cal. Civ. Code § 1798.185(a)(7).

²⁷ Cal. Civ. Code § 1798.140(y) (A verifiable consumer request is “a request that...the business can reasonably verify, pursuant to regulations adopted by the AG pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information.”).

²⁸ Cal. Civ. Code § 1798.115(d).

²⁹ Cal. Civ. Code § 1798.140(w) (“Third party” means a person who is not... [t]he business that collects personal information from consumers under this title... [or a] person to whom the business discloses a consumer’s personal information for a business purpose pursuant to a written contract....”).

personal information all together due to the fact they cannot provide explicit notice of this practice to consumers. The CCPA, therefore, would have the unintended effect of rendering third parties entirely unable to sell consumers' personal information. This result could undermine competition and threaten the general availability of online products, services, and content that consumers value, as advertisers' ability to fiscally support publishers' free online offerings would be inhibited. The data-driven advertisers that help provide these digital goods and services collect information from publisher websites, and often do not directly interact with a consumer in order to provide "explicit notice," and this could lead to such advertisers abandoning publishers due to the unclear nature of the "explicit notice" requirement.

To rectify this practical problem in a way that aligns with the spirit of the CCPA, we urge the AG issue a rule stating that contractual, written, or other assurances between businesses and third parties is one method for satisfying the requirements of the law when one party has fulfilled the "explicit notice" obligation to consumers. Specifically, the business that transfers data to a third party can represent, and the third party can rely upon such representations, that the consumer has been offered "explicit notice," thereby satisfying the obligation under Section 1798.115(d). The AG has authority to issue this rule pursuant to his ability to create rules to "facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130."³⁰ A business that has a direct relationship with a consumer could help facilitate providing explicit notice to consumers rather than third parties that lack such a relationship, and in instances where this relationship occurs companies should be able to choose to agree how they will provide explicit notice. Issuing a rule allowing businesses to meet the requirement to provide explicit notice in this manner will help ensure that opt-out disclosures are provided to consumers by the entities that have a direct relationship with them. Without such an interpretation of the law, many products and services in the digital economy are threatened, as the data transfers needed to create or deliver those products could be impeded.

VIII. Clarify that the CCPA Does Not Require Individualized Privacy Policies

IAB requests that the AG clarify that a business is not required to list the specific pieces of information it has collected about that consumer in a personalized privacy policy. The CCPA suggests that a business must disclose "specific pieces of personal information the business has collected about that consumer" in its privacy policies.³¹ However, this requirement appears in a section of the law that sets forth a consumer's right to access their data, which could mean that businesses only need to disclose "specific pieces of personal information" in response consumer access requests. As currently written, the requirement is unclear, but if it applies to privacy policies provided online to the general public, it would be onerous for businesses and detrimental to consumer privacy. Businesses would need to create individualized privacy policies for each California consumer who visits their website or engages with their products or services to

³⁰ Cal. Civ. Code § 1798.185(a)(7).

³¹ Cal. Civ. Code § 1798.110(c) ("A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130: (5) The specific pieces of personal information the business has collected about that consumer."); Cal. Civ. Code § 1798.130(a)(5)(B) ("In order to comply with [Section]... 1798.110... a business shall, in a form that is reasonably accessible to consumers... [d]isclose... in its online privacy policy... [f]or purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.").

comply with the CCPA or risk a personal data breach. Aside from the fact that this requirement presents an impossible obligation for businesses, creating such individualized privacy policies would likely increase the possibility that consumers' personal information would be accidentally disclosed to individuals who should not have access to such information. This would detract from consumer privacy rather than advance it.³²

We urge the AG to clarify that specific pieces of information should be provided to consumers only in response to a verifiable consumer access request and that a business need not create individualized privacy policies for each California consumer to comply with the CCPA. The CCPA gives the AG authority to “[e]stablish rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer’s...ability to obtain information...”³³ In creating rules that explain when “specific pieces of information” should be provided to a consumer, the AG can facilitate a consumer’s ability to obtain information under the law, and ease compliance without detracting from the goals of the CCPA.

IX. Clarify that “Aggregate Consumer Information,” and “Deidentified” Information Are Not “Personal Information” or Are Fully Exempt from the CCPA

We ask that the AG issue a rule clarifying that deidentified information and aggregate consumer information are not personal information or are fully exempt from the CCPA. We make this request because there is language in the CCPA that has the unintended consequence of potentially sweeping in deidentified information and aggregate consumer information into the coverage of the law. Without this clarity, companies and consumers alike will be uncertain what rights apply to these two data types, and it will create unintentional confusion about how the CCPA should be implemented.

First, the CCPA broadly defines personal information as “information that... is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”³⁴ The law attempts to carve out deidentified and aggregate consumer information by creating separate definitions for each data set.³⁵ The definitions suggest that each data set is exempted from the definition of personal information, but no explicit carve out for deidentified information and aggregate consumer information is stated. Thus, any minor or technical difference in the definitions could be inappropriately interpreted to mean that deidentified information or aggregate information is covered by the definition of personal information.

Second, the CCPA provides a broad exception for the deidentified and aggregate consumer information when it states, “The obligations imposed on businesses by this title shall

³² Furthermore, in a survey of 1,039 California adults conducted by the DAA via SurveyMonkey from January 29-30, 2019, over 87% of individuals surveyed indicated they would prefer to receive generic information from a business based on broad interest and demographic categories rather than detailed information based on the individual’s specific activities, identity, and interests. DAA, *California Perspectives on Privacy Issues* (Jan. 2019), available at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/DAA_CA_privacy_survey_January_2019.pdf.

³³ Cal. Civ. Code § 1798.185(a)(7).

³⁴ Cal. Civ. Code § 1798.140(o)(1).

³⁵ Cal. Civ. Code § 1798.140(h); 1798.140(a).

not restrict a business's ability to... (5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information,"³⁶ but this exception is vaguely drafted and does not explicitly state that de-identified and aggregate consumer information is not covered by the CCPA since it has no bearing on consumer privacy.

Combining the two issues above, an inappropriate interpretation of the definition of personal information could include deidentified information and aggregate consumer information. And since the full exemption for deidentified information and aggregate consumer information elsewhere in the law is vaguely worded, the unintentional result could be consumer requests not to share deidentified and aggregate consumer information, or claims of price or service discrimination based on these data sets after a consumer exercises their deletion or opt-out rights under the CCPA, which are all tied to the definition of personal information.

We urge the AG to clarify that "deidentified" information and "aggregate consumer information," are not "personal information" and are fully exempt from the CCPA. The AG has authority to promulgate such a rule pursuant to his ability to issue regulations to "further the purposes of [the CCPA]."³⁷ This interpretation would further the purposes of the CCPA by ensuring that the law remains focused on protecting consumer privacy and does not unintentionally hinder the collection, use, and sharing of non-personal information. A rule clarifying that these kinds of data are not personal information is consistent with the language of the CCPA, and furthers the spirit and intent of the law.

X. Interpret the Non-Discrimination Section So Businesses May Charge Consumers who Opt Out of Data Sharing a Reasonable Fee to Access Content

IAB asks the AG to allow businesses to charge a reasonable subscription fee to consumers who have opted out from businesses' sale of their data. The CCPA's non-discrimination section prohibits businesses from offering consumers who have exercised CCPA rights different prices for goods or services or a different quality or level of goods or services than that which would be offered to a customer who did not exercise CCPA rights.³⁸ However, the law explicitly allows a business to charge different prices or provide a different quality or level of goods or services "if [the] difference is reasonably related to the value provided to the consumer by the consumer's data."³⁹ The CCPA offers no information regarding how a businesses should understand when a charge is "reasonably related to the value provided to the consumer by the consumer's data." The law also allows businesses to offer "financial incentives" for the collection, sale, or deletion of personal information, which may not be "unjust, unreasonable, coercive or usurious in nature," and for businesses to offer different prices, levels, or qualities of goods or services if the "price or difference is directly related to the value provided to the consumer by the consumer's data."⁴⁰ Although the CCPA creates these abilities and requirements for businesses, it offers no definition of "financial incentive," no guidance for how businesses should interpret "directly related to the value provided to the

³⁶ Cal. Civ. Code § 1798.145(a)(5).

³⁷ Cal. Civ. Code §§ 1798.185(a), (b).

³⁸ Cal. Civ. Code § 1798.125(a)(1).

³⁹ Cal. Civ. Code § 1798.125(a)(2).

⁴⁰ Cal. Civ. Code §§ 1798.125(b)(1), (4).

consumer by the consumer's data," and no clarity regarding what constitutes an unjust, unreasonable, coercive, or usurious financial incentive.

Without clarification, the non-discrimination provision could prevent publishers and others from charging consumers who have opted out of data sharing a reasonable fee or rate for access to content, or otherwise offering a different experience that is reasonably related to the choices a consumer has made. Developers of media rely on third-party advertisers to generate revenue to produce and provide sought-after information and content. When consumers opt out of the ability to share their data, many publishers will not be able to generate sufficient revenue and may need to turn to subscription models to continue to function. However, an overly-broad interpretation of the CCPA's non-discrimination provision could preclude the use of subscription models and jeopardize the existence of these publishers. Interpreting the CCPA in this manner ultimately harms consumers, as the availability of free and varied online content would inevitably shrink due to publishers' inability to create revenue from their content, products, and services.

IAB urges the AG to issue a rule clarifying that businesses may charge consumers who have opted out of data sharing a reasonable subscription fee or rate as an alternative to using advertising-supported services, and that such a reasonable subscription fee is *per se* directly related to the value provided to the consumer based on the consumer's data. The AG has authority to issue such a rule pursuant to his ability to "further the purposes of [the] title."⁴¹ The rule we seek would further the purposes of the title because as it is currently written, the non-discrimination provision is vague and may conflict with Section 1798.145 of the CCPA, which states: "[t]he rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers."⁴² Without a rule clarifying that reasonable subscription fees do not conflict with the CCPA's anti-discrimination provision, the accumulation of individual decisions by consumers to delete or opt out of data sharing would threaten the availability of free online content for all, which will adversely affect the rights of other consumers that desire to access free, ad-supported content.

XI. Make Clear that the CCPA Does Not Create a Data Retention Requirement

We ask the AG to issue a rule stating that the CCPA does not indirectly create a data retention requirement. The CCPA requires businesses to disclose and deliver information to a consumer covering "the 12-month period preceding the business's receipt of the verifiable consumer request..."⁴³ The law does not, however, note whether this means that businesses must begin retaining data before the law's enforcement date to comply with a potential consumer access request that could occur on January 1, 2020.⁴⁴ Such an interpretation would effectively impose an immediate 12-month data retention requirement on businesses, even though no data retention requirement is explicitly created by the law and businesses will not create CCPA compliance processes until the final rules interpreting the law have been issued.

⁴¹ Cal. Civ. Code §§ 1798.185(a), (b).

⁴² Cal. Civ. Code § 1798.145(j).

⁴³ Cal. Civ. Code § 1798.130(a)(2).

⁴⁴ Cal. Civ. Code § 1798.198(a) notes that the CCPA "shall be operative on January 1, 2020."

We urge the AG to clarify that businesses do not need to retain data collected 12 months before the enforcement date of the CCPA as no such data retention requirement exists in the law. The AG may regulate these issues based on his authority to adopt rules to “further the purposes of [the] title.”⁴⁵ Clarifying that businesses need not retain data would further the purposes of the CCPA by allowing companies to delete data that is no longer needed.

XII. Clarify “Publicly Available” Information

We ask the AG to issue a regulation clarifying that businesses may use “publicly available” information unless other legal requirements explicitly prohibit a particular use of such information. The CCPA excludes “publicly available” information from the definition of “personal information” without clearly defining what comprises publicly available information.⁴⁶ Although the law states that “information is not publicly available unless it is used for the purpose for which it was made available in a government record,”⁴⁷ this phrase does not provide sufficient clarity, and in fact creates additional ambiguity regarding what constitutes publicly available information, as government records often do not disclose the reasons why they were released. This ambiguity creates an open question of how businesses should treat information that is publicly available when the reason for the release of such information is not explicitly disclosed.

We urge the AG to clarify that information made available by government disclosures can be used even if no purpose for such information’s release is disclosed, unless a particular use of the information is expressly prohibited in other laws. The AG can issue this rule under his authority to adopt regulations to further the purposes of the CCPA.⁴⁸ Making a consumer’s rights to information contingent on whether a business’s use of the information was for the purpose for which the government made the information available creates arbitrary and confusing restrictions on the ability for consumers to exercise their rights under the CCPA. Clarifying that publicly available information includes information made public by the government for any purpose, unless other laws directly prohibit a particular use of such information, will further the intent of the CCPA by decreasing consumer confusion and allowing businesses to streamline responses to consumer requests.

XIII. Allow for Additional “Business Purposes”

The CCPA’s definition of “business purpose” includes seven enumerated, permissible purposes. The AG should clarify that these listed business purposes are merely exemplary and do not constitute an exclusive list of allowable business purposes under the law. The CCPA defines the term “business purpose” as “the use of personal information for the business’s or a service provider’s operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected.”⁴⁹

⁴⁵ Cal. Civ. Code §§ 1798.185(a), (b).

⁴⁶ Cal. Civ. Code § 1798.140(o)(2).

⁴⁷ *Id.*

⁴⁸ Cal. Civ. Code §§ 1798.185(a), (b).

⁴⁹ Cal. Civ. Code § 1798.140(d).

After defining the term, the CCPA states, “Business purposes are:” and lists seven permissible purposes.⁵⁰ This language could be read to limit the definition of “business purpose” to the seven enumerated examples in the law. This drafting poses a practical problem for businesses, because they often share information with service providers for business purposes that are not enumerated in the CCPA, and new business purposes are created over time in the innovative digital economy.

We urge the AG to clarify that the seven listed categories of “business purposes” are examples instead of the only acceptable business purposes that may fit within the definition of the term. The AG can issue such a rule based on his authority to adopt rules to “further the purposes of [the] title.”⁵¹ The general definition of business purpose that precedes the seven examples suggests that the term was intended to encompass more than what is expressly listed in the text of the law, and that those seven examples are not the only “business purposes” that the legislature intended to cover. Otherwise, the legislature would have omitted the general description of business purposes and only provided the seven examples. Therefore, understanding the listed business purposes as examples rather than the only allowable business purposes under the definition would further the purposes of the title by aligning with legislative intent.

XIV. Clarify the Deletion Right and Consumer Rights Related to Backup and Archived Data

IAB asks the AG to clarify (1) the exception to the deletion rule so that businesses may provide expected subscription messages to consumers that are reasonably anticipated within the context of the business’s ongoing relationship with such consumer and (2) information held in backup or archival storage need not be subject to a consumer request. The CCPA requires businesses to delete “any personal information about the consumer which the business has collected from the consumer” upon receipt of a verifiable consumer request.⁵² Although the law exempts businesses from the need to delete personal information if maintaining it is necessary for the business to “provide a good or service... reasonably anticipated within the context of a business’s ongoing business relationship with the consumer, or otherwise perform a contract with the consumer,” it does not explain what conduct can be considered “reasonably anticipated” within an “ongoing business relationship” with a consumer. The CCPA also creates an exception for requests that are “manifestly unfounded” or “excessive” but not define these terms, which creates uncertainty for the application of a consumer request related to backup and archived data.⁵³

We urge the AG to clarify what is “reasonably anticipated within the context of a business’s ongoing business relationship with the consumer.” Such a regulation should confirm that expected subscription messages are reasonably anticipated within an ongoing business relationship with a consumer that maintains a subscription with the company following a deletion request. The AG may issue these rules pursuant to his authority to further the purposes

⁵⁰ *Id.*

⁵¹ Cal. Civ. Code §§ 1798.185(a), (b).

⁵² Cal. Civ. Code §§ 1798.105(a), (c).

⁵³ Cal. Civ. Code §§ 1798.145(g)(3).

of the CCPA,⁵⁴ as such interpretations would advance consumer privacy by helping fulfil the consumer rights listed in the law and reduce uncertainty around the kinds of data businesses must delete in response to a verifiable request.

We also urge the AG to clarify that “manifestly unfounded” or “excessive” includes a response to consumer request related to backup or archival data. If consumer requests can reach the data held on backup or archival systems, the costs associated with these requests would be excessive and, in the specific circumstance of a deletion request, businesses’ ability to rebound from data failures and comply with legal obligations would be severely limited. Further, in the case of a deletion right or opt-out right for backup or archived data, clarity is needed to ensure that businesses can mitigate data loss issues without having to contact the consumer for assistance in restoring (or gaining the ability to share) necessary information from a backup or archived file.

XV. Clarify the Definition of “Research”

We ask the AG to clarify that the definition of “research” is not limited to studies conducted “in the area of public health.” According to the CCPA, research means “scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest *in the area of public health*.”⁵⁵ An overly limited interpretation would find that “in the area of public health” is the only area of allowable research, even though the definition states that research means “scientific, systematic study and observation” and then states that it “includes” studies in the area of public health.” As a result of an overly narrow interpretation, studies in the area of public safety or otherwise in the public interest would not be included.

To ensure that “research” remains a viable concept in the CCPA for a variety of purposes, and to avoid stifling innovation, we urge the AG to clarify that the use of personal information for research outside the area of public health is permissible. The AG has authority to issue such a rule pursuant to his ability to “further the purposes of [the] title.”⁵⁶ Such an interpretation would further the purposes of the title by making sure the concept of research retains meaning and usefulness under the law.

XVI. Clarify the Definition of “Business”

We ask the AG to clarify what it means to “do business” in the state of California and explain that the terms “household” and “device” only apply households and devices associated with California residents. To qualify as a “business” that is subject to the requirements of the CCPA, a legal entity must do business in California and satisfy certain revenue or data processing thresholds. One such threshold deems a legal entity a business if it “[a]lone or in combination, annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more

⁵⁴ Cal. Civ. Code §§ 1798.185(a), (b).

⁵⁵ Cal. Civ. Code § 1798.140(s) (emphasis added).

⁵⁶ Cal. Civ. Code §§ 1798.185(a), (b).

consumers, households, or devices.”⁵⁷ While the CCPA defines “consumer” as California residents,⁵⁸ the law does not define the term “household” and the definition of the term “device” is not limited to devices associated with California residents.⁵⁹ As a result, these terms could be interpreted to include any household or device—not just those located in or associated with California residents or consumers. This imprecise drafting could have the effect of subjecting more legal entities than intended to the bounds of the CCPA, and could sweep in businesses that have minimal operations in California or even the United States.

IAB urges the AG to clarify (1) what it means to “do business” in the state of California and (2) that the use of the terms “household” and “device” throughout the CCPA only applies to households in California or devices of California residents. The AG may issue these rules based on his authority to “further the purposes of [the] title,”⁶⁰ as such regulations would further the intent of the law to only apply to businesses that do business in California and collect or process Californians’ data. This will help businesses respond to actual Californian requests in a timely and efficient manner, without a backlog of non-covered requests related to non-California households and devices.

XVII. Clarify the Time Period for Businesses to Comply with Consumer Requests

We request that the AG clarify that businesses may invoke both of the extension periods listed in the CCPA before responding to a consumer request under the law. The CCPA states: “In order to comply with... [the access, deletion, and opt-out rights]... a business shall, in a form that is reasonably accessible to consumers... [d]isclose and deliver the required information free of charge within 45 days of receiving a verifiable consumer request from the consumer.”⁶¹ The CCPA also states that “[t]he time period to provide the required information may be extended once by an additional 45 days when reasonably necessary...”⁶² It later allows for the “time period for a business to respond to any verified consumer request” to “be extended by up to 90 additional days where necessary.”⁶³ Because two sections in the CCPA address the potential for extending time for businesses to comply with consumer requests, clarity from the AG is needed to harmonize the sections and ensure businesses are able to comply with CCPA requests in the required time frame and within the allowable time extensions. Also, with respect to the deletion right, even though the CCPA requires a business to “disclose and deliver” information within a certain timeframe, there will be no information for the business to “disclose and deliver” to the consumer, because businesses will delete information rather than provide it to a consumer.

IAB therefore urges the AG to clarify how the two extension periods allowed for in the law apply to businesses effectuating consumers’ CCPA requests. We ask the AG to clarify that both extension periods—the 45 day extension mentioned in Section 1798.130 and the 90 day extension mentioned in Section 1798.145—apply where necessary when the business informs the consumer of such extension within 45 days of receiving a CCPA request. We also ask the AG to confirm in its interpretation of the law that that a company does not need to provide any personal

⁵⁷ Cal. Civ. Code § 1798.140(c)(1)(B).

⁵⁸ Cal. Civ. Code § 1798.140(g).

⁵⁹ Cal. Civ. Code § 1798.140(j).

⁶⁰ Cal. Civ. Code §§ 1798.185(a), (b).

⁶¹ Cal. Civ. Code § 1798.130(a)(2).

⁶² *Id.*

⁶³ Cal. Civ. Code § 1798.145(g)(1)

information to a consumer in response to a deletion request. The AG has authority to interpret all of these provisions per his authority to “facilitate a consumer’s or the consumer’s authorized agent’s ability to obtain information pursuant to Section 1798.130,” including taking into account the burden placed on the business.⁶⁴

* * *

We appreciate the opportunity to submit these comments, and we look forward to working with the AG on developing regulations to interpret the CCPA. If you have questions, please contact us.

Respectfully submitted,

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
[REDACTED]

Michael Hahn
Senior Vice President & General Counsel
Interactive Advertising Bureau
[REDACTED]

cc: Michael Signorelli, Venable LLP
Rob Hartwell, Venable LLP

⁶⁴ Cal. Civ. Code § 1798.185(a)(7).

Message

From: Vance Gudmundsen [REDACTED]
Sent: 3/7/2019 4:07:31 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Vance Gudmundsen [REDACTED]
Subject: Comments on CCPA

Thank you very much for considering my comment on behalf of FICO (Fair Isaac Corporation) about the California Consumer Privacy Act (CCPA), which FICO supports.

It appears that CCPA requires covered business to retain personal information for 12 months just so that the business can respond to a consumer request for access to that data. If the business would normally delete that information prior to 12 months in the normal course of its business activities, this requirement exposes the information to additional unauthorized access, and it imposes an additional storage and handling burden on the business.

Perhaps Section 1798.110(d)(1) and (2) are intended to address this situation

1798.110(d) This section does not require a business to do the following:

(1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.

(2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

Note that similar language in Section 1798.100(e) is confusing because of the misplaced comma after the word "transaction", which should follow the phrase "retained by the business".

1798.100(e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

Even with the correction to 1798.100(e), questions arise under 1798.110(d). Would a business be entitled to delete personal information in the normal course of business if it had not sold it? Would a business be entitled to

pseudonymize personal information and then decline to reidentify the information in response to a data access request.

The General Data Protection Regulation (GDPR) has considered and partially solved this problem in GDPR Recital (64), which expressly permits a business to delete personal data if there is no business purpose for retaining it, solely to respond to data access requests:

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

But even Recital 64 isn't the full answer. A California resident should be able to ask if her personal information was shared with a third party before the business deleted any personal information it collected. So, we propose adding a new subsection, which is an amendment to §1798.110(d), as new subsection 1798.110(d)(3):

(3) Retain personal information for the sole purpose of responding to access requests if in the ordinary course of business that information about the consumer is not retained and has not been shared with a third party.

Respectfully submitted,

Vance Gudmundsen, VP

FICO

Vance Gudmundsen

FICO Regulatory Counsel, Data Privacy Officer

[REDACTED]

[REDACTED]

This email and any files transmitted with it are confidential, proprietary and intended solely for the individual or entity to whom they are addressed. If you have received this email in error please delete it immediately.

Message

From: Jerry Desmond Jr. Esq. [REDACTED]
Sent: 3/6/2019 4:52:31 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Attachments: CMAC CCPA Comments 3-6-19.pdf

To whom it may concern:

Attached please find the comments of the Cemetery and Mortuary Association of California [CMAC] in this pre-rulemaking phase as the California Attorney General's Office develops regulations and solicits broad public participation to further the purposes of the CCPA, establish procedures to facilitate consumers' rights under the Act, and provide guidance to businesses for how to comply.

CMAC is a non-profit organization that serves California cemeteries and funeral homes. Upon its foundation in 1931, the association sponsored the California Cemetery Act under the belief that sound protection of consumers and endowment care funds was in the best long-term interest of the industry.

Today, the CMAC membership is comprised of cemeteries and funeral homes of all types; for-profit, not-for-profit, religious and fraternal. The association works to serve ethical cemeteries in a manner that protects and enhances the interests of the families who utilize our services during a most sensitive time of their lives.

Thank you for this opportunity to submit our comments, and please feel free to contact me at any time.

Best,

Jerry Desmond

Executive Vice President

CEMETERY AND MORTUARY ASSOCIATION OF CALIFORNIA

925 L Street, Suite 260

Sacramento, CA 95814



www.CMACcalifornia.org

Comments of the Cemetery and Mortuary Association of California
California Consumer Privacy Act

March 6, 2019

Civil Code Section 1798.185, within the recently-enacted California Consumer Privacy Act [CCPA], requires the Attorney General [AG] to solicit broad public participation and adopt regulations to further the purpose of the Act.

The Cemetery and Mortuary Association of California [CMAC] provides the following comments and requests that the AG provide clarity on several provisions that are important to the ability of the funeral and cemetery industry to comply with the requirements of the Act.

First and foremost, the CCPA's right to request deletion of consumer data poses significant compliance challenges to the funeral and cemetery industry. Health and Safety Code Sections 8110 through 8112 state that the person in charge of any premises on which interments or cremations are made shall keep a record of all remains interred or cremated and of the interment of remains on the premises under his charge, in each case stating the name of each deceased person, place of death, date of interment, and name and address of the funeral director. The law further requires that these records shall at all times be open to official inspection.

CMAC urges the AG to clarify in the regulations that the CCPA does not require cemeteries to delete personal information that they are required by law to maintain.

With regard to specific provisions of the CCPA, CMAC requests that the regulations address the following issues:

1. Please provide acknowledgement that the definition of a Consumer does not include personal information that a business collects regarding that business's employees for employment-related purposes. Including employees within the scope of the CCPA does not align with the spirit of the law, which is designed to protect customers and potential customers that are external to a business and not individuals who are internal to a business.
2. Please provide acknowledgement that the definition of Personal Information does not include Personal Information that a business collects regarding that business's employees for internal use by that business.
3. Please include a good faith clause in the regulations, providing a safe harbor for those businesses that demonstrate that they have employed commercially reasonable efforts to comply with the CCPA or that they have complied with the CCPA in all material respects. This would be helpful in the event that businesses inadvertently miss some hard copy documents or electronic data elements when responding to a verified consumer request. Capturing every single piece of personal information across an entire enterprise will create an undue burden on businesses and unreasonable exposure to liability.

4. Please provide guidance in the regulations on how businesses should verify a consumer request without collecting more information about the consumer and potentially reducing the consumer's privacy.
5. Please specify in the regulations how long a consumer request should be kept on file.
6. Please provide in the regulations an acknowledgement that the consumer right to request disclosure of and/or access to personal information does not apply in the context of ongoing litigation with that consumer or where communication with that consumer or information concerning that consumer is covered by a litigation hold.
7. Please provide clarification in the regulations regarding the process for extensions including the number and time period of extensions that businesses may request in order to comply with each of the following consumer rights afforded under the CCPA: i) a consumer request for disclosure regarding personal information, ii) a consumer request for access to personal information, and iii) a consumer request for deletion of personal information.
8. Please provide clarification on how a business demonstrates compliance with the requirement that a business that receives a verifiable request from a consumer to delete that consumer's personal information must also direct any of that business's services providers to delete the consumer's personal information from the service provider's records.
9. Please provide clarification on how a business demonstrates compliance with the requirement that a business provide electronic data to consumers who request access to such data in a portable format.
10. Modern software systems are dependent on relational databases to operate. It is possible that some consumer requests to delete personal information would cause substantial, and potentially crippling, system failures for businesses. Please provide clarification in the regulations that businesses are exempted from deleting a consumer's personal information if and to the extent that any of this data is required to keep a business's internal systems functioning.
11. Please provide clarification on the dispute resolution or appeal process. Further clarification is also needed on what constitutes a violation.

Message

From: Stuart McNair [REDACTED]
Sent: 3/4/2019 6:27:39 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Flag: Follow up

Thank you for making a platform available for those of us who cannot attend a workshop. This is a daunting process and is greatly concerning to our business and we hope for clarity in the coming months on how we are to operate under these new regulations.

Our business is a recruiting service for truck drivers, mechanics and other positions relating to the trucking industry. As an example, when you are driving down the interstate and see an advertisement on the back of a tractor-trailer that they are looking for drivers that phone number or website listed is run by our company. We have applicants that apply to one or more of our hundreds of recruiting sites in order to find them a job. We are contracted with every major fleet to help them find drivers. When we have an applicant that meets the requirements of that particular company the data is transferred to the company looking to hire a driver. This is no different than any other internet job site.

The concern is that we will have to create websites that are solely dedicated to California applicants or significantly modify our existing websites to accommodate the CCPA rules for opt-out. For our business that would be very burdensome and expensive. It is quite confusing that this is a necessary law for our type of business as we are only gathering information on people who are willingly filling out our forms so we can aid them in finding a job.

It seems there should be an exception in the law for websites where individuals are actively seeking help in finding employment. Has this been discussed? It is not our intention to cause harm to anyone who uses our sites. We do not gather data on random users and only utilize data that has been given to us directly by the party.

Please let me know if there is any additional information that I can provide.

Thank you.

Stuart McNair
Senior Project Manager, Audience
[REDACTED]

Randall-Reilly | 3200 Rice Mine Road NE, Tuscaloosa, AL 35406

randallreilly.com | facebook.com/randallreilly | twitter.com/randallreilly

Message

From: Wright.Gary [REDACTED]
Sent: 2/11/2019 12:43:47 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Flag: Follow up

Recommendation:

I've observed confusion between categories of personal information shown in the Cal Civil code 1798.80 and the definition of Personal Information in 1798.83. I would recommend clarifying the following:

1. In 1798.80 many are disregarding "including, but not limited to" in the definition of Personal information in paragraph (3)
2. In 1798.83, Personal information is better defined and clear. This definition is preferred in the CCPA and more inclusive.

PI defined at the time of disclosure, identified, described, or was able to be associated with an individual, including-but not limited to-27 listed categories

- (i) Name and address.
- (ii) Electronic mail address.
- (iii) Age or date of birth.
- (iv) Names of children.
- (v) Electronic mail or other addresses of children.
- (vi) Number of children.
- (vii) The age or gender of children.
- (viii) Height.
- (ix) Weight.
- (x) Race.
- (xi) Religion.
- (xii) Occupation.
- (xiii) Telephone number.
- (xiv) Education.
- (xv) Political party affiliation.
- (xvi) Medical condition.
- (xvii) Drugs, therapies, or medical products or equipment used.
- (xviii) The kind of product the customer purchased, leased, or rented.
- (xix) Real property purchased, leased, or rented.

- (xx) The kind of service provided.
- (xxi) Social security number.
- (xxii) Bank account number.
- (xxiii) Credit card number.
- (xxiv) Debit card number.
- (xxv) Bank or investment account, debit card, or credit card balance.
- (xxvi) Payment history.
- (xxvii) Information pertaining to the customer's creditworthiness, assets, income, or liabilities.

a.

Gary Wright – HCISPP



HealthCare Information
Security and Privacy Practitioner

Wright Compliance Services

Consultant – CCPA/GDPR Subject Matter Expert



*** Disclaimer ***

This communication (including all attachments) is solely for the use of the person to whom it is addressed and is a confidential AAA communication. If you are not the intended recipient, any use, distribution, printing, or copying is prohibited. If you received this email in error, please immediately delete it and notify the sender.

Message

From: Barbret, John [REDACTED]
Sent: 2/8/2019 10:44:13 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Attachments: JB Statement to CA AG on CCPA - 20190205.pdf
Flag: Follow up

Hello California Attorney General's Office,

Thank you for the opportunity to speak at the forum in Sacramento on February 5th. Attached are the comments I delivered.

I'm happy to follow up if you have any questions.

Thanks again for the opportunity to participate in the rulemaking process.

jb

John Barbret
Privacy Officer

VW Credit, Inc.
1401 Franklin Blvd

Libertyville, IL 60048

United States of America

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**Statement of John Barbret, Certified Information Privacy Professional (CIPP), to the California
Attorney General on the California Consumer Privacy Act
5 February 2019**

Good morning. We've had some great comments today. I'd like to build on them by talking about compliance timeframes.

My name is John Barbret, and I am a Certified Information Privacy Professional (CIPP). I'm here to speak on behalf of all the people who have to build the stuff required by the CCPA. I've been extremely fortunate in that over the course of my career I've worked for many companies in several different industries. This has allowed me to develop a unique perspective on privacy, as well as an understanding of the technical challenges around operationalizing privacy controls.

As a consumer, I strongly support the underlying goals of the CCPA. Privacy is a fundamental social value, one to which I have dedicated my professional career. As recognized, ambiguity in the law has raised concerns, but uncertainty as to *when* changes must be implemented is also a major issue.

As you work through the issues, I ask the AG to consider that the act appears to become operative before companies have had a reasonable amount of time to implement measures required by the regulations. As written, companies are given six months or less to implement requirements of unknown complexity, with no consideration for the level of effort required by the average small to mid-size company.

Proponents of the CCPA often site the GDPR as an example of why they believe the requirement of the new California law are easily attainable. This may be true for large, international companies. However, the CCPA will apply to many small and mid-size *US only businesses*, to which the GDPR has *never* applied.

Additionally, the GDPR was an update of an existing law – the EU Directive – so affected companies were already in “near compliance” with the new GDPR requirements. Unlike the GDPR, the CCPA will require many small and mid-size *US only businesses* to build entirely new programs from the ground up.

Furthermore, companies were given over two years to implement measures required under the GDPR. And the timeline for implementation of the GDPR (and the EU directive) spanned nearly six years from initial proposal to ultimate implementation date. Drafters took into account the complexity of the requirements, and gave companies several years to build systems to meet those requirements.

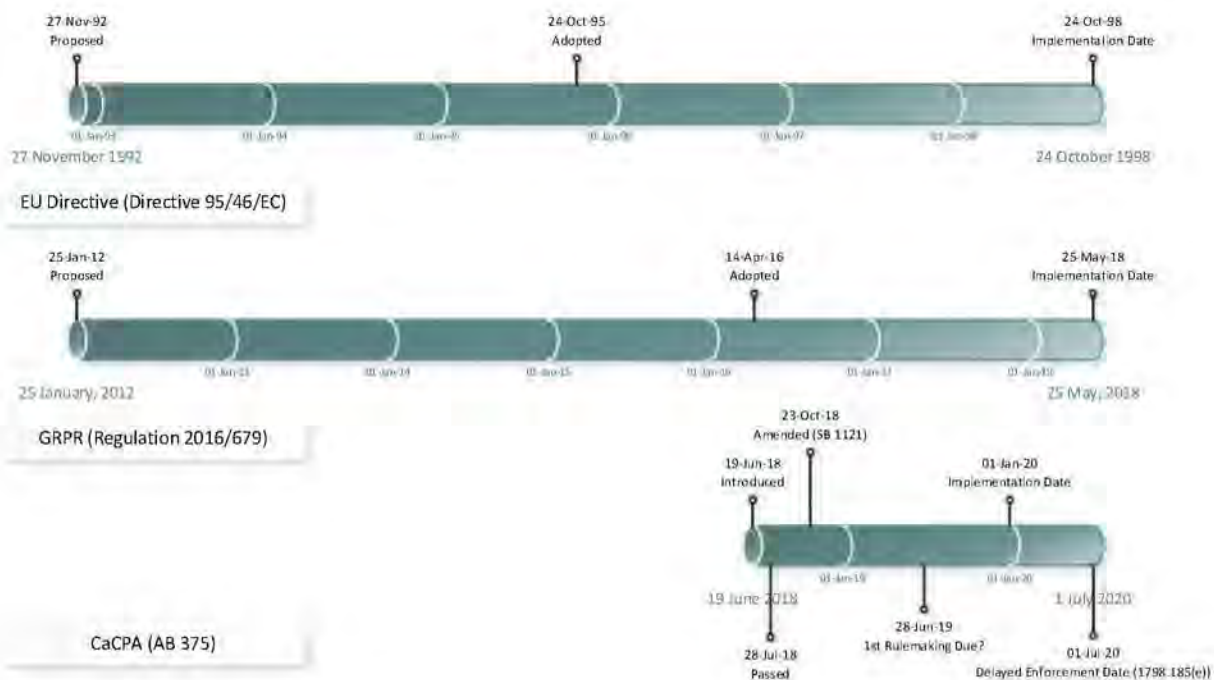


Figure 1: Comparative timeframes for EU and California privacy laws

Again, depending on the complexity of the measures identified in the AG rulemaking, it may take more than the allotted six months to: design, develop, purchase, test, secure, and ultimately implement systems that meet CCPA requirements. For example, just for one piece of the reporting requirement, to make sure we have on hand the data that we've collected and used in the past year, I asked about using existing system logs for one system. The conversation went something like this:

IT: Yeah, we only keep that for 30 days.

ME: Okay, can we just change that to a year?

IT: Yeah, no. We'd need to write new code to log the data you want. That'll make the logs bigger, and there's currently not enough space in the system, so we'll need to redesign the architecture. Oh, and if you're gonna add personal information, we'll need to redesign the security around those logs. And if you wanna to keep a year's worth of data, we'll need to buy new servers to have enough space. That means finding rack space in our data centers, building and configuring new network segments, securing them, and setting up long-term management of those servers. And since we're talking new hardware, we need budget, so purchasing will have to be involved...

ME: Okay, okay, okay. What if we just used the cloud?

IT: Maybe, but we'll still need to purchase that service, build the necessary system interfaces, and need to make sure the cloud vendor will build in the necessary security, which means purchasing & legal will have to negotiate new contracts, and that all takes time too. All in addition to our day jobs...

And that's just for one part of one CCPA requirement.

So I'm here today to ask that each rule specify its own timeline for compliance.

This is an approach that has been taken by US federal regulatory agencies in the past. For example, the FCC's "Robocall Rules" specified different timeframes for compliance with different measures. It gave companies:

- 9 months to implement the abandoned calls rules;
- 11 months to implement an automated, interactive opt-out; and
- 18 months to implement and obtain prior express written consent.

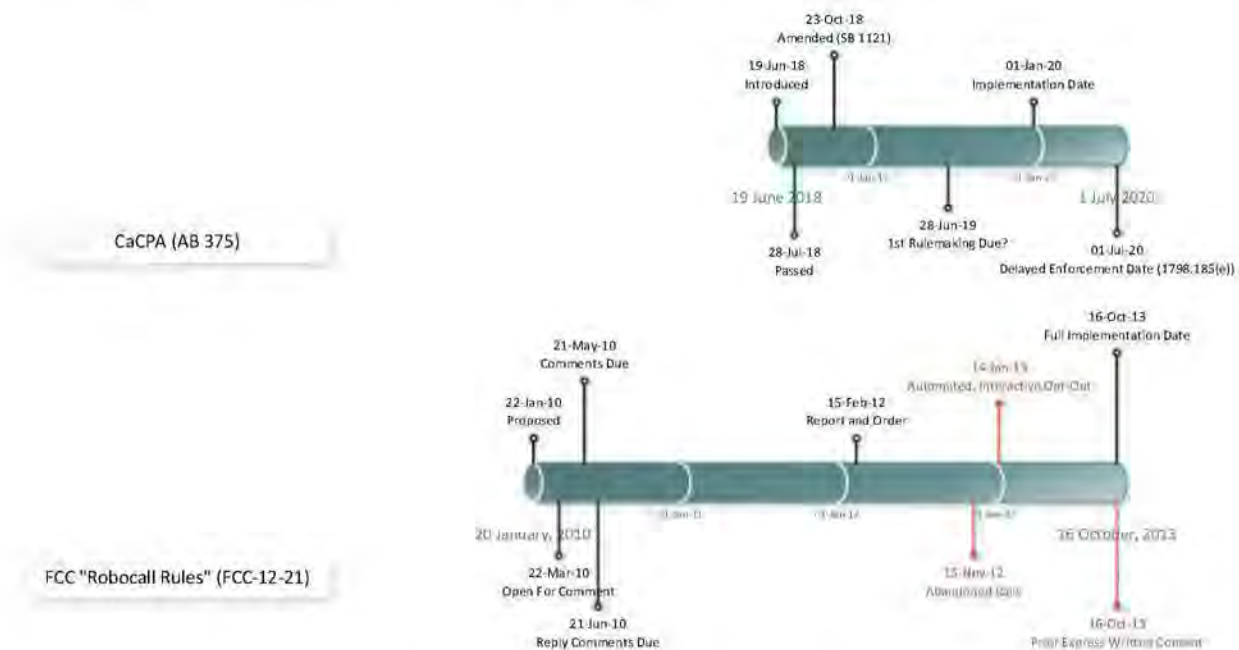


Figure 2: Comparative timeframes for FCC and California regulations

I am committed to meeting the requirements of the CCPA. However, specifying six months to comply with a regulation, absent any knowledge of the complexity of the requirements, seems arbitrary and almost capricious.

Therefore, I respectfully submit that compliance timeframes should be specified by the AG in each rulemaking, based on the demands of a specific rule, that gives companies a reasonable period of time to meet the requirements of that rule.

I'm gonna give it my best shot, but please give me enough time to get it done.

Thank you again for your time today.

John Barbret
Privacy Officer

VW Credit, Inc.
1401 Franklin Blvd
Libertyville, IL 60048
United States of America

Message

From: Steven Boms [REDACTED]
Sent: 2/1/2019 10:11:41 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Attachments: Yodlee AG Comment Letter Final.pdf
Flag: Follow up

Good morning,

Please find attached a submission from Yodlee regarding the CCPA.

Many thanks,


Steven Boms

President

Allon Advocacy, LLC

[REDACTED]

[REDACTED]

 @allonadvocacy

www.allonadvocacyllc.com



February 1, 2019

ELECTRONICALLY SUBMITTED

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 South Spring Street
Los Angeles, CA 90013

Re: Comments on Consumer Privacy in California

To Whom It May Concern:

Investnet Yodlee ("Yodlee") appreciates the opportunity to share our perspective regarding consumer privacy policies in California in response to the California Department of Justice's ("the Department") requests for comments regarding the implementation of the California Consumer Privacy Act of 2018 ("CCPA"). As the leading consumer-permissioned financial account aggregation platform provider globally, with nearly two decades in the industry, Yodlee strongly believes in the ability of technological innovation to empower consumers by increasing competition and providing broader access to technology-based financial tools that drastically improve their financial wellbeing, while adhering to best-in-class privacy and data security standards.

Yodlee is a business-to-business consumer permissioned financial data aggregation and analytics platform headquartered in Redwood City that enables financial institutions and financial technology firms alike to provide consumers with innovative new products and services that can help them improve their finances. These customers use the Yodlee platform to connect millions of retail and small businesses and individual consumers and investors with their own financial data to provide financial wellness solutions. These applications can, for example, provide a single platform to track, manage, and improve consumer financial health across a host of different banks and financial institutions, provide financial advice, and offer expanded access to credit.

Customers also use Yodlee's platform to establish the authenticity of account holders in real time and to improve the real-time affordability checks required by providers of credit. Yodlee's customers include 13 of the 20 largest banks in the United States and top global banks in more than 20 countries, including Bank of America, Goldman Sachs, Wells Fargo, and American Express. Leading global financial innovators like Kabbage and PayPal are also Yodlee's customers.

The Department's request for comments on consumer privacy and data access is timely, as industries across sectors are seeking to collaborate with regulators and policymakers globally as market stakeholders seek to strike the appropriate balance between consumer privacy and innovation in a 21st century economy. This issue is particularly relevant for international firms, like Yodlee, that have been engaged with policymakers globally for the last several years to provide input and expertise into national and continental privacy regimes.

The financial technology industry has created incredible benefits for consumers through innovative financial tools. Yodlee and many of its customers operate in jurisdictions across the globe, each with unique privacy and data regimes, as well as some ecosystems that have implemented Open Banking standards. Accordingly, we endeavor to operate under several high-level universal principles that serve our central mission of delivering benefits to consumers' financial wellbeing in a fully consent-driven model that protects their privacy. These same principals should be applied to any successful data privacy regime in the United States, either at the state or federal level. These principals consist of four core components:

- 1) Consumers must be able to access their financial account data for purposes of using any legitimate application;
- 2) Consumers must provide affirmative consent on the basis of clear and conspicuous disclosure regarding the use of their data;
- 3) All entities who handle consumer account information must adhere to that consent, as well as best practices for security standards and implement traceability/transparency; and
- 4) The entity responsible for a consumer's financial loss must make the consumer whole. All stakeholders in the ecosystem have shared responsibility – this will start with traceability in the United States and move towards shared responsibility.

In order for any digital ecosystem to work effectively, Yodlee believes it is imperative that consumers have the absolute ability to provide their consent to permission and to revoke access to their personal data to third parties of their choosing. Clear and understandable disclosures coupled with consumer consent must be at the foundation of any framework that seeks to ensure strong consumer privacy protections and sound data security. In the absence establishing the consumer's consent as the fundamental building block for such protections – or in a system that allows the consumer's consent to be overridden by any entity that accesses or holds their personal data – the consumer's control of their data has been lost and the ecosystem is not appropriately serving its end users.

In order for all parties in the ecosystem to rely on consumer consent, consent must be tied to an unassailable identity. In the financial context, once the consumer's identity has been verified, consumers must be able to access their accounts, transactions, and other personal data an entity with which they do business holds without obstruction or selective withholding of information. Additionally, with their consent, a consumer should have the ability to responsibly share their own data with other entities and third parties within the ecosystem however they choose in order to receive some benefit from a product or service that relies on that consumer's permissioned data to provide that benefit. Any entity to which the consumer permissions their data should be required to comply with appropriate privacy regulations, and the consumer should understand clearly what data they are permissioning in exchange for receiving a product or service. Furthermore, while Yodlee believes every piece of a consumer's financial data should be made available for that consumer to share with third parties of their choosing, to power the use case of their choice. In the financial services market, these services include lending, financial wellness, financial planning, credit verification, and investing, among many others.

To build an ecosystem in which responsibility for notifying and making consumers whole is easily understood and enforced, further consideration should be given to the institution of traceability as part of any data privacy regime. Traceability conveys that any party accessing a consumer's data with the consumer's permission is identified through technical mechanisms, such as unique, coded headers embedded in the authorization call that the party uses to access the consumer data, as a requirement to provide its service. In a traceable ecosystem, every entity to which a consumer has permissioned their data is identifiable. In the event of a data breach, this chain of identifiers can be used as forensic evidence to trace, with significantly more certainty than exists in systems without traceability, the source of the breach to the party that was responsible for it.

Accountability is a principle that logically follows traceability. A successful framework will implement traceability as a means of ensuring that any party responsible for a breach of consumer credentials is liable for any financial loss incurred by the consumer. Accordingly, Yodlee supports the notion of an ecosystem in which every party that holds consumer data is able to make their customers whole for their direct losses in the event a breach of their systems results in consumer financial loss. In other geographies, this has been accomplished through a combination of capital and minimum levels of liability insurance commensurate with the potential risk each party presents to consumers in the case of a security event. Under a system in which both traceability and accountability are implemented, all parties involved in a breach would be aware of what entity was responsible and would have assurances that the responsible party is held liable for any losses, thus addressing the key hurdle that traditional financial institutions now face under the existing statutory and regulatory framework when their consumers elect to use third-party tools.

One of the systemic disadvantages facing the fintech ecosystem in the United States as compared with many other countries that have imposed standards with regard to consumer-permissioned data access, security, and privacy is the immense relative regulatory fragmentation that exists for the U.S. financial system. There are at least eight federal regulatory agencies with jurisdiction over at least some portion of financial data access in the United States: the Bureau of Consumer Financial Protection, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Federal Reserve Board of Governors, the Securities and Exchange Commission, the Commodity Futures Trading Commission, and the Federal Trade Commission. There are also regulatory authorities in each state that have jurisdiction over entities that play a role in the fintech market, financial services providers and fintech firms alike. A range of industries in the United States encounter a similar fragmentation within the regulatory frameworks that govern them. To the extent possible, Yodlee would respectfully encourage the policymaking community to endeavor to harmonize efforts related to building data security and privacy regimes.

Yodlee is supportive of the notion of a national set of minimum data privacy and control standards that would encapsulate best practices, provided that standard is both enforceable and effective and applied as universally as possible. Furthermore, from an international competitiveness perspective, it is imperative that federal and state policymakers establish a framework that maintains some degree of interoperability with other regimes globally to ensure that American companies – and consumers – do not face an international competitive disadvantage in the years ahead.

California is leading the way at the state-level with these efforts, and accordingly, it is important to consider how to ensure that implementation of the CCPA will prompt future harmonization rather than a continuance of regulatory fragmentation. True harmonization will be achieved when all stakeholders are held to the same standard and operate under the same set of regulations. Comprehensive application will be best achieved through active collaboration and coordination between the private sector and state and federal government agencies with the goal of ensuring strong consumer protections and accountability across all industries.

The landscape of the financial sector is somewhat unique with regard to data privacy and security given the multitude of existing statutes and regulations governing the collection, processing, and storage of financial data. Accordingly, while Yodlee is supportive of a holistic approach, clear guidance is required for how any new privacy regime will interact with myriad existing statutes.

In the financial services sector, decades of existing statute and regulation, including the Bank Secrecy Act and anti-money laundering rules, could require financial firms to retain data for law enforcement or investigatory purposes. A privacy standard that affords, for example, consumers with a blanket “right to be forgotten” or “right to deletion” could very well create a scenario under which a financial firm would be forced to select whether to comply either with existing laws and regulations or the new privacy regime. As another example, the national privacy regime for financial data enacted under the Gramm-Leach-Bliley Act, designed to enforce the account holder’s consent over the use of their data by the financial institution, is sometimes misrepresented to deny consumers the use of their data with other third parties. Accordingly, ensuring harmonization across the existing regulatory framework is crucial to prevent such situations, and Yodlee encourages the Department to consult with federal regulators and policymakers as it seeks to refine such provisions in the CCPA.

As a company that operates in multiple jurisdictions globally, Yodlee has experience operating under many different regulatory frameworks. To the extent that the private sector and other regulatory agencies come together to develop best practices that could be adopted broadly across the financial services sector and other industries, the European Union’s recently-enacted General Data Protection Regulation (“GDPR”) is a framework that U.S. policymakers may look to as a basis for what could work in the U.S. ecosystem.

GDPR, in large part due to its attempt to universally apply to every conceivable use or application of a consumer’s data, takes a very broad view both of what a consumer’s personal data may be and the privacy rules governing that data. Though designed to provide European consumers with complete control over how their data is used, GDPR has the potential to make more difficult some uses cases that provide consumer benefit in the financial services context. In order to inform its own development of privacy proposals, the Department may benefit from monitoring the European market in the months ahead for signs of what provisions are working and where challenges with compliance remain. With thousands of U.S. multinational companies, including Yodlee, already complying with GDPR requirements and with the Federal Trade Commission having acknowledged it will enforce those standards on U.S. companies who have adopted them, it may behoove California regulators and policymakers to further examine this framework for effective consumer protections. Of course, adjustments would be required to determine whether a framework resembling GDPR could work in the U.S. market, especially as

California Department of Justice
February 1, 2019

more individual states seek to implement their own privacy frameworks, and look to California as an example.

Yodlee appreciates the opportunity to provide input on the Department's request for comments and thanks the Department for its thoughtful and exhaustive approach to ensuring a sound, effective, and consumer-focused approach as it promulgates regulations in conjunction with the CCPA. Yodlee hopes the Department finds this input beneficial. We look forward to further collaboration with the Department on its efforts.

Sincerely,

A handwritten signature in black ink, appearing to read 'S. Boms', followed by a long horizontal line extending to the right.

Steven Boms
On Behalf of Yodlee

Message

From: Brooks, Scott [REDACTED]
Sent: 1/28/2019 2:08:51 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Attachments: CCPA Regulations Public Comment_FINAL12519.pdf

Good afternoon,

We wish to thank Attorney General Becerra and his staff for their efforts during the CCPA rulemaking process to hear the diverse opinions of consumers, business, and other interested parties. We feel the public forums you are hosting are an important part of ensuring CCPA regulations are both well thought out and fair minded.

We have previously provided a hard copy of our comments to Jennifer King of the DOJ's staff, but have attached a digital copy for your review.

Please feel free to reach out if you have any questions, comments, or concerns.

Scott Brooks | Quicken Loans

Director, State Government Affairs

Southwestern U.S.

[REDACTED]



Quicken Loans®

January 25, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

Re: *California Consumer Privacy Act of 2018 Rulemaking Process*

To Whom It May Concern:

Quicken Loans is pleased to submit its comments on the *California Consumer Privacy Act of 2018* ("CCPA") rulemaking process. We appreciate Attorney General Xavier Becerra's leadership in holding public forums as it explores CCPA regulations.

BACKGROUND

As background, Detroit-based Quicken Loans is the nation's largest home mortgage lender. The company closed more than \$400 billion of mortgage volume across all 50 states from 2013 through 2017. Quicken Loans moved its headquarters to downtown Detroit in 2010. Today, Quicken Loans and its Family of Companies employ more than 17,000 full-time team members in Detroit's urban core. The company generates loan production from web centers located in Detroit, Cleveland and Phoenix. Quicken Loans also operates a centralized loan processing facility in Detroit, as well as its San Diego-based One Reverse Mortgage unit. Quicken Loans ranked highest in the country for customer satisfaction for primary mortgage origination by J.D. Power for the past nine consecutive years, 2010 – 2018, and also ranked highest in the country for customer satisfaction among all mortgage servicers the past five consecutive years, 2014 – 2018.

Quicken Loans was once again named to FORTUNE magazine's "100 Best Companies to Work For" list in 2018 and has been included in the magazine's top 1/3rd of companies named to the list for the past 15 consecutive years. The company was also named the #1 place to work in technology in 2017 by Computerworld magazine's "100 Best Places to Work in IT," a recognition it has received 8 times in the past 12 years.

COMMENTS

Digital commerce gives consumers more choice and convenience in services than ever before. As they become increasingly tech savvy, protecting consumers' personal information and ensuring confidence to take advantage of benefits of the ever-changing marketplace is crucial. As an internet-based company, Quicken Loans does not follow the traditional "brick and mortar" model. We've proudly built an internet mortgage lending process that is dedicated to the best client experience possible. Our clients' happiness is our #1 priority.

With the passage of the CCPA, we thank AG Becerra for the opportunity to provide comments as the rulemaking process begins. Our comments are divided into two sections: definitions and specific provisions

Definitions

A. Consumer

CCPA defines a consumer under section (g) as “a natural person who is a California resident as defined by Section 17014 of Title 18 of the California Code of Regulations”. In that tax code definition, a resident is “(1) every individual who is in the State for other than a temporary or transitory purpose and (2) every individual who is domiciled in the State who is outside the state for a temporary or transitory purpose”.

This definition in CCPA is problematic because it covers an unidentifiable group of people outside of California. We ask for regulations that softly interpret the definition to be any individual who has identified themselves as a California resident or for whom the business has a California residential address.

B. Personal Information

Section (o)(1) has the broadest possible definition of personal information, calling all information that “identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household” personal information.

This means that physical descriptors such as hair color or height would themselves be considered “personal information”, as it describes a consumer. We ask for regulations to clarify what this means and how it relates to the rest of the Act.

The definition also goes on to state that personal information “includes, but is not limited to...” and lays out 11 separate categories of information. As the definition states personal information is “not limited to” those enumerated categories, it stands to reason that all information outside of the government record information laid out in the exception in (o)(2) is considered “personal information”. While governments do have a large quantity of data on citizens, an equally large quantity of data is already available publicly on the internet but would be seen as personal information under this act. We suggest that the regulation export the definition of public to include widely distributed media, like Regulation P does.

Lastly, this section lists information that is associated with both an individual and a household as being covered under CCPA, but without any clarity as to what constitutes a “household” (family members, roommates, etc.). We would request that the AG’s office in its rule making clarify what a “household” is for the purposes of enforcement of this act.

Provisions

A. Purpose Limitation

Section 1 subsection (b) says “a business shall not collect additional categories of personal information or use personal information collected for additional purposes” outside of the purpose initially disclosed by a business to a consumer either at or before the point of collection.

We ask for clarification on how specific the categories and purpose disclosures need to be. Unclear in the statute, the requirement says businesses (each with their own processes and regulations) must give constant disclosures which could disclose proprietary information in the process, to consumers even if they have not requested said information. Subsection (b) of 1798.100 is rendered moot by subsection (a) which gives the consumer the power to ask for personal information if they so choose, rather than be bombarded randomly with information they may not have asked for, cared about, or be able to understand the purpose of. If a purpose disclosure is desired, subsection (a) should have a purpose disclosure added to it which would give information if the consumer requests it, but without a business having to send out countless unrequested disclosures

B. Verifiable Consumer Request

Section 1, subsection (c) uses the term “verifiable consumer request” for the first time. This phrase appears in multiple provisions of CCPA but with no reference to a mechanism for determining if a request is indeed from the consumer related to the business they are requesting information of.

We ask that regulations allow for requests to be vetted before being submitted to a business. An example of this could be a third party who uses encrypted, web-based forms and Knowledge Based Authentication (KBA) questions to determine the identity of a consumer and the validity of the request for information before alerting the business in question of the request, now having been “verified”. If a company has taken reasonable steps to ensure a request is “verified”, it should have safe harbor from private rights of action if a request is determined to be the result of fraud/identity theft.

C. Access Request Report

Clearly define the portability requirements. As written, the law is vague on the requirements of portability except that the information must be “portable” and in a “readily usable format”.

A company might use software that creates file extensions common in business but may not be seen as "readily usable" by a consumer. This also doesn't take into account file extensions that might be "readily usable" but readable by software that consumers either have to purchase, or are unfamiliar with (by way of example, .docx is a familiar word processing format, but requires the purchase of word processing software like Microsoft Word, or the technical knowledge to either locate and download "open sourced" software or to convert to a format read by software at the consumer's disposal).

D. Look Back Period

Enforcement actions will not take place until the earlier of July 1, 2020 or 6 months after final rules are published. This creates a great deal of uncertainty around creating technology to comply with consumer data requests.

Rather than a large date range for businesses to have radically new technologies in place for both data retention and disclosure, the latest date for final rules should be adopted as the beginning of any and all data retention and disclosure efforts by business. This will ensure all rules and provisions will be codified and businesses will know what they need to comply with and how. All look backs would contain a full 12 months of information on or after July 1, 2021, and would be prorated for requests from July 2, 2020 through June 30, 2021 (so by way of example, a consumer request from December 1, 2020 would only have 5 months of information back to the beginning of required data retention and disclosure of July 1, 2020, but a request from December 1, 2021 would have a full 12 months of information).

Conclusion

We appreciate the opportunity to comment as Attorney General Becerra works through the CCPA rulemaking. We look forward to a continued dialogue with the Attorney General's Office as it examines how to balance consumer protection while allowing businesses to provide services to clients. Should you have any further questions, please contact me at

[REDACTED] or [REDACTED] or Scott Brooks, Director of Government Affairs, at [REDACTED] or [REDACTED].



Gary Weingarden
Senior Counsel
Quicken Loans Inc.

Message

From: Elizabeth Bojorquez [REDACTED]
Sent: 3/8/2019 4:36:45 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Jacqueline Kinney [REDACTED]; Carolyn McIntyre [REDACTED]
Subject: Comments on CCPA
Attachments: CCTA Comments to AG on CCPA 3.8.19.pdf

Good Afternoon,

The California Cable and Telecommunications Association submits these comments pursuant to direction from the Attorney General regarding pre-rulemaking activities to implement the California Consumer Privacy Act.

Thank you,

Elizabeth Bojorquez

California Cable & Telecommunications Association

1001 K Street, 2nd Floor

Sacramento CA 95814

[REDACTED]

[REDACTED]

[REDACTED]



Carolyn McIntyre
President

1001 K STREET, 2ND FLOOR
SACRAMENTO, CA 95814



March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

Submitted via privacyregulations@doj.ca.gov

RE: California Consumer Privacy Act Regulations

The California Cable and Telecommunications Association ("CCTA") submits these comments pursuant to direction from the Attorney General ("AG") regarding pre-rulemaking activities to implement the California Consumer Privacy Act ("CCPA").¹

CCTA is a trade association of member companies that provide video, voice, and Internet service to millions of customers across California. At the outset, CCTA emphasizes that our member companies are committed to protecting customer privacy and currently operate subject to a variety of existing federal and state privacy laws and regulations. Some CCTA members also are subject to the European Union's General Data Protection Regulation ("GDPR"). CCTA has been actively engaged in legislative activity related to the CCPA and has participated in the AG's related public hearings. CCTA's goal has been, and continues to be, working with policy makers, and learning from our customers, to ensure that the CCPA is workable and will effectively improve privacy protections.

CCTA's comments focus on key regulations that are necessary to address the significant operational issues that our member companies face to comply with the new law. It is our hope and belief that a clear understanding by the AG of these issues and the time and resources needed for compliance will result in regulations that will be feasible to implement and protect privacy in the most reasonable, least burdensome and cost-effective manner. To that end, CCTA also plans to submit information to the AG by May 1, 2019, regarding implementation costs and economic impact of the CCPA.

CCTA recognizes that the AG rulemaking activities and the 2019 legislative session are underway simultaneously and that both offer opportunities for improved privacy protection under the CCPA. Several bills already introduced to amend the CCPA, if enacted, could moot the need for some of the regulations CCTA proposes. In some instances, a legislative fix to an issue may be more effective and provide more certainty for businesses and consumers, but

¹ See AG information on CCPA rulemaking activities at <https://oag.ca.gov/privacy/ccpa>.

CCTA nonetheless recommends a regulation under current law at this time. CCTA respectfully requests the opportunity to update its input to the AG to reflect ongoing legislative activities.

I. CCPA and Administrative Procedure Act Direction for AG Regulations

CCTA proposes the regulations described below in recognition of key provisions of the Administrative Procedure Act (“APA”)² that govern the scope of agency rulemaking authority and standards for determining whether regulations the AG adopts are legally valid. These include the following provisions of the Government Code:

Section 11342.1 ... Each regulation adopted, to be effective, shall be within the scope of authority conferred and in accordance with standards prescribed by other provisions of law.

Section 11342.2 Whenever by the express or implied terms of any statute a state agency has authority to adopt regulations to implement, interpret, make specific or otherwise carry out the provisions of the statute, no regulation adopted is valid or effective unless consistent and not in conflict with the statute and reasonably necessary to effectuate the purpose of the statute.

The CCPA expressly directs the AG to adopt regulations to implement the CCPA, including regulations that the AG is *required* to adopt to address issues enumerated in Civil Code Section³ 1798.185(a), and any “*additional regulations as necessary* to further the purposes” of the CCPA, as provided in Section 1798.185(b). Thus, under both the APA and the CCPA, it is necessary to consider the purpose of the CCPA, as reflected in the statutory language and legislative history. As a starting point, the legislative findings adopted with enactment of AB 375 highlight the Legislature’s specific concern with consumer harm caused by large data mining firms.⁴ These findings describe the consumer harm that the CCPA is intended to prevent as follows:

The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm.⁵

The CCPA reflects legislative intent to prevent this potential consumer harm in two ways – by (1) granting consumers rights to protect the privacy of their personal information a business collects, sells, or discloses, and (2) ensuring that the process for consumers to exercise these rights does not create additional privacy risks. The intent to address this second potential harm is reflected in clear legislative direction for the AG to specify requirements for a business to verify any consumer request to access, delete, sell, or disclose personal information. Furthering the

² Government Code Sections 11340 to 11361.

³ All further section references are to the Civil Code, unless otherwise specified.

⁴ AB 375 (Chau 2018), Ch. 55, Stats. 2018, Sec. 2(g).

⁵ Id., at Sec. 2(f).

legislative purpose to prevent consumer harm in both of these scenarios must be a touchstone for each regulation the AG adopts.

The APA further requires an agency to state why each proposed regulation is reasonably necessary to address a specific problem posed by the authorizing statute.⁶ The public benefits of the regulation, and alternatives that may be less burdensome and equally effective in achieving the purpose, must be considered.⁷ In addition, the rulemaking agency is required to consider potential adverse economic impact of each regulation on California businesses and individuals, with the goal of “avoiding the imposition of unnecessary or unreasonable regulations or reporting, recordkeeping, or compliance requirements.”⁸

In addition to the legislative purpose and general APA requirements, specific directives in the CCPA are highly relevant to determining what AG regulations should be adopted to implement, interpret, or otherwise carry out the provisions of the CCPA. For example, the CCPA provides that it is intended to supplement existing federal and state law and that it should be harmonized with other laws when possible, while also acknowledging that federal law may preempt or create conflicts with the CCPA.⁹ While Section 1798.194 provides that the CCPA should be “liberally construed to effectuate its purposes,” other provisions emphasize consumer choice¹⁰ and ensuring that the rights afforded to one consumer do not result in harm to another. Section 1798.145(j) provides that the rights afforded to consumers and the obligations imposed on businesses by the CCPA “shall not adversely affect the rights and freedoms of other consumers.” Section 1798.145(k) similarly provides that these CCPA rights and obligations shall not apply to the extent that they infringe on noncommercial free speech activities protected by the California Constitution.

Moreover, despite the CCPA’s affirmative grant of rights to consumers and imposition of obligations on businesses, Section 1798.145 contains a long list specifying what these obligations shall *not* do and to which they shall *not* apply. These include, for example, not restricting a business’s ability to comply with federal, state, or local laws, and not restricting a business’s ability to collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.¹¹ Regarding the specific issues for which the AG is required to adopt regulations, the CCPA instructs the AG to give consideration to “obstacles to implementation” and “the goal of minimizing the administrative burden on consumers” and “the

⁶ Government Code Section 11346.2(b)(1).

⁷ Id.

⁸ Government Code Section 11346.3(a).

⁹ See Section 1798.196 (the CCPA “is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution”); and Section 1798.175 (the CCPA “is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers’ personal information... [and] should be construed to harmonize” with other privacy laws).

¹⁰ See, for example, Section 1798.192 (prohibiting a contract that waives CCPA rights, but expressly providing that consumers shall not be prevented from choosing to authorize a business to sell their personal information).

¹¹ Section 1798.145(a).

burden on business.”¹² The Legislature acknowledged the potential overwhelming burden on business by providing for flexibility given the “complexity and number” of consumer requests and in the event of a business receiving “requests from a consumer [that] are manifestly unfounded or excessive.”¹³ The Legislature’s recognition of the complexity of the CCPA and uncertainty about precisely what conduct the CCPA actually requires also is evident in Section 1798.155, which authorizes any business or third party to seek guidance from the AG on how to comply with the CCPA. Thus, as this rulemaking proceeds, it is important that the AG consider all of these provisions that highlight implementation obstacles, potential burdens, and uncertainty in combination with the APA’s general requirement that agency regulations be “reasonable.”¹⁴

CCTA’s proposed regulations focus primarily on “verifiable consumer requests,” which is the key construct essential to operationalize CCPA consumer rights and business obligations. Included are proposed regulations on how a consumer or third party submits a request, how a business verifies a request, what personal information and in what form that personal information should be provided to a verified requester, and the timing that governs the obligation of a business to respond to a consumer or third-party request. All of these are essential to further the CCPA purpose – to empower all consumers with a process to protect the privacy of personal information any business has about them, and also to ensure that this process itself does not lead to disclosures that diminish anyone’s privacy. CCTA also addresses a few other key issues, including overall timing for the effective date and enforcement of AG regulations and CCPA obligations.

II. Verification of a Consumer’s Request to Exercise CCPA Rights.

Section 1798.140(y) defines a “verifiable consumer request” as follows:

“Verifiable consumer request” means a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer’s behalf.

Given this definition, along with CCPA provisions that specify business obligations triggered by a “verifiable consumer request,” it is clear that AG regulations must address, at a minimum,

¹² Section 1798.185(a)(1), (2) and (7).

¹³ Section 1798.145(g)(3).

¹⁴ See Government Code Sections 11342.2 and 11346.3(a).

methods of verification and timing of the obligation to respond to a request – both for a request by a consumer and by a third party.

A. Methods of Verification – Consumer Request

Section 1798.175(a)(7), which requires the AG to adopt regulations related to a “verifiable consumer request,” specifies some options for particular methods of verifying a consumer request and emphasizes the goals of minimizing administrative burdens on both consumers and business:

[The AG shall establish] rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer’s or the consumer’s authorized agent’s ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business’s determination that a request for information received by a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business’s authentication of the consumer’s identity....

While this provision calls out a password-protected account as one method of verifying a request, other verification options also are available that will further the legislative purpose of preventing disclosure of personal information to an unauthorized person. Given the wide scope of businesses subject to the CCPA, it is reasonable to provide flexibility and allow businesses to verify requests based on, among other factors, a consumer’s relationship with the business. This relationship varies depending if the consumer is a current account holder, former account holder, someone who is not an account holder but has a business relationship, or the consumer has no relationship with the entity subject to the CCPA. Businesses often develop initial verification and authentication techniques when opening a customer account. But when there is no underlying consumer account, or an account lacks necessary consumer information, verification is more difficult. Each consumer relationship presents different issues that are best addressed with a flexible approach to verification.

In addition, the AG should consider verification methods that many businesses already utilize to comply with other privacy laws. For example, the GDPR and California Shine the Light Law use a mechanism similar to the CCPA’s “verifiable consumer request” to allow consumers to exercise controls over their data.¹⁵ The Children’s Online Privacy Protection Act, which requires that covered entities obtain verifiable parental consent for the collection, use, and disclosure of children’s personal information, does not mandate a specific method of verifying consent, but the Federal Trade Commission has approved several verification methods.¹⁶

¹⁵ GDPR Art. 15-22; Section 1798.83.

¹⁶ 16 CFR 312.5.

Allowing a business to comply with the CCPA verification requirement with similar methods that meet the requirements of other laws would be reasonable, minimize the burden of having to create new methods, and harmonize the CCPA with other state and federal laws.

In addition to authorizing flexibility, the AG regulation should provide businesses some protection from liability if an unauthorized disclosure occurs even while verifying a consumer request with a permissible method. Section 1798.140(y) expressly provides that a business is not obligated to disclose personal information to a consumer if the business cannot verify the requester pursuant to AG regulations. Thus, it follows that, if a business does disclose information by verifying a request in compliance with AG regulations, then the business should be protected from liability. Moreover, whatever method of verification is utilized, it should be permissible for a business to request additional information from a consumer making a request if the business has any doubts about the requester's identity based on the initial information provided. Based on these considerations, CCTA recommends the regulation below.

Proposed Regulation – Verifiable Consumer Request -- Method

(x) (1) A business is not obligated to disclose information in response to a request from a consumer unless the business can verify that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by a consumer to act on that consumer's behalf, which shall be deemed a "verifiable consumer request."

(2) A business shall verify a consumer request using a reasonable, documented method that takes into account the business relationship with the consumer, which may include a self-service portal for consumers to view or extract their personal information. A business maintaining consumer accounts may assume that a consumer request submitted through a password-protected account maintained with the business is sufficient to be deemed a "verifiable consumer request." A business not maintaining consumer accounts may use personal information supplied by consumers in the self-service portal to verify their identity through the use of a third-party identity verification service.

(3) If a business cannot verify the identity of the requester from the information initially submitted to conclude that it is a "verifiable consumer request," the business may request additional information from the consumer.

(4) A verification method shall be *per se* reasonable if it includes at least one of the following:

(A) Verification of identity through the collection of a government-issued identification.

(B) Verification of identity through use of personal information provided by the consumer or the person authorized to make a request on behalf of a consumer.

(C) Verification of identity through the use of a third-party identity verification service.

(5) [third-party consumer requests – see below]

(6) A business that complies with this [regulation] shall not be held liable, in any action by the Attorney General or other enforcement authority or in any private action under the CCPA or related data breach notification laws, for the unauthorized disclosure of personal information in response to a consumer request under the CCPA.

B. Methods of Verification – Third Party Request

In addition to a consumer request related to the requester's own personal information, the CCTA allows a request on behalf of a third party in Section 1798.135(c), which provides as follows:

A consumer may authorize another person solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General.

As set forth above, Section 1798.140(y) expressly provides that a business is not obligated to disclose personal information to a third-party requester if the business cannot verify, in compliance with AG regulations, that the requester is authorized by the consumer whose personal information is the subject of the request. Thus, CCTA recommends the regulation below as an additional paragraph (5) to specify methods for a business to verify a third-party requester.

Proposed Regulation – Verifiable Consumer Request – Method – Third Party

(5) For determining whether a request made on behalf of another consumer is a “verifiable consumer request,” the requester shall be required to demonstrate that the other consumer has knowingly and specifically authorized the requester to make a request regarding that other consumer's personal information. The following shall be *per se* reasonable as a verification method:

(A) Requiring a requester to be registered with the California Secretary of State as an agent of the other consumer with registration that includes authority to make a request related to disclosure of the other consumer's personal information.

(B) Requiring a requester to provide proof of appointment as the other consumer's legal guardian, fiduciary, or similar legally authorized and recognized person.

C. Timing of Compliance Requirement – Consumer Request

The following CCPA provisions affect the timing of when a business subject to the CCPA is required to respond to a consumer request:

- Section 1798.198(a) provides that the CCPA shall be operative January 1, 2020.
- Section 1798.185 requires the AG to adopt regulations on or before July 1, 2020, including regulations that are *required* to address specified issues, and any “*additional regulations as necessary* to further the purposes” of the CCPA.
- Section 1798.185(a)(7) provides that AG regulations are *required* to specify the form and procedures for consumers to submit a request to a business and the rules and procedures for a business to determine that a request received is a “verifiable consumer request.”
- Section 1798.140(y) defines “verifiable consumer request” as a request by a consumer (or consumer on behalf of a minor) “that the business can reasonably verify, pursuant to regulations adopted by the Attorney General” as required by Section 1798.185(a)(7).

These sections, and the overall statutory scheme, provide that any CCPA obligation of a business to respond to a consumer request is not triggered until *after* the AG has adopted regulations to specify how a business can determine if it is a “verifiable consumer request.” It would thus be contrary to the plain language of the CCPA, as well as unreasonable and contrary to the purpose of the CCPA, to require a business to respond to a consumer request *prior* to the AG adopting regulations on a “verifiable consumer request.” The legislative history of the CCPA and discussion at AG public forums and recent legislative hearings describe how critical verifying a consumer request is to furthering the privacy protection purposes of the CCPA. Disclosure by a business of requested personal information without verification pursuant to AG regulations could violate other laws and “adversely affect the rights and freedoms of other consumers,” which the CCPA expressly provides it shall not be interpreted to do.¹⁷

However, notwithstanding the clear provisions noted above, it is possible that some may claim that CCPA’s operative date of January 1, 2020 obligates a business to respond to a consumer request at any time after that operative date, even if final AG regulations are not adopted and in effect. Thus, CCTA recommends that the AG adopt the regulation below to clearly implement the statutory scheme, avoid the harm the CCPA is intended to prevent, and provide certainty to both consumers and business as to the timing of the obligation to respond to a consumer request.

¹⁷ Section 1798.145(j).

Proposed Regulation – Verifiable Consumer Request -- Timing

(x) Any obligation of a business imposed by the CCPA to respond to a consumer request shall apply only after the adoption and effective date of final regulations that specify the rules and procedures for a business to determine that a request received is a “verifiable consumer request.”

D. Timing of Compliance Requirement – Third Party Request

Similar to the CCPA express statutory language requiring that a “verifiable consumer request” be determined pursuant to AG regulations, Section 1798.135(c) specifies that a business shall comply with an opt-out request received from a person authorized to act on another consumer’s behalf “pursuant to regulations adopted by the Attorney General.” The consumer harms and loss of privacy from unauthorized disclosure of personal information identified in legislative findings could easily result in the case of third-party requests. The Legislature clearly expressed an intent that a business follow specific direction from the AG to ensure such unauthorized disclosures are not made to a person not authorized by a consumer. Thus, CCTA recommends that the AG adopt the regulation below.

Proposed Regulation – Third-Party Consumer Request -- Timing

(x) Any obligation of a business imposed by the CCPA to respond to a consumer request to opt-out of the sale of the consumer’s personal information, when that request is made on behalf of the consumer by a third party, shall apply only after the adoption and effective date of final regulations that specify the rules and procedures for a business to determine that the third party is authorized to make the request on behalf of the consumer.

III. Lookback Period for Information Subject to Disclosure

Section 1798.130 establishes the so-called “lookback” requirement by specifying that information a business is required to disclose in response to a “verifiable consumer request” shall include information covering “the 12-month period preceding the business’s receipt of the verifiable consumer request.” This means that a request for identification of categories of personal information or specific pieces of personal information collected by a business about the requesting consumer applies to all personal information collected in the preceding 12 months¹⁸ and a request to identify categories of personal information sold or disclosed by the business applies to all categories of personal information sold or disclosed in the preceding 12 months.¹⁹

As discussed above, the obligation of a business to respond to a consumer request is not triggered until after the AG adopts final regulations specifying how a business is to determine what is a “verifiable consumer request.” While the timing of the adoption and effective date of AG regulations is uncertain at this time, that date will almost certainly be less than 12 months

¹⁸ Section 1798.130(a)(3).

¹⁹ Section 1798.130(a)(4).

after the CCPA’s operative date of January 1, 2020. Thus, to account for this short-term potential gap where a lookback period would be less than 12 months from the operative date, CCTA recommends the regulation below.

In addition, there is some potential ambiguity as to whether the 12-month period begins on the date the business *receives* the consumer request, or the date the business *verifies* the request. Section 1798.130(a)(2) provides that a business “shall promptly take steps to determine whether the request is a verifiable consumer request” but does not define “promptly.” Until the AG adopts regulations on how to determine if a request is a “verifiable consumer request,” it is uncertain how long the required verification process may take. However, Section 1798.130(a)(2) also requires disclosure of the requested information to the consumer “within 45 days of receiving a verifiable consumer request.” For counting the 45 days, the provision is specific in stating that the time needed to verify the request “shall not extend the business’s duty to disclose and deliver the information within 45 days of *receipt* of the consumer’s request.” Thus, in the interest of clarity and certainty for counting the 12-month period, it is reasonable and consistent with the specific language on the 45 days to also count the 12 months from the date of *receipt* of the request. CCTA’s recommended regulation below follows this interpretation.

Proposed Regulation – 12-Month Lookback -- Timing

- (a) To calculate the 12-month period relating to the obligation of a business to disclose information to a consumer covering the 12-month period preceding the business’s receipt of the verifiable consumer request, the preceding 12 months shall be counted from the date the business receives the request, regardless of the time required to verify the request.**
- (b) To calculate the 45 days relating to the obligation of a business to disclose information to a consumer within 45 days of receiving a verifiable consumer request, the 45 days shall be counted from the date the business receives the request, regardless of the time required to verify the request.**

IV. Disclosure of Specific Pieces of Personal Information

The CCPA requires a business to disclose “specific pieces of personal information” about a consumer in the following provisions:

Section 1798.100(a) A consumer shall have the right to request that a business that collects a consumer’s personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

Section 1798.110(a)(5) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following... the specific pieces of personal information it has collected about that consumer.

Section 1798.110(c)(5) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of

subdivision (a) of Section 1798.130.... the specific pieces of personal information the business has collected about that consumer.

For this purpose, “specific pieces of information” could include highly sensitive information such as social security numbers, credit card numbers, and health information. While this information is routinely collected for a valid business purpose, transmitting it in response to a consumer request can create cybersecurity risks and, in the event of a data breach, create the very harm the CCPA is intended to prevent. There is also some risk of unauthorized disclosure even with compliance with AG regulations on a “verifiable consumer request.” CCTA urges the AG to consider options for minimizing this risk, which could include allowing a business to confirm with the requester, once verified, that specific pieces of information are held by the business rather than transmitting the actual information.

V. Exceptions to CCPA for Intellectual Property

Section 1798.185(a)(3) requires the AG to adopt regulations “necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights.” This direction is consistent with Section 1798.196, which provides that the CCPA shall not apply if preempted by, or in conflict with, federal law. A CCPA exception for intellectual property is necessary to ensure that an obligation to comply with a verifiable consumer request does not jeopardize intellectual property protected by other laws. Copyright, patent, service mark, and trade secret laws protect intellectual property, including any formula, pattern, compilation, program, device, method, technique, or process developed to process or analyze personal information, and any information derived from such process or analysis. A consumer’s request to delete or disclose personal information could result in loss of protected intellectual property. The lack of an intellectual property exception creates a disincentive for business innovation and technological progress that frequently lead to intellectual property rights. Thus, to protect intellectual property and ensure California remains a leader in innovation, CCTA recommends that the AG adopt the regulation below.

Proposed Regulation – Intellectual Property Exception

(x) Any obligation of a business imposed by the CCPA shall not apply if it would result in loss or infringement of intellectual property of that business subject to copyright, patent, service mark, or trade secret protection, including any formula, pattern, compilation, program, device, method, technique, or process developed to process or analyze personal information, and any information derived from such process or analysis.

VI. Notice to Consumers of CCPA Rights Regarding Personal Information

The CCPA directs the AG to adopt “rules, procedures, and any exceptions necessary” to ensure that customer notices required by the CCPA are “provided in a manner that may be easily understood by the average consumer,” among other requirements.²⁰ AG regulations that specify

²⁰ Section 1798.185(a)(6).

such rules, procedures, and exceptions to CCPA notice requirements must further the legislative purpose of protecting consumers' "right to know,"²¹ while also considering what is reasonable, most effective in furthering this right, and least burdensome for the broad range of businesses subject to the CCPA.

A. Notice of Personal Information Collected

Section 1798.100(b) specifies a general consumer notice requirement as follows:

A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

The manner in which each business provides this required notice so as to effectively reach an average consumer may vary depending on the business model. Many transactions that result in collection of personal information occur online and in the context of a customer relationship, making online privacy policies, with which consumers already are familiar, an effective manner of complying with this notice requirement. For transactions in a physical space or without a customer account, such as at an amusement park or movie theater, an online privacy policy, combined with a directive to see the online policy posted at the ticket sale location, may also be the most reasonable and effective way to ensure that the average consumer is notified of the required information. Accordingly, CCTA recommends that the AG adopt the regulation below.

Proposed Regulation – Consumer Notice on Information Collected

(x) (1) A business shall be deemed in compliance with Section 1798.100(b) if the business includes the information specified in this notice requirement in its online privacy policy.

(2) A business without an Internet web site shall be deemed in compliance with Section 1798.100(b) if it posts the information specified in this notice requirement in a clear and conspicuous location at its place of business.

B. Notice of Do Not Sell Right

A business subject to the CCPA that sells consumers' personal information to third parties is required by Section 1798.120 to notify consumers of the right to opt-out of this sale of their information.²² The key sections provide as follows:

²¹ SB 375 Sec. 2, (i)(1) and (2).

²² Section 1798.115(d), 1798.120(b), and 1798.135(a).

Section 1798.135(a)(1) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:... [p]rovide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

1798.135(b) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

These provisions reflect legislative intent to accommodate reasonable options for the manner of providing the required notice with consideration of existing business practices, such as an account relationship with a consumer and how a business establishes its web pages to effectively communicate with the public and its customers. Similarly, current business practices with online privacy policies should be considered in AG regulations, especially given that consumers already are familiar with these policies to learn about their privacy rights. Allowing the option of compliance through an online privacy policy is consistent with the CCPA's broad directive to establish notice requirement "rules, procedures, and any exceptions necessary." Moreover, this flexibility would further the legislative purpose of protecting the consumers' right to know – in this case the right to know about the right to opt-out – by authorizing notice to be provided in a manner readily available and familiar to the average consumer.

In addition, the AG should further clarify the options in Section 1798.135(b) to reflect the commonly used reference to a website's "initial landing page" as the location most accessible to the average consumer for receiving a notice. Thus, CCTA recommends the regulation below.

Proposed Regulation – Consumer Notice on Do Not Sell Right

(x) A business shall be deemed in compliance with the notice requirement in Sections 1798.120(b) and 1798.135(a) if the business includes the required information on the right to opt-out of the sale of personal information on its website initial landing page or in its online privacy policy.

VII. Effective Date of AG Regulations and Enforcement

Several provisions of the CCPA relate to the timing for adoption and enforcement of AG regulations and reflect the Legislature's concern for the complexity and uncertainty as to specific conduct that could constitute a violation of the new law.

- Section 1798.185 requires the AG to adopt regulations on or before July 1, 2020, and specifies that certain key regulations will need updating to address “obstacles to implementation,” among other concerns.²³
- Section 1798.185(c) provides that the AG shall not bring an enforcement action under the CCPA until six months after the publication of final AG regulations, *or* July 1, 2020, *whichever is sooner*.
- Section 1798.155(a) provides that “[a]ny business or third party may seek the opinion of the Attorney General for guidance on how to comply with the [CCPA].”
- Section 1798.155(b) provides that a business will be notified of alleged noncompliance and then have 30 days to cure before the business is subject to an enforcement action for violating the CCPA.

Several issues presented by these provisions need interpretation in AG regulations. First, given the use of “or” in Section 1798.185(c), it provides that the AG *could* bring an enforcement action any time after July 1, 2020, even if that date is less than six months after publication of final AG regulations – and even if AG regulations are not adopted at all by that date. However, this would be an absurd result, especially in light of CCPA provisions that make certain obligations on businesses applicable only *after* AG regulations are adopted such as regarding a “verifiable consumer request,” as discussed above. Moreover, Section 1798.185(c) does not require enforcement starting July 1, 2020; it merely does not prohibit enforcement after that date. Thus, CCTA recommends that the AG adopt the regulation below to state its intent to not bring an enforcement action until six months after the publication of final AG regulations.

Second, the statute does not directly state the actual effective date of the AG regulations, -- the date by which compliance is required and when failure to comply could constitute a violation. While an enforcement action may not commence until six months after publication of AG regulations, it would be unreasonable to expect compliance starting on the same date final regulations are published. Moreover, the APA specifies that agency regulations generally become effective on a quarterly basis and no less than two calendar months after final regulations are filed with the Secretary of State unless, among other reasons, the authorizing statute specifies otherwise.²⁴ In this case, the CCPA specifies a 6-month *enforcement* date, which is reasonable to construe as being the same as the *effective* date of the regulations under the language of the APA. Thus, CCTA’s recommended regulation below specifies an effective date of the regulations when compliance is required.

Third, the statute does not specify how the right of a business to seek an opinion from the AG on compliance intersects with the timing of a potential enforcement action. Given the Legislature’s clear recognition of the need for AG guidance, it would undermine this intent and

²³ Section 1798.185(a)(1) and (2).

²⁴ Government Code Section 11343.4.

be unreasonable for a business to be subject to an enforcement action while awaiting AG guidance pursuant to Section 1798.155(a). On the other hand, to avoid any potential for abuse of this provision to avoid enforcement, it is reasonable to infer a good faith standard for a business invoking this right to seek AG guidance. Thus, CCTA's recommended regulation below provides for implementing this provision as it relates to AG enforcement.

Proposed Regulation – Effective Date of AG Regulations and Enforcement

- (a) These regulations implementing the CCPA shall take effect and compliance shall be required no later than six months after publication of final regulations.**
- (b) (1) The Attorney General may bring an enforcement action under the CCPA and these regulations at any time starting six months after publication of final regulations, subject to additional requirements pursuant to paragraphs (2) and (3).**
 - (2) The Attorney General may bring an enforcement action against a business for an alleged violation of the CCPA and these regulations no sooner than 30 days after the business receives notification from the AG of alleged noncompliance.**
 - (3) The Attorney General may not bring an enforcement against a business based on conduct for which that business has, in good faith, submitted a request to the AG for an opinion on guidance as to whether that conduct complies with the CCPA.**

CCTA appreciates the opportunity to submit these preliminary comments and looks forward to participating in the formal rulemaking. In addition, as noted above, CCTA requests an opportunity to update these comments as needed to reflect legislative changes to the CCPA. Please contact me with any questions or if you would like a briefing on technical and operational issues related to cable providers' compliance with the CCPA.

Respectfully submitted,

Carolyn McIntyre

Carolyn McIntyre
CCTA President

Cc: Jacqueline R. Kinney, CCTA Senior Vice President and General Counsel

Message

From: Richard DeWaele [REDACTED]
Sent: 1/25/2019 12:48:16 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA

Thank you for your efforts to hold public forums and establish this email box to accept comments to the CCPA.

Given my experience with GDPR regarding drafting, negotiating and revising data processing addendums with numerous suppliers, distributors and customers, I would like the Attorney General to consider issuing as part of the regulations model clauses, standard templates, web site notices and other related documents such as privacy policies and privacy statements which are compliant with the CCPA. Businesses will then be able to can easily implement the law with documents that all parties can agree are standard, official documents which meet the requirements of the law.

Best regards,

Rich DeWaele

Richard M. DeWaele | [Senior Business Attorney](#)

Registered In-House Counsel

Contracts and Legal Services

Esri | 380 New York Street | Redlands, CA 92373 | USA

[REDACTED]
email: [REDACTED] www.esri.com

PRIVILEGED AND CONFIDENTIAL: The preceding message and all attachments thereto are only for use of the intended recipient(s), and may contain information that is confidential or legally privileged. If you have received this message in error, please notify me by return email at

CCPA00000518

[REDACTED] and then delete this message immediately without retaining any copies or other record of its contents. Thank you for your cooperation.

Message

From: Arguelles, Emma [REDACTED]
Sent: 3/8/2019 3:29:51 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA

Comments for consideration in the category of a company's activities that should be ruled as exempt from CCPA. Healthcare organizations, health plans, and hospitals engage in credentialing and/or privileging activities to evaluate the qualifications and legitimacy of medical professionals. Credentialing, re-credentialing and ongoing monitoring of network providers are critical quality control mechanisms that contribute to the overall quality improvement philosophy that healthcare services are delivered safely and with high quality to members of the Company. Privileging entails the process of authorizing a medical professional's scope of patient care services. These activities conform with the intentions of Title IV of the Health Care Quality Improvement Act of 1986 (HCQIA) – encouraging good faith professional review activities. There are several governing and regulatory bodies like The Joint Commission, Centers for Medicare and Medicaid Services, National Committee for Quality Assurance (NCQA) that provide guidance on how these activities should be conducted along with accrediting entities like NCQA that audit actual performance. Health Plan credentialing activities by definition collect personal information at the request from medical professions interested in joining the company's provider networks. The point of collection is directly from medical professionals. The Health Plan will engage with full transparency in primary source verification going straight to the source of specific credentials (education, training, licensure) with the full knowledge and permission of the medical profession. The information is maintained with the highest confidentiality and several security mechanisms are in place to ensure access is restricted and information is protected in accordance with Title 42 ,Chapter IV, Subchapter B, Part 422 – Medicare Advantage Program Subpart E—Relationships With Providers. There is no loss of privacy to the medical professional or control over their information and the company is using the information in a lawful manner that is compatible with the context in which the medical professional provided the information. Credentialing activities should be exempt/excluded from CCPA.

CONFIDENTIALITY NOTICE: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information or may otherwise be protected by law. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message and any attachment thereto.

Message

From: Herrera, Yvette G. [REDACTED]
on behalf of Recht, Philip R. [REDACTED]
Sent: 2/13/2019 12:05:49 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA [MB-AME.FID2260852]
Attachments: 2568_001.pdf
Flag: Follow up

Philip R. Recht
Partner in Charge
Mayer Brown LLP

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

350 S. Grand Avenue, 25th Floor
Los Angeles, CA 90071
www.mayerbrown.com

 Please consider the environment before printing this email.

This email and any files transmitted with it are intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. If you are not the named addressee you should not disseminate, distribute or copy this e-mail.

Mayer Brown is a global services provider comprising an association of legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian partnership).

Information about how we handle personal information is available in our [Privacy Notice](#).

February 13, 2019

BY U.S. MAIL & EMAIL

The California Department of Justice
Attn: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

F: +1 213 625 0248
www.mayerbrown.com

Philip R. Recht

Re: Matters for Inclusion in CCPA Regulation

To whom it may concern:

Our firm represents a variety of companies that provide background report, e-commerce fraud detection, and other people search services. These services are widely used and highly valued by law enforcement, other government agencies, private businesses, and individuals and families alike. Unlike businesses that collect personal information directly from consumers, these companies (a) collect information about consumers only from public and other third party sources, and (b) do not otherwise have direct relationships or accounts with the consumers whose personal information they collect and make available. Below we discuss a number of matters that require regulatory illumination by the Attorney General (AG) so as to make the California Consumer Privacy Act (CCPA) workable for these and other companies without direct consumer accounts or relationships.

I. Notice of collection and sale of personal information. The CCPA requires covered businesses to provide consumer notice in two instances—first, at or before the collection of a consumer's personal information (PI), at which point consumers must be informed of the categories of PI collected and the purposes for which they are to be used (Civil Code section 1798.100(b))¹; and second, before selling a consumer's PI to a third party, at which point consumers must be provided the right to opt out of (i.e., prevent) the sale (section .115(d)).

The manner in which businesses may provide the pre-sale notice required by section .115(d) is specified in the CCPA. Specifically, section .120(b) provides that covered businesses shall provide such notice in accordance with section .135. That section, in turn, provides that the opt-out notice must be provided on a business' Internet homepage and in online privacy policies. However, nothing in the CCPA indicates how businesses may or must provide the pre-collection notice under section .100(b).

As a practical matter, businesses that do not collect information directly from, and do not otherwise maintain direct relationships or accounts with, consumers lack the ability to provide individualized notices directly to consumers. This is particularly the case at or before the

¹ Hereinafter, all statutory references will be to subsections of Civil Code Section 1798 unless otherwise indicated.

The California Department of Justice
February 13, 2019
Page 2

collection of a consumer's information. At that point in time, the businesses lack any information, contact information and otherwise, about a consumer. As such, the best and only way these companies can provide pre-collection notice under section .100(b) is on their Internet homepages.

Notice in this fashion is appropriate for various reasons. It is consistent with the manner in which the CCPA mandates pre-sale notice under section .115(d). It equally is consistent with the manner in which consumers typically search for Internet company disclosures, including those concerning company privacy policies and practices. This fact is reflected in the CCPA's broad definition of "homepage" (section .140(l)), which includes an introductory page of an Internet web site, as well as a download page, a link within an app, an "about" or "information" page, or any other location that allows consumers to review the notice required by section .135(a).²

The AG should include clarification in the regulations that businesses without direct consumer accounts may provide the pre-collection notice required under section .100(b) on their Internet homepages. The CCPA specifies in section .185(a)(6) that the manner in which businesses provide required notices under the CCPA is a topic to be covered by the regulations. Given the CCPA's silence on the point, the CCPA inherently is uncertain as to how companies without direct consumer relationships or accounts may properly provide notice under section .100(b). Finally, Internet homepage notice is not only the only practicable manner for these businesses to provide such notice, but is consistent both with the CCPA's approach on notice under section .115(d) and with consumer behavior.

II. Verification of consumer identity re consumer request and PI determinations. Sections .110 and .115 of the CCPA require covered businesses to provide consumers certain information concerning the businesses' collection and sale of consumers' PI, as well as reports up to twice a year containing the specific pieces of PI collected about consumers, all upon receipt by the businesses of a "verifiable consumer request." The CCPA also requires a covered business to refrain from selling the PI of a consumer who has provided "opt out" notice to the business through a link on the business' Internet homepage.

As the CCPA makes clear, however, a business is not obligated to provide the information and reports required under sections .110 and .115 unless the business can verify, based on the regulations to be adopted by the AG, that the consumer making the request is, in fact, the consumer about whom the business has collected information or is a person authorized by the consumer to act on the consumer's behalf. Section .140(y). While the CCPA does not use the term "verifiable consumer request" to describe an opt-out request, it seems clear that a business equally is not obligated to comply with an opt-out request unless the business can confirm the identity of the person opting out.

² Section .140(l) actually refers to section .145. However, this is an obvious typo. The reference clearly is meant to be section .135(a).

The California Department of Justice
February 13, 2019
Page 3

For businesses with direct consumer accounts, verifying the legitimacy of a consumer information or opt out request can be a relatively simple undertaking. As acknowledged in the CCPA (see section .185(a)(7)), direct consumer accounts can be equipped with password protection and other features that serve to verify consumers' identities. However, the same is not true for businesses without direct consumer accounts. These companies cannot rely on passwords or other security measures established in advance by the consumers making the requests. Moreover, the CCPA prohibits businesses from requiring consumers to create accounts to exercise opt-out rights. Section .135(a).³

For many years, businesses like those we represent have been ahead of federal, state, and local law, voluntarily allowing consumers, at no cost, to search their websites, receive a summary of the PI collected about them by the businesses, and opt-out of the sale of that information. The CCPA's requirements that these businesses provide information concerning their collection and sale of consumers' PI, as well as reports up to twice a year containing the specific pieces of collected PI, all upon receipt of a "verifiable consumer request," convert this heretofore voluntary activity into a mandatory duty of significantly broader scope. Moreover, failure to properly comply with these responsibilities subjects businesses to liability.

To meet these new legal obligations, a covered business without direct consumer relationships needs to be able to request PI from consumers submitting verifiable consumer requests for two equally important purposes. First, as discussed, such a business may need further information to confirm the requesting consumer is who he/she claims to be. Second, the business may need additional information to determine if data in the business' databases relates to this particular consumer and, thus, constitutes the consumer's PI. Without the ability to verify the identity and certain distinguishing characteristics of the consumer (e.g., whether the consumer is the Tim Smith living in Los Angeles or the other Tim Smith living in San Diego), a business cannot properly determine whether data can be reasonably linked to or associated with a particular consumer so as to constitute the consumer's PI. See discussion in III below

The CCPA acknowledges that covered businesses will be able to, and will, obtain additional PI from consumers to verify opt out requests. Specifically, section .135(a)(6) provides that a business may only use PI collected from a consumer in connection with the submission of that consumer's opt-out request, solely for the purposes of complying with such request.

The AG's regulations should similarly make clear that businesses without direct consumer accounts will be able to obtain such additional PI as is necessary to confirm the authenticity of verifiable consumer requests. The CCPA explicitly requires the AG to include in its regulations a mechanism for consumers who do not maintain direct accounts with a business to request information through the business' authentication of the consumer's identity. Section .185(a)(7).

³ The CCPA does not prohibit businesses from requiring the creation of accounts to otherwise verify consumer requests.

The California Department of Justice
February 13, 2019
Page 4

So, this is a mandatory topic for the regulations. As a practical matter, businesses without direct consumer accounts cannot properly authenticate consumer requests (and thus honor consumer requests for information concerning and reports containing their collected PI) absent the ability to obtain such additional PI. Finally, the ability to obtain additional PI to authenticate verifiable consumer requests is consistent with CCPA's allowance for same in the case of verifying opt-out requests.

Given that businesses also need the ability to verify the identity and distinguishing characteristics of consumers to properly determine whether certain data constitutes their PI (and thereby avoid over- or under-disclosing that PI when requested to do so by consumers—again, see discussion in III below), the AG regulations should equally make clear that businesses of all kinds are able to request additional information from consumers for purposes of determining the scope of their PI.

III. Determining what data is “capable of” constituting PI. Various of the CCPA's requirements concern the use of a consumer's PI. For example, upon receipt of a verifiable consumer request, a covered business must disclose to the consumer the categories and specific pieces of PI the business has collected, as well as a report containing the consumer's PI collected by the business. Sections .100(c) and (d), .110(b). Upon receipt of an opt out request, a business must refrain from selling a consumer's PI. Section .120. Given these requirements, covered businesses must be able to understand and accurately identify what data and information comprises a consumer's PI.

In certain respects, the CCPA's definition of PI, found in section .140(o)(1), provides appropriate guidance. For example, the definition includes certain specific identifiers (e.g., real name, postal address, email address), as well as various categories of information that “could reasonably be linked, directly or indirectly,” with a particular consumer. However, the definition also includes information that merely “is capable of being associated with” a particular consumer. This open-ended language, lacking even a reasonableness requirement, provides no guidance as to the lengths a business must go to determine if a connection does, or even theoretically could, exist between any random piece of data and a consumer; nor does it advise a business of the extent of its obligation, if any, to provide or refrain from selling theoretically associable data.

Such uncertainty is unfair and problematic for both businesses and consumers alike. Without further guidance, businesses seeking to avoid claims of non-compliance may err on the side of over-disclosing, providing a requesting consumer with data concerning all others with shared names, addresses and other attributes, even in the absence of information indicating any reasonable link between that data and the consumer. Such an overbroad disclosure not only may be confusing to the consumer, but unfair to the others whose unrelated and unlinked data has been revealed without their permission or knowledge. Alternatively, businesses may determine that the risk of over-disclosure or non-compliance is too great and cease doing business in California altogether.

The California Department of Justice
February 13, 2019
Page 5

The AG's regulations should make clear that PI includes only data that is "reasonably" capable of being associated with a particular consumer. The CCPA directs the AG to update the definition of PI to, among other things, address "obstacles to implementation." Clearly, the uncertainty surrounding the "capable of" language in the PI definition poses a major obstacle to the smooth implementation of the CCPA. Imposing a reasonableness standard with respect to the "capable of" language is consistent with all other portions of the PI definition. Finally, imposing such a standard is consistent with basic legal principles requiring that uncertain statutory language be interpreted in a fashion that is reasonable, consistent with other provisions of the overall statute, and avoids absurd results (as would be the case if businesses were required to identify, provide, and refrain from selling all data even theoretically associable with a consumer).

IV. Clarifying allowable uses of government records data. The CCPA provides that data that is lawfully made available from federal, state, or local government records does not constitute PI and, thus, is not subject to the CCPA's disclosure, deletion, and opt-out requirements. This exception is not available if the data is used for a purpose that is "not compatible with the purpose for which the data is maintained or made available in the government records or for which it is publicly maintained." Section .140(o)(2).

However, the CCPA provides no guidance as to how to determine the purposes for which such data is maintained and made available, let alone whether a use is compatible with such purposes. Other statutes using similar "compatible use" language are of little help. Specifically, the federal Privacy Act's "routine use" exception (5 USC section 552a(b)) and certain California regulations patterned thereafter (e.g., 5 CCR section 42396.2, 15 CCR section 2087) apply primarily to transfers of non-public confidential information between government agencies. Moreover, these laws either identify acceptable purposes for such transfers or require the collecting agency to publish a list of routine or compatible purposes. *See* 5 USC section 552a(e)(4)(D).

Here, in contrast, the limitation is being applied to information that is publicly available and, thus, no longer confidential. In this regard, the limitation may well conflict with open government laws (e.g., federal Freedom of Information Act, CA Public Records Act) which grant consumers and others access to public data compiled by government agencies. Moreover, the limitation applies to data made available by *all* government agencies. This includes agencies in other states, not to mention various California and federal agencies, that doubtfully have published lists of routine and compatible uses.

All told, the limitation creates uncertainty as to the allowable use of government records data. Given the legal risks of non-compliance, this uncertainty likely will dissuade the use of, if not altogether undermine, the public data exception. Such a result would be unjustified, particularly since the data already is publicly available and the government agencies that compiled the data, except in instances where they have expressly indicated to the contrary, ostensibly have no objection to its broad and unfettered use. As well, such a result would be unconstitutional. The U.S. Supreme Court has emphasized that vague and uncertain content-based speech restrictions raise "special First Amendment concerns," because of "the obvious chilling effect" on speech

The California Department of Justice
February 13, 2019
Page 6

and the equally obvious risk of selective and discriminatory enforcement. *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 871-72 (1997).

The AG regulations should clarify that government records data is subject to the “compatible use” limitation only when and to the extent the government agency making the data available has explicitly indicated certain inappropriate uses of the data. Such a clarification would eliminate yet another “obstacle to implementation” of the CCPA. The limitation is inherently uncertain as drafted and, absent such a reasonable interpretation, likely will have an unduly restrictive and discriminatory effect. Finally, the suggested interpretation is reasonable given the already public nature of the information in question, and provides covered businesses and consumers clear guidance and, thus, reasonable certainty as to the scope of the government records data exception.

We hope these comments are helpful. Please let us know if you have any questions.

Very truly yours,



Philip R. Recht

Message

From: Valdetero, Jena [REDACTED]
Sent: 3/8/2019 1:50:56 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Zetoony, David [REDACTED]; Beehler, Anne Redcross [REDACTED]
Subject: Comments on CCPA

Subject: Rulemaking regarding privilege, work-product, and client confidentiality and the CCPA.

Dear Privacy Regulations Coordinator:

We write to request that Attorney General Becerra issue rulemaking concerning attorney-client privilege, work product, and client confidentiality and the CCPA.

The CCPA confers an obligation upon businesses (a term which could apply to many law firms and their corporate clients depending upon the factual circumstances) to provide privacy notices to individuals about whom information is collected, to provide individuals with access to information held about them, and, in some instances, to delete information about individuals upon their request. As it is currently written, the CCPA contains an exemption which states that the "obligations imposed on businesses by Sections 1798.110 to 1798.135 [of the CCPA], inclusive, shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law" While the exception presumably was intended to ensure that the CCPA did not require a business or an attorney to disclose privileged, work-product, or other confidential information concerning its clients, on its face, it is limited only to the obligations imposed by "Sections 1798.110 to 1798.135." More specifically, on its face, it does not apply to the obligations imposed by other sections of the CCPA including Sections 1798.100 or 1798.105.

Sections 1798.100 and 1798.105 are particularly relevant when it comes to attorney-client privilege, work-product, and an attorney's duty to maintain confidentiality of client information. Section 1798.100 contains within it the requirement that a business must, in response to an access request, "provide" to a consumer "specific pieces of personal information the business has collected" about the individual. Section 1798.105 contains within it the requirement that a business must, in response to a valid deletion request, "delete the consumer's personal information from its records. . . ." The net result is that the statute does not on its face prevent a California resident from requesting that an attorney, or a business, disclose privileged, work-product, or confidential information that relates to the California resident, nor does it prevent the California resident from requesting that a law firm (or its client) delete privileged, work-product, or confidential information that relates to the individual.

Other provisions in the CCPA provide that (1) none of the “rights afforded to consumers and the obligations imposed on the business” should “adversely affect the rights and freedoms of other consumers” (Cal. Civil Code § 1798.145(j)); (ii) the obligations imposed on businesses by this title shall not restrict a business’s ability to ... [c]omply with federal, state, or local laws (Cal. Civil Code § 1798.145(a)(1)); and that (3) “the obligations imposed on businesses by this title shall not restrict a business’s ability to ... [e]xercise or defend legal claims.” Cal. Civil Code § 1798.145(a)(3)) However, as written, it is unclear whether these general exceptions would allow an attorney to withhold privileged, work-product, and confidential information concerning its clients under state evidentiary and ethics rules that pre-date the CCPA.

In short, as written, the CCPA does not clearly exempt privileged, work-product, and confidential information concerning an attorney’s client from disclosure or deletion. This lack of clarity could create harmful results for law firms and their clients. Rulemaking that clarifies whether privileged, work-product, and confidential client documents are exempt from the CCPA is necessary.

Thank you for your time and consideration of these issues.

Regards,



JENA VALDETERO
Partner



BRYAN CAVE LEIGHTON PAISNER LLP
161 North Clark Street, Suite 4300, Chicago, IL 60601-3315

bclplaw.com

This electronic message is from a law firm. It may contain confidential or privileged information. If you received this transmission in error, please reply to the sender to advise of the error and delete this transmission and any attachments.

We may monitor and record electronic communications in accordance with applicable laws and regulations. Where appropriate we may also share certain information you give us with our other offices (including in other countries) and select third parties. For further information (including details of your privacy rights and how to exercise them), see our updated Privacy Notice at www.bclplaw.com.

Message

From: Sandy B. Garfinkel [REDACTED]
Sent: 3/8/2019 10:04:46 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA

To Whom It May Concern:

The purpose of this e-mail is to provide comments for consideration as part of the Attorney General's rulemaking process for the California Consumer Privacy Act ("CCPA"). These comments are submitted on behalf of certain clients of my firm that may be impacted the CCPA.

The comments specifically relate to Section 1798.140(c), the definition of "Business" under the CCPA. That section provides, in pertinent part:

1798.140. For purposes of this title:

...

(c) "Business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) *Has annual gross revenues in excess of twenty-five million dollars (\$25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.*

(B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

(emphasis supplied).

It is not clear from the text of Section 1798.140(c)(1)(A) whether the phrase "annual gross revenues" is intended to mean company-wide revenues derived from any geographical area, or is instead intended to be limited to revenues derived from business conducted within the State of California.

Given that the CCPA's purpose is to protect consumers who are California residents (see 1798.140(g)), and that the CCPA expressly applies only to entities which do business in California (see 1798.140(c)(1)), it is my clients' position that the "annual gross revenues" under Section 1798.140(c)(1)(A) should be interpreted to mean annual gross revenues derived from business conducted in California.

Therefore, to the extent that the Attorney General's regulations can shed light on the meaning of "annual gross revenues" under Section 1798.140(c)(1)(A), it is urged that the regulations promulgated by the Attorney General include a clarification that "annual gross revenues" under Section 1798.140(c)(1)(A) means annual gross revenues derived from business conducted in California.

Thank you for your attention and consideration. If you have any questions, please feel free to contact me.

Sandy B. Garfinkel, Esq. | Member

ECKERT SEAMANS CHERIN & MELLOTT, LLC

600 Grant Street • 44th Floor • Pittsburgh, PA 15219

[REDACTED] | [REDACTED]

[REDACTED]



This e-mail message and any files transmitted with it are subject to attorney-client privilege and contain confidential information intended only for the person(s) to whom this email message is addressed. If you have received this e-mail message in error, please notify the sender immediately by telephone or e-mail and destroy the original message without making a copy. Thank you.

Neither this information block, the typed name of the sender, nor anything else in this message is intended to constitute an electronic signature unless a specific statement to the contrary is included in this message.

Message

From: Tom Lee [REDACTED]
Sent: 3/7/2019 5:40:43 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Attachments: Mapbox CCPA Comment - March 8 2019.pdf

Please find the comments of Mapbox attached to this email. We appreciate the opportunity to contribute our perspective to the implementation of CCPA and look forward to working with your office.

Tom Lee
Policy Lead, Mapbox



50 Beale Street, Ninth Floor
San Francisco, CA 94105

8 March 2019

The following comments are submitted on behalf of Mapbox, a leading provider of map and location services, in response to a call for comments by the California Department of Justice regarding rulemaking associated with the California Consumer Privacy Act of 2018 (CCPA).

Mapbox considers the responsible stewardship of the data in our possession to be among our most important duties. The privacy of our customers' and users' personal data shapes our engineering, business and legal decisions on a daily basis. Unfortunately, this commitment is not shared by all parties in our industry. We therefore welcome California's leadership on this issue and your office's efforts to craft regulations that offer strong privacy guarantees without unduly burdening businesses that collect and use data ethically.

CCPA was drafted in haste, and although it has been improved by subsequent legislation, we believe the law still contains a number of provisions that are unclear, unwise or dangerous. It is our hope that your rulemaking process will address and ameliorate some of the following concerns.

The definition of "personal information" requires clarification

The statutory definition of "information that...is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" is vague and appears self-contradictory to Section 1798.145(a), which states: "(a) The obligations imposed on businesses by this title shall not restrict a business's ability to . . . (5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information."

However, there is no explicit carve-out from the definition of "personal information" for deidentified, pseudonymized, or in the aggregate consumer information, even though each of these terms is defined in the legislation. Instead, subsection (K)(2) of the definition of "personal information" states it "does not include publicly available information" but that "Publicly available" *does not include* consumer information that is deidentified or aggregate consumer information" (emphasis added).

This confusing definition leaves companies to guess at how to comply. For example, it is routine for a website to keep a log of Internet Protocol (IP) addresses and access times for security purposes to detect malicious behavior. If the website stores the log of IP addresses separately from a log of visitor activity on the website (e.g., the website knows a user visits the homepage of the website, then the product page followed by the contact information page, but does not know the IP address, name, or any other information about the identity of the user), then is the log of the visitor activity “deidentified” information? Does it matter if the company randomly assigns each visitor a session ID for each visit? Does it matter if the company discards the IP addresses after 30 days?

When Mapbox worked to comply with GDPR, one point on which we needed outside guidance was the definition of personal information under the law. Various European regulatory authorities issued clarifying guidance ahead of the implementation date.

As companies prepare to comply with CCPA, it would be very helpful for your office to issue examples of specific scenarios in which information is not “personal information” and examples of specific deidentification techniques your office views as sufficient to qualify information as “deidentified.”

Data deidentification often requires a grace period

On a typical day, Mapbox collects over one hundred and fifty million miles of anonymized telemetry data from users of our maps. This information allows us to offer real-time traffic predictions, detect unmapped roads, and informs many other tasks we perform to improve the services we offer.

We are able to collect this data in part because of the anonymization practices that we employ. Shortly after data is collected it is stripped of permanent identifiers and broken into smaller pieces, and the beginnings and ends of journeys are discarded. Through these measures we produce a dataset that is useful for improving our maps, but useless for identifying individuals. We do not collect end users’ names, email addresses, phone numbers or similar personal information (we do receive IP addresses and related information in the course of providing our services, but we take steps to separate such information from other user information and to minimize its retention). We do not resell individuals’ data, and all phases of our processing pipeline, including the anonymized data, are subject to strong encryption and access control policies.

We believe that these practices confer robust privacy protections and represent the objectives of the CCPA. The law attempts to lower the burden associated with possession of deidentified data. This is a wise and laudable goal: deidentified data typically poses substantially fewer risks to users than data that has not been so processed.

Unfortunately, even our systems might fail to meet the law’s standards for deidentified data. There are two reasons why.

First, unlike some of our competitors, Mapbox does not control a major mobile operating system. This introduces technical limitations which necessitate that some deidentification processes occur on our servers rather than on users' devices.

Second, the collection of any data over the internet requires the disclosure of IP addresses. This is a fundamental aspect of how communication occurs on modern networks. The CCPA identifies IP addresses as a type of personal information that triggers the law's protections.

The CCPA defines "collection" but does so with insufficient precision. It identifies IP addresses as personal information, but the law's structure makes it implausible that its authors meant to identify all internet-transmitted information as triggering CCPA's strongest protections. These ambiguities will at minimum induce considerable uncertainty among those working to comply with the law. At worst, they leave open the possibility of tendentious readings of the statute that could make it difficult or impossible for smaller businesses like Mapbox to make good-faith efforts to deidentify user data in a way that comports with CCPA.

This situation could be improved both by clearer definitions and by identifying a reasonable grace period for processing and deidentification of data rather than tying it to the act of collection. We believe that long-term storage and/or resale of personal data represent the overwhelming majority of the data risk that concerns consumers and that motivated the authors of the CCPA.

The definition of "consumer" requires clarification

Mapbox recognizes the the importance of consumer privacy and the legislature's motivation in passing CCPA. At the same time, the definition of "consumer" as "a natural person who is a California resident" captures many situations involving persons we would not conversationally refer to as "consumers."

For example, we do not believe that concerns about employee information led the legislature to take up CCPA, and this leads to potential for confusion or business hardships. Employees have very different privacy interests than customers, and there are already existing regulations regarding employees that address the privacy interests of those individuals while acknowledging businesses' need to record and retain certain information about those individuals. Reconciling them with CCPA when the laws do not make direct reference to each other will impose considerable compliance burdens on businesses or hamper their effectiveness.

For example, a delivery service has a business need to track the movement and timing of deliveries made by its drivers. At the same time, the delivery service also has a business need to *avoid* disclosing that information in a convenient electronic format to a former driver who has left to work for a competitor. A business might also track the salary information of all employees, including past employees, for various financial and planning purposes. It would be unreasonable for an ex-employee to demand deletion of that information. Even requiring businesses to

analyze and respond to such requests is an unnecessary burden outside of the consumer-protection purposes of CCPA.

Similarly, we do not believe information about routine business contacts was among the concerns that motivated the CCPA's authors. Information like business phone number, business email, and business address are relevant to a business relationship. Businesses should not need to justify collecting and storing such information, and an employee should not be able to request deletion of business contact information, which may be contrary to the wishes or needs of the employer on whose behalf the business relationship was pursued.

We believe this office should issue a guideline that excludes employees or contractors of a business acting in their roles as employees or contractors from the definition of consumer in Section 3. This is the path taken by the Washington State legislature in its version of CCPA, Senate Bill 5376.

Data portability and deletion requirements pose risk to both businesses and consumers

In its original form as a ballot measure, the CCPA required the disclosure of the types of data that are collected and how they will be used. In statutory form, the CCPA requires the disclosure of the specific data collected. The law also extends a mechanism by which consumers can request that their data be deleted. These requests may also be made by an agent authorized to act upon the consumer's behalf.

Providing a means by which personal data may be deleted or disclosed substantially increases the risk faced by consumers relative to the simple disclosure of what kinds of data have been collected. Identity thieves and vandals are sure to make use of these new capabilities. Perhaps most worryingly, the CCPA defines the scope of "personal information" to include an entire household, creating the chilling possibility that the law could be turned against victims of domestic abuse.

These potentially dire consequences make the task of confirming a requester's identity a serious responsibility. This is likely to impose a substantial burden on businesses. This is doubly true in the case of requests made by an authorized agent: in such cases the businesses may be responsible for confirming both the user's identity and the veracity of the delegation of authority.

The problem of verifying requests is also likely to induce businesses to collect more sensitive data than they otherwise might. A business might have little need for a driver's license or social security number except in order to verify a user's identity upon receipt of a CCPA request. This will make the consequences of data breaches more severe, a result that is clearly at odds with the CCPA's objectives.

In the case of business-to-business ("B2B") companies like Mapbox, it is not clear that the CCPA's data export and deletion scheme is workable at all. Mapbox has relationships with customers and provides services to those customers' users. We typically do not have a direct

relationship with those users--they do not have Mapbox user accounts and we have no means of contacting them. We also do not have information like names, birth dates, phone numbers, and addresses that could be used for verification purposes. This makes the problem of identity verification all the harder.

We suggest four measures to address this problematic dynamic:

1. Create a safe harbor for businesses when they have a good faith suspicion that a request is illegitimate. In such circumstances a business should be empowered to deny the request or ask for more information in order to confirm its legitimacy.
2. Create a licensure regime for all agents authorized to make requests on consumers' behalf. When a request is made through such an agent, that agent should bear the legal responsibilities and risks associated with ensuring the request is legitimate.
3. If a business holds a consumer's personal information in connection with an account registered with that business by the consumer, the business should be entitled to require the consumer to log in to the account as a means of confirming a CCPA data export or deletion request's legitimacy.
4. If a business holds a consumer's personal information as the result of a consumer's interaction with another service--such as in the case of a shipping company ("the secondary vendor") holding a consumer's address in the course of the fulfillment of an online order with another business ("the primary point of contact")--the secondary vendor should be empowered to require that CCPA data export or deletion requests be filed with the primary point of contact. While a secondary vendor who elects this form of verification should be required to verify the identity of the primary point of contact, this should be an option for businesses legitimately attempting to minimize the amount of personal information they collect. This will reduce the risk of fraudulent requests being filed en masse against B2B companies; and will reduce the need of such businesses to retain additional personal data in order to comply with CCPA requests.

Disclosure requirements will be more useful if matched to their context

We welcome CCPA's enhanced disclosure requirements. Its authors' efforts to make the law accessible to all Californians are laudable. We understand this aim to be the motivation behind CCPA's requirement that businesses offer a toll-free number by which consumers may file requests.

For some businesses this requirement might make sense. In the case of our own business, it seems likely to confuse consumers. Mapbox does not typically communicate with customers or users by phone--not for sales and not for support. Our services and the ways in which users interact with them are fundamentally mediated by interfaces like smartphones and computers. In this context a telephone interface seems unhelpful at best, and perhaps even confusing.

We acknowledge the need to ensure that CCPA's guarantees are made apparent to users of services, but we believe that consumers will be better served by notice mechanisms that are harmonized with the nature of the services to which they apply.

In closing

We realize that in some cases the issues we have identified might require statutory changes. However, we understand that your office is in dialogue with the California legislature as that body continues to improve the CCPA. We therefore offer these suggestions in the hopes that they might inform the goal we all share: producing the best privacy law possible.

We welcome the Department's attention to this matter and thank you for your consideration of these comments. We look forward to working with the Department as it proceeds toward implementation of the CCPA.

Thomas Lee
Policy Lead, Mapbox

[REDACTED]

Kathleen Lu
IP and Open Data Counsel, Mapbox

[REDACTED]

Message

From: Maureen Mahoney [REDACTED]
Sent: 3/8/2019 4:59:08 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Attachments: CR CCPA Comments to CA AG.pdf

Attached, please see the comments submitted by Consumer Reports regarding CCPA implementation. Please do not hesitate to reach out with any questions.

Thank you for your consideration -

Best,
Maureen

--

Maureen Mahoney
Policy Analyst
[REDACTED]

[CR.org](https://www.consumerreports.org) [CR.org/advocacy](https://www.consumerreports.org/advocacy)



This e-mail message is intended only for the designated recipient(s) named above. The information contained in this e-mail and any attachments may be confidential or legally privileged. If you are not the intended recipient, you may not review, retain, copy, redistribute or use this e-mail or any attachment for any purpose, or disclose all or any part of its contents. If you have received this e-mail in error, please immediately notify the sender by reply e-mail and permanently delete this e-mail and any attachments from your computer system.



March 8, 2019

California Department of Justice
300 S. Spring Street
Los Angeles, CA 90013
ATTN: Privacy Regulations Coordinator

Re: Rules Implementing the California Consumer Privacy Act (CCPA)

Consumer Reports¹ appreciates the opportunity to submit input to the California Attorney General's office (AG) as it prepares to propose rules to implement the California Consumer Privacy Act (CCPA). Consumer Reports has long fought to expand privacy protections for consumers, and is pleased that the CCPA guarantees important privacy safeguards, including the right to opt-out of the sale of personal information.² The AG has the opportunity to ensure that the CCPA is workable for consumers, as it has broad leeway to issue regulations to further the privacy intent of the CCPA.³ The AG should issue common-sense proposed rules that would:

- Maintain the definition of personal information;
- Tighten restrictions on targeted advertising;
- Restrict access and deletion rights with respect to unauthenticated data;
- Make it easy to opt-out of the sale of personal information, by requiring companies to honor Do Not Track signals and by creating a Do Not Sell registry modeled after the National Do Not Call Registry;
- Put reasonable limits on financial incentives for the sharing or sale of personal information to third parties; and
- Require detailed privacy policies that provide real transparency and impose limits on companies' data practices.

Now, more than ever, consumers want real privacy protections. Currently, the burden is on the consumer to decipher long, confusing privacy policies, or to decide between using a potentially helpful service or device and guarding their privacy. And, they're fed up. 92 percent of Americans think that their Internet Service Provider (ISP) should obtain their permission before sharing their data with third parties.⁴ Over

¹ Consumer Reports is an expert, independent, non-profit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. Consumer Reports is the world's largest independent product-testing organization, using its dozens of labs, auto test center, and survey research department to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

² Sec. 1798.120

³ Sec. 1798.185

⁴ Bree Fowler, *Americans Want More Say in the Privacy of Personal Data*, CONSUMER REPORTS (May 18, 2017), <https://www.consumerreports.org/privacy/americans-want-more-say-in-privacy-of-personal-data/>.

Headquarters Office
101 Truman Avenue
Yonkers, New York 10703-1057

South West Office
11801 Domain Blvd, 3rd Floor
Austin, TX 78701

Washington Office
1101 17th Street, NW #500
Washington, DC 20036

West Coast Office
1535 Mission Street
San Francisco, CA 94103-2512

half don't trust social media companies to keep their information safely protected.⁵ And almost three-quarters said that it's very important to have control over their information.⁶ Recent scandals involving the illicit sharing or sale of personal information without consent, such as the Cambridge-Analytica incident⁷ and reports of unauthorized location tracking,⁸ have revealed broad unease among the general public of data sharing without the consumers' active consent. Clearly, consumers value their devices, connected products, and other apps and services, but they don't have the confidence that their information is safe. Consumers and businesses need clear rules of the road with protections that ensure that consumers have privacy by default.

1. The AG should reject requests to narrow the categories of personal information covered by the law and the definition of unique identifier, to ensure that sensitive data is protected.

The CCPA gives the AG the authority to adjust the categories of personal information covered by the legislation, as well as the definition of unique identifier, in order to reflect “changes in technology, data collection, obstacles to implementation, and privacy concerns.”⁹ Some industry representatives have sought to dramatically scale back the information covered by the CCPA, particularly information associated with a device, such as IP addresses, information associated with a household, as well as pseudonymous information.¹⁰ The AG should reject requests to narrow information covered by the CCPA, which would eliminate important rights for consumers and directly counter legislative intent.

While there are valid concerns about access and deletion rights to device- and household-level information in shared environments—members of a household should not be allowed to access unauthenticated data because they could end up accessing the private information of another person—those concerns should be dealt with narrowly, for example, by restricting access and deletion rights to unauthenticated data (see *infra*, section 3). With respect to information tied to a device, if the device has a discrete and known number of users, it may be appropriate to provide access and deletion if practicable to get consent from all users.¹¹ It should not be dealt with by limiting the definition of personal information, which would remove consumers' ability to opt out of its sale—a key protection under the law. Bill sponsor Alastair MacTaggart laid out an expansive definition of personal information, which includes information that is “capable of being associated with . . . a particular consumer or household”¹² to cover the ways that companies use and share information today, including for advertising purposes.¹³

⁵ Lee Rainie, *Americans' Complicated Feelings about Social media in an Era of Privacy Concerns*, PEW RESEARCH CTR. (Mar. 27, 2018)

<http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/>.

⁶ Mary Madden and Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RESEARCH CTR. (May 20, 2015), <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.

⁷ Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.

⁸ Joseph Cox, *I Gave a Bounty Hunter \$300. Then He Located Our Phone*, MOTHERBOARD (Jan. 8, 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

⁹ Sec. 1798.185(a)(1)-(2)

¹⁰ Letter from California Chamber of Commerce et al. to Bill Dodd, Re: SB 1121 (Dodd): Business Community Requests to be Included in AB 375 Clean-Up Legislation at 4-6 (Aug. 6, 2018), <http://src.bna.com/A44> [hereinafter Chamber Letter].

¹¹ Electronic Frontier Foundation, EFF Comments to the California Attorney General Regarding CCPA Rulemaking at 4 (Mar. 8, 2019) [hereinafter EFF Comments].

¹² Sec. 1798.140(o)(1)

¹³ Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley — and Won*, N.Y. TIMES (Aug. 14, 2018), <https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html>.

Device and household-level data is very sensitive, and consumers deserve protections around its use—particularly the right to opt out of its sale.

Removing IP address from the definition of personal information would weaken protections against the sale of location data to ad tech companies, data brokers, and other third parties. Many IP addresses are static or change infrequently, allowing companies to track user behavior over time even without access to cookies or other identifiers.¹⁴ Moreover, correlation of IP addresses is one of the most effective means for companies to engage in cross-device tracking, as devices that share local networks are considerably more likely to be operated by the same persons.¹⁵ Currently, the CCPA gives consumers the right to opt out of its sale to third parties, but removing IP address from the definition of personal information would rescind this right.

Covering household data is important as well. Household data—collected through services like Nest or communal devices such as smart TVs—can also be used to track whether consumers are in their home or not—a potential gold mine for thieves.¹⁶ Facebook recently took out a patent to better determine the family members or others that consumers live with—by using facial recognition technology to analyze photos posted on Facebook or Instagram. This information would then be used to better target advertising towards consumers.¹⁷ Again, consumers find this information to be extremely sensitive—85 percent consider relationship history to be sensitive information.¹⁸ Thus, it would be inappropriate to narrow the definition of personal information.

On the other hand, we do not object to the AG clarifying that the phrase “capable of being associated”¹⁹ in the CCPA’s definition of personal information does not render *any* piece of information necessarily covered by CCPA. Rather, only information that could reasonably be associated with a person, device, or household should be considered within the scope of the law’s protections.

2. The AG should tighten restrictions on targeted advertising.

Targeted advertising, including based on pseudonymous data, must remain covered by the legislation, and other collection methods such as social sharing widgets should fall under the scope of sale as well. While industry groups such as the California Chamber of Commerce have sought to explicitly exempt behavioral advertising from the CCPA’s right to access and third-party sharing opt-out protections,²⁰ this undermines a main goal of the CCPA and ignores consumers’ stated preferences. A principal purpose of the CCPA is to give consumers the ability to opt out of the sale of their personal information, including for online advertising. Bill sponsor Alastair MacTaggart sought to “slowly dry up the supply of personal information that companies could buy or trade on the open market” in order to address some of the worst abuses.²¹ For example, while many state statutes cover only a handful of types of personal

¹⁴ Dennis Hartman, *The Advantages & Disadvantages to a Static IP Address*, TECHWALLA (last visited March 7, 2019), <https://www.techwalla.com/articles/the-advantages-disadvantages-to-a-static-ip-address>.

¹⁵ *Cross-Device Tracking: An FTC Staff Report*, FED. TRADE COMM’N at 3 (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.

¹⁶ Lauren Kirchner, *Your Smart Home Knows a Lot About You*, PROPUBLICA (Oct. 9, 2015), <https://www.propublica.org/article/your-smart-home-knows-a-lot-about-you>.

¹⁷ Nicole Nguyen, *Facebook Filed a Patent to Predict Your Household's Demographics Based On Family Photos*, BUZZFEED NEWS (Nov. 16, 2019), <https://www.buzzfeednews.com/article/nicolenguyen/facebook-household-prediction-patent>

¹⁸ Mary Madden, *Americans Consider Certain Kinds of Data to be More Sensitive than Others*, PEW RESEARCH CTR. (Nov. 12, 2014), <http://www.pewinternet.org/2014/11/12/americans-consider-certain-kinds-of-data-to-be-more-sensitive-than-others/>.

¹⁹ Sec. 1798.140(o)(1)

²⁰ Chamber Letter, *supra* note 10, at 10.

²¹ Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley — and Won*, N.Y. TIMES (Aug. 14, 2018), <https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html>.

information,²² the privacy provisions in the CCPA cover a broad swath of consumer data, including information tied to a device, to give consumers control over the data used for advertising purposes.²³ Similarly, the CCPA has an inclusive definition of the “sale” of information, to help ensure that consumers can opt out of data sharing for online advertising.²⁴ If a consumer who opts out of the sale of their data on an shoe store’s website ends up seeing retargeted ads for those shoes all over the internet, consumer choice will be frustrated, and the CCPA will have failed to achieve its objectives.

Furthermore, the AG should clarify that all online sharing for measurement, analytics, and related uses should be considered within the scope of sale unless the recipient is prohibited from any beneficial secondary usage of the data. Cross-site, app, and service measurement and analytics data can be very sensitive. The CCPA places no limits on the ability of companies to collect data to advertise to their own customers. But, it enforces much-needed accountability in the context of the current ecosystem by placing real limits on companies all along the data-sharing chain and disincentivizing data purchases. If online tracking is considered outside of scope of the CCPA, then it would not achieve its stated goals. Data brokers were the intent of the bill,²⁵ and online ad tech companies—including Facebook and Google—are the modern data brokers. As Berkeley professor Chris Hoofnagle explains, Google and Facebook provide app developers privileged, valuable information—your data—in return for services that help increase engagement with their platforms.²⁶

For that same reason, it’s important to tighten operational exceptions for consumers’ opt-out choices. Section 1798.140(t)(2)(C) states that the business purpose exemption for service providers is allowed only when *necessary* for those purposes. However, this exception must not be allowed to swallow the rule, allowing for profligate third-party sharing contrary to user directives and expectations. Last year, Facebook made headlines when they were discovered to have given companies like Microsoft, Amazon, and Spotify extensive access to consumer data under the guise of a “service provider” relationship.²⁷ Recently, Mark Zuckerberg published an op-ed in the *Wall Street Journal* that implied that millions of websites and apps needed to share details of website visits with Facebook for security and account fraud prevention.²⁸ The AG should clarify that sharing in spite of an opt-out instruction must be reasonably constrained and proportionate, and subject to reasonable retention requirements. The Electronic Frontier Foundation articulated a set of rules for limited operational sharing despite receiving a browser “Do Not Track” instruction; that guidance should inform the AG’s own guidance around reasonable exceptions.²⁹

3. The AG should restrict access and deletion rights with respect to unauthenticated data to ensure that consumer privacy is protected.

The CCPA also empowers the AG to establish rules regarding requests to access and delete personal information—including honoring those submitted by a consumer logged into an account with the company and those without an online account.³⁰ While we strongly urge the AG to maintain an

²² See, for example, California’s data breach notification statute, California Civil Code 1798.82.

²³ Sec. 1798.140(o)(1)(A)

²⁴ Sec. 1798.140(t)(1)

²⁵ Confessore, *supra* note 21.

²⁶ Chris Hoofnagle, *Facebook and Google Are the New Data Brokers* (Dec. 2018), https://hoofnagle.berkeley.edu/wp-content/uploads/2018/12/hoofnagle_facebook_google_data_brokers.pdf.

²⁷ Gabriel J.X. Dance, Michael LaForgia and Nicholas Confessore, *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), <https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html>.

²⁸ Mark Zuckerberg, *The Facts About Facebook*, WALL ST. J. (Jan. 24, 2019), <https://www.wsj.com/articles/the-facts-about-facebook-11548374613>.

²⁹ Electronic Frontier Foundation, A Privacy-Friendly Do Not Track (DNT) Policy (last visited March 7, 2019), <https://www.eff.org/dnt-policy>.

³⁰ Sec. 1798.185(a)(7)

expansive definition of personal information, including information associated with a device and a household, the AG should clarify that unauthenticated data is exempt from access and deletion rights.

To avoid unauthorized and inappropriate disclosure of personal data in responding to requests, steps must be taken to verify identity, for both consumers that have an online account with a company and those that do not. Even consumers who have logged in to their accounts should be required to log-in separately for access and deletion requests, to help avoid unauthorized access to their personal information.³¹ Additionally, the use of two-factor authentication should be encouraged.³² Consumers without online accounts with the company should be required to provide additional identification to prove that they are the person whose information has been collected and used.³³ For third-party access requests, the third party must prove that they have the authorization of the consumer to submit access and deletion requests.³⁴

The AG should allow companies to deny access and deletion requests when the data cannot be authenticated or reasonably tied to a specific person. While transparency, data portability, and access rights are incredibly important, the risk of disclosure of sensitive information to a person other than the consumer is simply too great. In addition, while the CCPA already notes that businesses need not reidentify or link data in order to comply with access requests,³⁵ we have no objection to clarifying further that there is no need to collect and associate information with a real name in order to provide access.³⁶ Otherwise, there is the potential that someone other than the consumer, including a spouse or roommate, could obtain sensitive information about the consumer without their authorization.

Companies that can tie specific data to an individual *must* provide the specific pieces of information as mandated by CCPA. For example, companies often supplement their files with information from data brokers.³⁷ It's important for accountability that consumers are able to access those specific pieces of data. Some limitations on access may be appropriate. For example, we have no objection to clarifying that companies are not required to release financial account information, birthdates, or SSNs or other specific pieces of information that could be used for identity theft.³⁸

4. The AG should make it easy to opt-out of the sale of personal information, by requiring companies to honor Do Not Track signals and by creating a Do Not Sell registry modeled after the National Do Not Call Registry.

An opt-out regime can only work if consumers can opt out universally with simple tools. Opting out site by site, store by store is not practical. To remedy this, the AG should (1) clarify that companies need to comply with platform-level opt-outs similar to iOS Limit Ad Tracking and Do Not Track if offered. The AG should also (2) set up a registry of identifiers, such as email addresses, phone number, etc., for users to globally opt out of the sale of their information.

Companies should be required to honor global, platform-level requests to opt out of the sale of consumer data. Currently, browsers including Internet Explorer³⁹ and Chrome⁴⁰ give consumers the option to

³¹ EFF Comments, *supra* note 11, at 3.

³² *Id.*

³³ *Id.* at 4.

³⁴ *Id.* at 5.

³⁵ Sec. 1798.110(d)(2)

³⁶ Chamber Letter, *supra* note 10, at 8.

³⁷ *Data Brokers: A Call for Transparency and Accountability*, FED. TRADE COMM'N at 24 (May 2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

³⁸ Chamber Letter, *supra* note 10, at 8. In these instances, companies should still be required to disclose the category of information collected.

³⁹ Microsoft, Use Do Not Track in Internet Explorer 11 (last visited March 7, 2019),

indicate their tracking preferences. Do Not Track signals from a California IP address could be interpreted as an opt out, or browsers could offer new signals to publishers to convey CCPA opt-out requests to all publishers.⁴¹ Selecting these platform controls clearly indicates that a consumer intends to limit the sharing of personal information to third parties. For unauthenticated data not associated with a specific person, platform-level controls are the most efficient manner to globally convey opt-out requests.

Second, the AG should create and house a Do Not Sell registry, modeled on the FTC's popular Do Not Call (DNC) registry, that businesses would be required to check before selling consumer data tied to those identifiers. The AG would collect consumers' identifiers, such as emails and phone numbers, and companies would pay in order to consult the list (thus ensuring that companies seeking to sell data would absorb the costs for the operation of the website). Consumers could add their identifiers to the registry through public portal, much like Do Not Call. This would enable consumers to easily and globally express their preferences to opt-out of the sale of their data. Companies should be required to check this database before selling (or purchasing) consumers' information, much as they do today for the DNC registry. The DNC registry currently includes over 235 million numbers, indicating that this is an easy way for consumers to opt out of telemarketing messages.⁴² The same should be done for online privacy. Sen. Ron Wyden, in his proposed Consumer Data Protection Act, outlines a similar system to facilitate global opt outs for both unauthenticated and authenticated data.⁴³

Finally, we have no objection to the AG clarifying that business may offer consumers the opportunity to opt out of the sale of some, but not all, of their data,⁴⁴ as long as companies are also required to provide a way to opt out of all third party sales at once under the CCPA. Companies should make it as easy as possible for consumers to opt-out of the sale of their data by giving them a universal opt-out, but the CCPA does not prohibit, and we have no objection to, businesses creating multiple options for consumers.

5. With respect to financial incentives, discriminatory treatment should be presumed where markets are consolidated and consumers lack adequate choices.

The existing text of the CCPA supports loyalty programs that reward consumers for repeated patronage. A loyalty program rewards customers for what they buy (e.g., every tenth coffee is free). Businesses collect consumer data in order to determine those rewards. The CCPA does not address or regulate this type of collection of data at all—leaving businesses free to create these programs. As such, we have no objection to the AG clarifying further that legitimate loyalty programs are permitted under the CCPA.⁴⁵ However, the AG should exercise its rulemaking authority with respect to financial incentives programs to clarify that discriminatory treatment should be presumed where markets are consolidated.

<https://support.microsoft.com/en-ca/help/17288/windows-internet-explorer-11-use-do-not-track>.

⁴⁰ Google Chrome Help, Turn "Do Not Track" On or Off (last visited March 7, 2019),

<https://support.google.com/chrome/answer/2790761?co=GENIE.Platform%3DDesktop&hl=en>.

⁴¹ Electronic Frontier Foundation, Do Not Track (last visited Dec. 18, 2018), <https://www.eff.org/issues/do-not-track>.

⁴² *National Do Not Call Registry Data Book FY 2018*, Federal Trade Commission at 5 (Nov. 2018),

https://www.ftc.gov/system/files/documents/reports/national-do-not-call-registry-data-book-fiscal-year-2018/2018_dnc_data_book_0.pdf. The efficacy of the DNC registry is of course limited by the fact that it only applies to legitimate telemarketers, and that it does not hinder scammers, debt collectors, and others in their communications.

⁴³ Consumer Data Protection Act, Discussion Draft (2018),

<https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20Discussion%20Draft%20Nov%20201.pdf>.

⁴⁴ ANA Urges California Attorney General to Clarify Key Provisions of California Consumer Privacy Act (CCPA) (Jan. 14, 2019),

<https://www.ana.net/content/show/id/52341> [hereinafter ANA Letter].

⁴⁵ *Id.*

Loyalty programs are clearly permitted under the CCPA. The CCPA provides a wide exemption in the right to delete provision in order “to provide a good or service requested by the consumer.”⁴⁶ This certainly accommodates rewards programs. The *fundamental purpose* of a loyalty program is to track purchases in order to determine when a customer is entitled to a free or discounted good. For example, someone who signs up for a coffee shop rewards program is requesting that the company log how many coffees she has purchased. This type of user-requested information collection is clearly allowed under the CCPA. Of course, the customer may have a right to delete *other* data that the company maintains, and of course can decide not to participate in the loyalty program at all.

Unfortunately, the CCPA goes even further to allow companies to offer financial incentives for the sale of personal information to third parties. True loyalty programs simply keep track of customer purchasing in order to incentivize repeat business. But other, more exploitative programs could provide discounts in exchange for building a profile for targeting offers, or could sell information about customer habits to third-party data brokers. The CCPA explicitly states that companies can charge higher prices to consumers who limit access to their data and can offer financial incentives to consumers for the collection and sale of their personal information.⁴⁷ This language was added to the CCPA over objections from advocates, who argued that consumers should not be penalized for exercising their privacy rights.⁴⁸ That behavior does nothing to reward consumer loyalty, and runs counter to what participating consumers would reasonably expect. For this reason, the California Supermarket Club Disclosure Act of 1999 already puts important limits on many California retailers—those that sell food—with respect to these exploitative practices.⁴⁹

Discriminatory treatment should be presumed where markets are consolidated and consumers lack choices. The AG currently has the authority under the CCPA to issue rules prohibiting the use of financial incentives in market sectors that lack competition,⁵⁰ and we urge the AG to do so. ISPs, for example, should not be allowed to charge consumers for exercising their privacy rights, because customers lack the meaningful opportunity to find more affordable options elsewhere. For example, for years, AT&T charged usurious rates—about \$30 per month—for not leveraging U-Verse data for ad targeting.⁵¹ Where consumers have few choices, market forces don’t impose sufficient constraints on companies from penalizing exercising privacy rights. And, there is rising concentration across many industries in the United States,⁵² further highlighted by the creation of a new Federal Trade Commission task force to monitor these trends.⁵³ The AG should exercise its authority to put reasonable limits on the these programs in consolidated markets.

6. The AG should require detailed privacy policies that provide real transparency and impose limits on companies’ data practices.

⁴⁶ Sec. 1798.105(d)(1)

⁴⁷ Sec. 125(a)(2) and 125(b)

⁴⁸ Consumers Union Letter re: AB 375 (Jun. 28, 2018), <https://advocacy.consumerreports.org/wp-content/uploads/2018/06/CU-Letter-AB-375-final-1.pdf>.

⁴⁹ California Civil Code 1749.60

⁵⁰ Sec. 1798.125(b)(4)

⁵¹ Jon Brodtkin, *AT&T to End Targeted Ads Program, Give All Users Lowest Available Price*, ARS TECHNICA (Sept. 30, 2016), <https://arstechnica.com/information-technology/2016/09/att-to-end-targeted-ads-program-give-all-users-lowest-available-price/>.

⁵² *Too Much of a Good Thing*, ECONOMIST (March 26, 2016), <https://www.economist.com/briefing/2016/03/26/too-much-of-a-good-thing>.

⁵³ *FTC’s Bureau of Competition Launches Task Force to Monitor Technology Markets*, FED. TRADE COMM’N (Feb. 26, 2019), <https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology>.

Consumers dislike reading privacy policies,⁵⁴ but they serve a real purpose. The FTC typically takes action against companies for privacy reasons only when they violate their terms of service.⁵⁵ Because there are no requirements for these disclosures, and because most FTC privacy cases are predicated upon a specific misstatement in a privacy policy or elsewhere, companies tend to make privacy policies as expansive as possible, so as to shield themselves from lawsuits and other enforcement actions.⁵⁶ To address this problem, privacy policies must provide detailed information about practices. The primary audience is not consumers but regulators, the press, and testing organizations like Consumer Reports.

These documents should be used primarily as compliance and accountability tools—so that intermediaries can hold companies accountable for the standards set forth in these documents. The AG should set guidelines to ensure that the privacy policies accurately and thoroughly describe companies' privacy and security practices. This will improve transparency and help rein in abusive privacy practices. The AG should supplement these mandatory, detailed disclosures with requirements to first provide simple instructions for consumers seeking to take advantage of their privacy rights. These bifurcated privacy policies would prioritize the actionable information for consumers while also providing substantially more information for those few with the bandwidth and interest to process such information.

Finally, we have no objection to the AG issuing guidance that companies need not develop individualized privacy policies containing specific pieces of personal information collected about the consumer. In the hearings and in written testimony, some industry representatives have raised concerns that the requirement in 1798.110(c) for companies to provide to consumers disclosures about the specific pieces of personal information the business has collected about that consumers could be interpreted to mean that each company must create an individualized privacy policy for consumers.⁵⁷ As explained by sponsors Alastair MacTaggart and Common Sense Media, that is not the drafters' intent.⁵⁸ We agree that companies should not be required to create individualized privacy policies for each consumer, and we have no objection to the AG issuing guidance to that effect.

Conclusion

Thank you for accepting feedback on the implementation of the CCPA. We look forward to continuing to work with you throughout the rulemaking process.

Justin Brookman
Director, Consumer Privacy and Technology Policy
Washington, DC

Maureen Mahoney
Policy Analyst
San Francisco, CA

⁵⁴ Aleecia M. McDonald, Robert W. Reeder, Patrick Kelley, Lorrie Faith Cranor, *A Comparative Study of Online Privacy Policies and Formats* at 6, <https://www.robreeder.com/pubs/PETS2009.pdf>.

⁵⁵ *Protecting Consumer Privacy in an Era of Rapid Change*, FED. TRADE COMM'N at 8-9 (Dec. 2010), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf>.

⁵⁶ *Id.* at 19.

⁵⁷ ANA Letter, *supra* note 44.

⁵⁸ Californians for Consumer Privacy and Common Sense Kids Action, Recommended Technical Amendments to AB 375 & SB 1121 (Jan. 19, 2019), <https://www.caprivacy.org/post/recommended-technical-amendments-to-ab-375>.

Message

From: Deborah Chang [REDACTED]
Sent: 3/7/2019 12:29:05 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Attachments: CA AG Letter.docx

Attached are HackerOne's comments on the implementation of CCPA.

Deborah Chang
VP Business Development and Policy
HackerOne
300 Montgomery Floor 12
San Francisco, CA . 94070
[REDACTED]

March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA. 90013

Thank you for the opportunity to give feedback on the California Consumer Privacy Act (CCPA) of 2018. HackerOne supports the implementation of CCPA, as it is consistent with HackerOne's own core values of transparency, vulnerability disclosure, and vulnerability sharing.

Our core focus as it relates to CCPA is mainly focused on the issues around cybersecurity. There have been many data breaches that have eroded consumer trust in how our data is handled. Consumers are not fully aware how data is collected, what it's used for, and how it's secured. Even companies who spend the millions of dollars on security and have very mature security practices have difficulty fighting against the bad actors, much less smaller companies with less developed security practices. This is why HackerOne believes that any privacy legislation should encourage the public's help in finding the vulnerabilities. A security vulnerability can be not only a software vulnerability, but can also include weaknesses in business processes, lack of policies and data vulnerabilities.

HackerOne respectfully submits the following recommendations to CCPA Implementation:

Under SB 1121 (Dodd), businesses that receive "verifiable consumer requests" to access personal information must abide by the request within the time frame specified. Businesses must be able to determine and process these "verifiable consumer requests" in a secure manner. We suggest that the CAG adopt regulations to require security procedures be in place to prevent vulnerabilities that would result in fraud, misuse and loss of data in connection with the execution of these requests by consumers.

In order to prevent breaches and misuses of data while processing these requests, the Office of the CAG should encourage businesses to adopt best practice security procedures, which includes the adoption of coordinated vulnerability disclosure policies by businesses. (ISO/IEC 29147:2014: Information Technology – Security Techniques – Vulnerability Disclosure).[1] Businesses should be ready and willing to receive information from consumers and security researchers about vulnerabilities that exist in this request process by acknowledging receipt of the initial vulnerability report to the consumer who submitted the vulnerability. And they should build an internal process by which to process, analyze, and remediate the vulnerability. By leveraging the power of the public, a business increases the likelihood of finding bugs before bad actors do.

hackerone

A vulnerability disclosure policy is a step that any business can take. And vendors such as HackerOne, offer a free policy builder on its website. <https://hackerone.com/policy-builder>.

Also, Section 13 1798.185(7) includes an example where if a consumer makes a request while being logged in the account, that it qualifies as a “verifiable consumer request.” We do not take issue with whether this constitutes a verifiable consumer request, but we do want to note that fundamentally, a business has to make that process secure. This includes not only having a Vulnerability Disclosure Policy (VDP), but also proactively reassessing risk assessments regularly, and seeking opportunities to reduce cybersecurity risks even when residual risk is acceptable.

Thank you for the opportunity to give feedback to the implementation of CCPA.

Deborah Chang

/s/

VP Policy
HackerOne

HackerOne is the #1 hacker-powered security platform, helping organizations find and fix critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative. The U.S. Department of Defense, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, the CERT Coordination Center and over 1,200 other organizations have partnered with HackerOne to find over 100,000 vulnerabilities and award over \$45M in bug bounties. HackerOne is headquartered in San Francisco with offices in London, New York, the Netherlands, and Singapore

[1] US Federal government also endorses the practice of vulnerability disclosure: The National Telecommunications and Information Administration (NTIA) located within the Department of Commerce issues guidelines on what to include in a VDP: https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf, and the Department of Justice issued a framework on VDPs: <https://www.justice.gov/criminal-ccips/page/file/983996/download>

Message

From: Olivia Lee [REDACTED]
Sent: 2/5/2019 1:43:50 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Flag: Follow up

Hi,

Thank you for your work in gathering comments for CCPA regulations, we truly appreciate it. Below are our comments:

1) Applicability of the Act to employee data: We would prefer to either specifically include definitional language that exempts employee data from being covered by the Act, or to limit the application of the Act to a reduced set of requirements for data used in the employment context (e.g., could say that prohibition on the sale of personal data and the need to protect it applies to employees, but the right for an employee to request deletion of their data or to limit processing doesn't except under certain circumstances). If the second approach is used, personal data would not need to be defined differently, but then a section could be added to specifically clarify the requirements that would and would not apply in the employment context.

2) Safe harbor and limiting private cause of action: We would recommend proposing language the following language: "The cause of action established by this section shall not apply when a business can demonstrate that it has effectively implemented a security management program based on a recognized information security standard."

Please feel free to reach out if you have any questions.

Best,

Olivia

Olivia Lee | Manager, Public Policy
LOS ANGELES AREA CHAMBER OF COMMERCE
350 S. Bixel St. | Los Angeles, CA 90017
[REDACTED] [REDACTED] [REDACTED]
[REDACTED] www.lachamber.com

Message

From: Barth-Jones, Daniel C. [REDACTED]
Sent: 3/8/2019 3:48:48 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Attachments: Daniel Barth-Jones, PhD Public Comments on the CCPA.pdf

Please accept these public comments submitted regarding the CCPA.

Sincerely,
Daniel C. Barth-Jones, PhD
Assistant Professor of Clinical Epidemiology
Department of Epidemiology
Mailman School of Public Health
Columbia University



EPIDEMIOLOGY

March 8, 2019

California Department of Justice
300 S. Spring St.
Los Angeles, CA 90013
ATTN: Privacy Regulations Coordinator

Re: Comments on CCPA (California Consumer Privacy Act)

Dear Sir/Madame:

Thank you for taking comments from the public about the California Consumer Privacy Act (CCPA). I am writing to express concerns about several important issues with the wording in the CCPA that I believe could negatively impact the conduct of medical, health care systems and public health research.

I am an Infectious Disease Epidemiologist with a faculty position as an Assistant Professor of Clinical Epidemiology in the Department of Epidemiology at the Mailman School of Public Health at Columbia University. I offer these comments in my role as an academic medical, health care systems and public health researcher who specializes in the area of statistical disclosure control with specific expertise in the area of HIPAA de-identification policy and practice, and I do not speak in any formal capacity with my comments here for the broader interests of Columbia University.

Of particular concern with respect to harmonization with activities currently conducted in accordance with the HIPAA Privacy Rule, I note that there is a need for careful consideration of the definitions of "personal information", "pseudonymize", and "deidentified" within section 1798.145.(h). As per this section, "*Deidentified*" means information that cannot reasonably identify, **relate to, describe, be capable of being associated with**, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

- (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
- (2) Has implemented business processes that specifically prohibit reidentification of the information.
- (3) Has implemented business processes to prevent inadvertent release of deidentified information.
- (4) Makes no attempt to reidentify the information.

This definition would seem be overly broad, in that, by definition, all information that pertains to an individual would be seen to **relate to, describe, be capable of being associated with** such individuals. This all inclusive definition could possibly be seen as being mitigated to some extent

by the word “reasonably” that proceeds it, but to be fully consistent with the HIPAA Expert Determination method found at §164.514(b)(1) of the HIPAA Privacy Rule¹, this “reasonably” condition would need to clearly convey the concept of a tolerance of the presence of some “very small” risk of being potentially linked (or related to, described, be capable of being associated) with a particular consumer.

At the same time, the definition of “deidentified” under section 1798.140(h) also seems unduly narrow in that it also specifically also requires implementation technical safeguards and business processes to prohibit reidentification and inadvertent release of the de-identified data. While such controls are often employed and specifically required as conditions of an Expert Determination of de-identification under the HIPAA Privacy Rule, this is typically used only as part of the conditions required to assure the existence of a very small risk of re-identification. Some data sets with very limited “quasi-identifiers” which in combination might uniquely identify consumers, might not specifically require such conditions as part of their meeting the conditions of the HIPAA de-identification standard. In fact, release of de-identified data under the HIPAA Safe Harbor provision found at 164.514(b)(1) does not require such additional conditions. Because of these concerns, the CCPA’s definition of “deidentified” is importantly at variance from the long-established HIPAA standard for “de-identification.”

Additionally, the CCPA’s definition of “personal information” is in need of some further harmonization with the HIPAA Privacy Rule in order to prevent unintentional consequences. As per, CCPA 1798.140 section (o) (1): “Personal information” means information that identifies, **relates to, describes, is capable of being associated with**, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

Of increased concern, is the fact that in this definition, the leading qualifier “reasonably” which could be possibly be seen as a mitigating factor expressing some tolerance for the existence of very small, but not de minimis, risks has not been placed in front of the problematic criteria **“relates to, describes, is capable of being associated with”**, which without this mitigating adjective could now be arguably seen as applying to virtually all information pertaining to a consumers.

Furthermore, under the CCPA “Personal Information” includes, but is not limited to, the following: ...

- (I) Professional or employment-related information.
- (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
- (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

¹ §164.514(b) Implementation specifications: Requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if: (1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and (ii) Documents the methods and results of the analysis that justify such determination;

These characteristics are only very vaguely defined and would clearly be seen to “relate to” many individuals and are, further, not constructed in a manner that would make it clear that these characteristics would be only be “reasonably” able to be linked to or identify an individual when they, in combination would uniquely characterize individuals. For example, a single attribute indicating that a consumer is employed would not be, in and of itself, identifying. But when combined with additional professional, employment or educational information, the combination of such characteristics might very well produce a risk of re-identification beyond the HIPAA Privacy Rule’s tolerance for the existence of such very small risks which might, on rare occasions, exist.

Finally, I wish to also note that the exemption for clinical trial data in section 1798.145(a)(1)(C) only exempts information that is collected as part of a clinical trial and is subject to the federal Common Rule, Good Clinical Practices (GCP) guidelines, or FDA human subject protections. I believe there is a need to recognize that such a narrow exception might have the potential to unproductively constrain a vast arena of health data “records based” research which is of great benefit to society and should be seen is an essential “public good”. The broad conduct of such data based research is an essential tool for society supporting scientific innovation and health system improvement and efficiency and serves as an engine driving forward innumerable essential health systems improvements: quality improvement, health systems planning, healthcare fraud, waste and abuse detection, and medical/public health research, including comparative effectiveness research, adverse drug event monitoring, patient safety improvements and the reduction health disparities.

Sincerely,

A handwritten signature in black ink, appearing to read "Daniel C. Barth-Jones". The signature is stylized with a large, prominent 'D' and 'B'.

Daniel C. Barth-Jones, MPH/PhD

Assistant Professor of Clinical Epidemiology

Department of Epidemiology

Mailman School of Public Health

Columbia University

Message

From: Chris Hoofnagle [REDACTED]
Sent: 3/8/2019 3:45:28 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Attachments: ccpa_comments_final.pdf

Dear Attorney General Becerra, please fine my comments on the CCPA attached. Chris

Chris Jay Hoofnagle
Adjunct Professor
UC Berkeley School of Information & School of Law
<https://hoofnagle.berkeley.edu/>



March 8, 2019


VIA Email

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

CHRIS JAY HOOFNAGLE
Adjunct Full Professor
School of Information
School of Law

Faculty Director
Berkeley Center for Law & Technology

University of California, Berkeley
102 South Hall
Berkeley, CA 94720-4600


<https://hoofnagle.berkeley.edu>

Re: Comments on Assembly Bill 375, the California Consumer Privacy Act of 2018

Dear Attorney General Becerra,

I helped conceive of the high-level policy goals of the privacy initiative that was withdrawn from the ballot with passage of AB 375. Here I provide comment to give context and explain the high-level policy goals of the initiative, in hopes that it helps your office in contemplating regulations for the CCPA.

Strong policy support for the initiative

As you interpret the CCPA, please bear in mind that the initiative would have passed because Americans care about privacy. In multiple surveys, Americans have indicated support for stronger privacy law and dramatic enforcement. Americans have rarely been able to vote directly on privacy, but when they do, they overwhelmingly support greater protections. One example comes from a 2002 voter referendum in North Dakota where 73% of citizens voted in favor of establishing opt-in consent protections for the sale of financial records.¹

A series of surveys performed at Berkeley found that Americans wanted strong penalties for privacy transgressions. When given options for possible privacy fines, 69% chose the largest option offered, "more than \$2,500," when "a company purchases or uses someone's personal information illegally." When probed for nonfinancial penalties, 38% wanted companies to fund efforts to help consumers protect their privacy, while 35% wanted executives to face prison terms for privacy violations.

Information is different

The CCPA is unusually stringent compared to other regulatory law because information is different from other kinds of services and products. When a seller makes an automobile or a refrigerator, the buyer can inspect it, test it, and so on. It is difficult for the seller to change a physical product. Information-intensive services however are changeable, they are abstract, and since we have no physical experience with information, consumers cannot easily see the flaws and hazards of them in the way one could see an imperfection in a car's hood.

¹ North Dakota Secretary of State, Statewide Election Results, June 11, 2002.



Because information services can be changed, privacy laws tend to become stringent. Information companies have a long history of changing digital processes to trick consumers and to evade privacy laws in ways that physical product sellers simply could not.²

Some of the CCPA's most derided provisions (e.g. application to household level data) are in response to specific evasions of industries made possible because information is different than product regulation. Here are common examples:

- Sellers claim not to sell personal data with third parties, but then go on to say we "may share information that our clients provide with specially chosen marketing partners."³ For this reason, the initiative tightened definitions and required more absolute statements about data selling. Companies shouldn't use the word "partner" or "service provider" to describe third party marketers.
- Companies have evaded privacy rules by mislabeling data "household-level information." For instance, the DMA long argued that phone numbers were not personal data because they were associated with a household.
- Many companies use misleading, subtle techniques to identify people. For instance, retailers asked consumers their zip code and used this in combination with their name from credit card swipes to do reverse lookups at data brokers.⁴
- Information companies use technologies such as hash-matching to identify people using "non personal" data.⁵

Careful study of information-industry tricks informed the initiative and resulted in a definitional landscape that attempts to prevent guile. Those complaining about it need only look to the industry's own actions to understand why these definitions are in place. For your office, this means that regulations must anticipate guile and opportunistic limitations of Californians' rights.

The advantages of privacy markets

Creating markets for privacy services was a major goal of the initiative. The ability to delegate opt out rights, for instance, was designed so that Californians could pay a for profit company (or even donate to a non-profit such as EFF) in order to obtain privacy services.

There are important implications of this: *first, the market-establishing approach means that more affluent people will have more privacy.* This sounds objectionable at first, but it is a pragmatic and ultimately democratizing pro-privacy strategy. A market for privacy cannot emerge without privacy regulation to set a floor for standards and to make choices enforceable. Once privacy services emerge, because they are information services and because they can scale, privacy services will become inexpensive very quickly. For instance, credit monitoring and fraud alert services are only available because of rights given to consumers in the Fair Credit Reporting Act that can be easily invoked by third party privacy services. These services have become very inexpensive and are used by tens of millions of Americans.

Some will argue that the CCPA will kill "free" business models and this will be iniquitous. This reasoning underestimates the power of markets and presents free as the only solution to news. The reality is much more complex. Digital advertising supported services do democratize news access, however, they also degrade quality. One cost of the no-privacy, digital advertising model is fake news. Enabling privacy will improve quality and this could have knock-on effects.

² Hoofnagle et al., *Behavioral Advertising: The Offer You Can't Refuse*, 6 Harv. L. & Pol'y Rev. 273 (2012).

³ Jan Whittington & Chris Hoofnagle, *Unpacking Privacy's Price*, 90 N.C. L. Rev. 1327 (2011).

⁴ *Pineda v. Williams Sonoma*, 51 Cal.4th 524, 2011 WL 446921.

⁵ <https://www.clickz.com/what-axiom-hash-figured-out/31429/> and <https://developer.myaxiom.com/code/api/endpoints/hashed-entity>

Second, the market strategy relieves pressure on your office. The market strategy means that the AG does not have to solve all privacy problems. (That is an impossible standard to meet and perfection has become a standard preventing us from having any privacy.)

Instead, the AG need only set ground rules that allow pro-privacy services to function effectively. A key ground rule that you should promote is a minimally burdensome verification procedure, so that pro-privacy services can scale and can easily deliver opt out requests. For instance, in the telemarketing context, the FTC made enrolling in the Do-Not-Call Registry simple because it understood that complexifying the process would result in lower enrollment.

There is almost no verification to enroll in the Do-Not-Call Registry and this is a deliberate policy choice. One can enroll by simply calling from the phone number to be enrolled, or by visiting a website and getting a round-trip email. What this means is that online, a consumer can enroll any phone number, even one that is not theirs, so long as they provide an email address. The FTC does not run email/phone number verification.

The low level of verification in the Do-Not-Call Registry is a reflection of two important policy issues: first, excessive verification imposes transaction costs on consumers, and these costs are substantial. Second, the harm of false registrations is so minimal that it is outweighed by the interest in lowering consumer transaction costs. Most people are honest and there is no evidence of systematic false registrations in the Do-Not-Call Registry. More than 200 million numbers are now enrolled.

The AG should look to the FTC's approach and choose a minimally invasive verification procedure for opt out requests that assumes 1) that most Californians are honest people and will not submit opt out requests without authority, and 2) that verification stringency imposes a real, quantifiable cost on consumers. That cost to consumers is likely to outweigh the interest of sellers to prevent false registrations. In fact, excessive verification could kill the market for privacy services and deny consumers the benefit of the right to opt out. A reasonable opt out method would be one where a privacy service delivers a list of identifiable consumers to a business, for instance through an automated system, or simply a spreadsheet of names and email addresses.

The AG should look to Catalog Choice as a model for opt outs. Catalog Choice has carefully collected all the opt out mechanisms for paper mail marketing catalogs. A consumer can sign up on the site, identify catalogs to opt out from (9,000 of them!), and Catalog Choice sends either an automated email or a structured list of consumers to sellers to effectuate the opt out. This service is free. Data feeds from Catalog Choice are even recognized by data brokers as a legitimate way for consumers to stop unwanted advertising mail. Catalog choice performs no verification of consumer identity. Again, this is acceptable, because the harm of a false opt-out is negligible, and because deterring that harm would make it impossible for anyone to opt out efficiently.

I served on the board of directors of Catalog Choice for years and recall no incidents of fraudulent opt outs. The bigger problem was with sellers who simply would not accept opt outs. A few would summarily deny them for no reason other than that allowing people to opt out harmed their business model, or they would claim that Catalog Choice needed a power of attorney to communicate a user's opt out. The AG should make a specific finding that a power of attorney or any other burdensome procedure is not necessary for delivering verified opt out requests.

The AG should assume that sellers will use guile to impose costs on opt out requests and to deter them. Recall that when consumer reporting agencies were required to create a free credit report website, CRAs used technical measures to block people from linking to it, so that the consumer had to enter the URL to the website manually. CRAs also set up confusing, competing sites to draw consumers away from the free one. The FTC actually had to amend its rule to require this disclosure on all "free" report sites.

THIS NOTICE IS REQUIRED BY LAW. Read more at [FTC.GOV](https://www.ftc.gov).

You have the right to a free credit report from AnnualCreditReport.com or 877-322-8228, the **ONLY** authorized source under federal law.

The definition of sell

The definition of sell in the CCPA reflects the initiative's broad policy goal of stopping guile in data "sharing."

From a consumer perspective, any transfer of personal information to a third party for consideration is a *sale* (subject to exceptions for transactional necessity, etc). But the information industry has interpreted "sale" to only mean transfers for money consideration. That is an unfounded, ahistorical interpretation.

The initiative sought to reestablish the intuitive contract law rule that any transfer for value is the "consideration" that makes a data exchange a sale. In the information industry's case, that valuable consideration is often a barter exchange. For instance, in data cooperatives, sellers input their own customer list into a database in exchange for other retailers' data.⁶ Under the stilted definition of "sale" promoted by the information industry, that is not data selling. But from a consumer perspective, such cooperative "sharing" has the same effect as a "sale."

Recent reporting about Facebook makes these dynamics clearer in the online platform context.⁷ Properly understood, Facebook sold user data to application developers. If application developers enabled "reciprocity" or if developers caused "engagement" on the Facebook platform, Facebook would give developers access to personal data. From a consumer perspective, users gave their data to Facebook, and Facebook transferred user data to third parties, in exchange for activity that gave economic benefit to Facebook. That's a sale. The AG should view transfers of personal information for value, including barter and other exchange, as "valuable consideration" under the CCPA. Doing so will make the marketplace more honest and transparent.

Disclosures that consumers understand

*Over 60% of Americans believes that if a website has a privacy policy, it cannot sell data to third parties.*⁸

I have come to the conclusion, based on a series of 6 large scale consumer surveys and the extensive survey work of Alan Westin, that the term "privacy policy" is inherently misleading. Consumers do not read privacy policies. They see a link to the privacy policy, and they conclude "this website must have privacy." My work is consonant with Alan Westin's, who over decades of surveys, repeatedly found that most consumers think businesses handle personal data in a "confidential way." Westin's findings imply that consumers falsely believe that there is a broad norm against data selling.

In writing consumer law, one can't take a lawyer's perspective. Consumers do not act nor do they think like lawyers. Lawyers think the issue is as simple as reading a disclosure. But to the average person, the mere

⁶ From Nextmark.com: "co-operative (co-op) database a prospecting database that is sourced from many mailing lists from many different sources. These lists are combined, de-duplicated, and sometimes enhanced to create a database that can then be used to select prospects. Many co-op operators require that you put your customers into the database before you can receive prospects from the database.

⁷ Chris Hoofnagle, Facebook and Google Are the New Data Brokers, Cornell Digital Life Initiative (2018) <https://www.dli.tech.cornell.edu/blog/facebook-and-google-are-the-new-data-brokers>

⁸ Chris Jay Hoofnagle and Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 Wake Forest Law Review 261 (2014).

presence “privacy policy” means something substantive. It looks more like a quality seal (e.g. “organic”) rather than an invitation to read.

This is why the initiative and the CCPA go to such extraordinary measures to inform consumers with “Do not sell my personal information” disclosures. Absent such a clear and dramatic disclosure, consumers falsely assume that sellers have confidentiality obligations.

The CCPA is trying to thread a needle between not violating commercial speech interests and disabusing consumers of data selling misconceptions. These competing interests explain why the CCPA is opt-out for data selling. CCPA attempts to minimize impingement on commercial free speech (in the form of data selling) while also informing consumers of businesses’ actual practices.

Let me state this again: the government interest in commanding the specific representation “Do not sell my personal information,” is necessary to both 1) disabuse consumers of the false belief that services are prohibited from selling their data, and 2) to directly tell consumers that they have to take action and exercise the opt out under CCPA. It would indeed make more sense from a consumer perspective for the CCPA to require affirmative consent. But since that may be constitutionally problematic, the CCPA has taken an opt out approach, along with a strong statement to help consumers understand their need to take action. Without a visceral, dramatic disclosure, consumers will not know that they need to act to protect their privacy. **Your regulatory findings should recite these value conflicts, and the need for compelled speech in order to correct a widespread consumer misconception.**

Data brokers and opting out

Vermont law now requires data brokers to register, and its registry should help Californians locate opt out opportunities. However, the AG can further assist in this effort by requiring a *standardized textual disclosure* that is easy to find using search engines. Standardized is important because businesses tend to develop arbitrary terminology that has no meaning outside the industry. Text is important because it is easier to search for words than images, and because logo-based “buttons” carry arbitrary or even conflicting semiotic meaning.

Non-discrimination norms

Section §125 of the CCPA is the most perplexing, yet it is harmonious with the overall intent of the initiative to create markets. My understanding of §125 is that it seeks to 1) prevent platforms such as Facebook from offering a price that is widely divergent from costs. For instance, Facebook’s claims its average revenue per user (ARPU) is about \$100/year in North America. The CCPA seeks to prevent Facebook from charging fees that would be greatly in excess of \$10/month. Thus, the AG could look to ARPU as a peg for defining unreasonable incentive practices. 2) CCPA was attempting to prevent the spread of surveillance capitalism business models into area where information usually is not at play, for instance, at bricks and mortar businesses.

One area to consider under §125 are the growing number of businesses that reject cash payment. These businesses are portrayed as progressive but actually the practice is regressive (consumers spend more when they use plastic, the practice is exclusionary for the unbanked, it subjects consumers to more security breaches, and it imposes a 3% fee on all transactions). Consumers probably do not understand that modern payment systems can reidentify them and build marketing lists. The privacy implications of digital payments are not disclosed nor mitigated, and as such, bricks and mortar businesses that demand digital payment may be coercive under CCPA.

Pro-privacy incentives

Privacy laws present a paradox: schemes like the GDPR can induce companies to use data more rather than less. This is because the GDPR’s extensive data mapping and procedural rules may end up highlighting

unrealized information uses. The CCPA can avoid this by creating carrots for privacy-friendly business models, something that the GDPR does not do.

The most attractive carrot for companies is an exception that broadly relieves them of CCPA duties. The AG should make the short term transient use exemption the most attractive and usable one. That exception should be interpreted broadly and be readily usable by those acting in good faith. For instance, short-term uses should be interpreted to include retention up to 13 months so long as the data are not repurposed. The broad policy goals of the CCPA are met where an exception gives companies strong pro-privacy incentives. There's no better one than encouraging companies to only collect data it needs for transactions, and to only keep it for the time needed to ensure anti-fraud, seasonal sales trend analysis, and other service-related reasons. For many businesses, this period is just in excess of one year.

Respectfully submitted,

/Chris Hoofnagle

Chris Jay Hoofnagle*

Adjunct full professor of information and of law

UC Berkeley

*Affiliation provided for identification purposes only

Message

From: Tobin, Timothy P. [REDACTED]
Sent: 3/8/2019 3:25:29 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA
Attachments: Auto Alliance Correspondence re CCPA to California Department of Justice....pdf

To Whom it May Concern:

Please find attached comments on the CCPA by the Alliance of Automobile Manufacturers (the "Auto Alliance").

Regards,

Timothy Tobin

Partner

Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004

Tel: [REDACTED]
Direct: [REDACTED]
Fax: [REDACTED]
Email: [REDACTED]
Blog: www.hidataprotection.com
www.hoganlovells.com

Please consider the environment before printing this e-mail.

About Hogan Lovells

Hogan Lovells is an international legal practice that includes Hogan Lovells US LLP and Hogan Lovells International LLP. For more information, see www.hoganlovells.com.

CONFIDENTIALITY. This email and any attachments are confidential, except where the email states it can be disclosed; it may also be privileged. If received in error, please do not disclose the contents to anyone, but notify the sender by return email and delete this email (and any attachments) from your system.



AUTO ALLIANCE

DRIVING INNOVATION™

803 7th Street N.W., Suite 300 | Washington, DC 20001

www.autoalliance.org

March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

RE: Comments of the Alliance of Automobile Manufacturers on the California Attorney General's Rulemaking Pursuant to the California Consumer Privacy Act

To Whom It May Concern:

The California Consumer Privacy Act ("CCPA") directs the California Attorney General to promulgate regulations on various specified topics and as necessary to further the purposes of the CCPA. As part of its preliminary activities in the rulemaking process, the Attorney General's Office has invited public comments. The Alliance of Automobile Manufacturers ("Alliance") welcomes the opportunity to provide these comments ("Comments") to the Attorney General's Office.

The Alliance is the leading advocacy group for the auto industry, representing 12 member companies that account for approximately 70 percent of all car and light truck sales in the United States. The members of the Alliance include (alphabetically) the BMW Group, Fiat Chrysler Automobiles, Ford Motor Company, General Motors Company, Jaguar Land Rover, Mazda, Mercedes-Benz USA, Mitsubishi Motors, Porsche, Toyota, Volkswagen Group of America, and Volvo Car USA.

In these Comments, the Alliance describes its members' commitments to consumer privacy and the significant steps that the Alliance and its members have already taken to establish comprehensive protections for consumers. We then set forth specific comments for the Attorney General to consider when developing CCPA regulations.

The Auto Industry's Commitment to Privacy

Automakers are driving innovation and continually seeking to enhance vehicle safety, vehicle performance, and convenience to consumers. Connected and automated vehicle technologies hold great promise to provide a range of benefits to consumers and society, such as crash avoidance, emergency response, congestion mitigation, reduced fuel consumption, vehicle health reports, and infotainment services. The development and delivery of such technologies,

however, relies on the collection and analysis of information collected from vehicle systems.

Automakers have long recognized the potential privacy considerations raised by this data collection and have taken proactive steps to protect consumer privacy. In 2014, the Alliance, the Association of Global Automakers (a trade association representing U.S. operations of certain international vehicle manufacturers and original equipment suppliers), and their respective members issued the Privacy Principles for Vehicle Technologies and Services ("Principles").¹ The Principles were groundbreaking. The Alliance's members have all committed to meet or exceed the commitments contained in the Principles when offering innovative vehicle technologies and services. Specifically, the Principles establish requirements for the collection, use, and sharing of information in association with vehicle technologies and services available on cars and light trucks sold or leased to individual consumers for personal use in the United States. "Covered Information," under the Principles, includes identifiable information that vehicles collect, generate, record, or store, that is retrieved from the vehicle by the automaker, as well as personal subscription information provided by individuals subscribing or registering for vehicle technologies and services.

The Principles are built around the internationally recognized Fair Information Practice Principles ("FIPPs"), and are designed to be flexible so that automakers can tailor them to their specific needs, reflecting differences in technologies and other distinguishing or company-specific factors. The Principles went into effect for Participating Members in 2016 with full implementation required no later than vehicle Model Year 2018. There are 20 Participating Members—including all members of the Alliance—representing 99.7 percent of car and light duty truck sales in the United States.² All Participating Members are subject to enforcement by the Federal Trade Commission ("FTC") under its Section 5 authority for unfair and deceptive business practices if they fail to abide by the commitments made in the Principles.

By committing to the Principles, Participating Members have voluntarily taken on or exceeded many of the obligations addressed under the CCPA. For example, like the CCPA, the Principles require Participating Members to describe in privacy notices the types of Covered Information that will be collected, the purposes for collecting Covered Information, and the types of entities that may receive Covered Information.³ Participating Members have also committed to

¹ Consumer Privacy Protection Principles (2014) [hereinafter "Principles"], *available at* https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf.

² For the full list of Participating Members, see <https://autoalliance.org/connected-cars/automotive-privacy/participating-members/>

³ Principles, *supra* note 1, at 7.

obtain affirmative consent for the sharing of geolocation, biometric, or driving behavior information with unaffiliated third parties for their own use.⁴ This goes beyond the sales opt-out requirement established under the CCPA. Participating Members also have committed to obtain affirmative consent before using geolocation, biometric, or driving behavior information for first-party marketing, which the CCPA does not address.

As the Principles demonstrate, U.S. automakers have committed to providing consumers with substantial privacy protections. U.S. automakers recognize that the California legislature and the Office of the Attorney General have, in enacting the CCPA and developing implementing regulations, respectively, embraced a similar commitment. However, the privacy protections embodied in the CCPA have the potential to create undue privacy risk and impede the development and delivery of innovative and highly beneficial technologies and services unless reasonable interpretations of and exceptions to CCPA requirements are recognized.

Connected and highly automated vehicle technologies raise a unique set of issues for privacy regulations. These technologies have the potential to save lives, reduce environmental impacts, and deliver substantial consumer benefits. They do so by collecting and processing location information, vehicle usage and system status information, and emergency response or crash signals. The vehicles from which the data is collected may be owned by families or participate in ride- or vehicle-sharing programs, creating challenges in determining who should properly be linked to a vehicle. Automakers collect and share vehicle data to deliver needed services, sell vehicles, conduct research on motor vehicle safety, improve vehicle safety and efficiency, and to understand and continue developing the technologies that will lead to fully automated and other beneficial mobility outcomes. The recipients of the data include not only automakers, but emergency response and roadside assistance providers, suppliers of vehicle parts and systems, and authorized dealers. Absent reasonable regulations to implement the CCPA, the statute risks:

- Requiring automakers to disclose vehicle location information to abusive spouses or other bad actors who wish to use the information to harm or harass co-users of vehicles;
- Endangering consumer safety by prohibiting automakers from sharing personal information with private, unaffiliated emergency response providers when owners have opted out of the sale of personal information;

⁴ *Id.* at 8.

- Requiring automakers to comply with consumer requests to access or delete vehicle data when the requestors have no true ownership interest in the vehicles that are associated with the requests;
- Preventing automakers from engaging in vital motor vehicle safety and performance research that relies on longitudinal and vehicle-specific data, even where reasonable steps are taken to deidentify vehicle data;
- Preventing, following an opt-out request, automakers from sharing personal information with suppliers and authorized dealers as reasonably necessary to support product improvement and the efficient delivery of repair and warranty services;
- Requiring automakers to divulge trade secrets when disclosing the specific pieces of information collected by highly automated vehicle systems or other connected vehicle technologies;
- Preventing automakers from offering reasonable financial incentive programs to consumers in association with mobility services that may be subsidized by data sharing arrangements; and
- Requiring automakers to implement substantial resources to comply with the CCPA for vehicle data that is collected and retained on vehicles without being transmitted to automakers.

To avoid these results, the Alliance respectfully requests that the Attorney General draft regulations that account for the comments below, particularly in light of the substantial steps that U.S. automakers have taken to protect consumer privacy, and the considerable public benefits that connected vehicle technologies offer.

Requests and Comments

(1) To protect consumer privacy and prevent bad actors from obtaining sensitive information, permit businesses to provide, at their option, summaries of personal information collected in response to access requests where disclosing specific pieces of personal information could put consumers at risk of harm

Much of the information that automakers collect is tied to vehicles, rather than individuals. In particular, automakers often use the Vehicle Identification Number ("VIN") to identify the vehicle from which information is collected. When looking at records tied to a vehicle, automakers may have little insight into who was driving the vehicle at the time that the information was collected. For example, when providing navigation services, an automaker may know where a vehicle

was at the time a driver or passenger requested services. But the automaker may have no information regarding who made the request. This helps promote privacy as automakers are able to provide services to specific vehicles without processing information that is directly tied to a specific person.

Surprisingly, the lack of a direct link to specific persons driving or riding in a vehicle could increase privacy concerns in the context of CCPA access rights. The CCPA provides consumers the right to access the “specific pieces of personal information” a business has collected about them.⁵ Vehicle-level data could be considered personal information if tied to a specific person, such as the vehicle owner. But vehicle-level data may reflect information regarding a range of vehicle operators or passengers—the owner, the owner’s spouse, the owner’s ex-spouse, children, and guests, among others. If automakers were required in response to an access request to provide vehicle owners with all of the information that could reasonably be tied to the vehicle, that could result in automakers, to the extent they possess such information, disclosing precise location information, detailed vehicle status information, and detailed service requests that would reveal the personal information of other individuals.

Such disclosures could create stalking or harassment risks, endangering individual or public safety, or it may otherwise adversely impact the privacy rights of non-owners. Specifically, if an automaker disclosed precise location information to a vehicle owner on grounds that the information is reasonably tied to the owner by virtue of the ownership relationship, that could enable an abusive individual to track and harm an estranged spouse, domestic partner, or others.⁶

The Alliance asks the Attorney General to clarify, as the CCPA contemplates, that automakers, and other businesses that process information associated with devices that are frequently operated by multiple users, are not required to provide in response to an access request specific pieces of personal information that have the potential to “adversely affect the rights and freedoms of other consumers.”⁷ The Attorney General has the authority to do so given its mandate to issue regulations as necessary to further the purposes of the CCPA⁸ and to establish reasonable procedures and exceptions regarding the information businesses provide to consumers.⁹

⁵ Cal. Civ. Code § 1798.100(a).

⁶ See, e.g., <https://www.theguardian.com/lifeandstyle/2015/jan/25/spyware-smartphone-abusive-men-track-partners-domestic-violence>.

⁷ Cal. Civ. Code § 1798.145(j) (“The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.”).

⁸ *Id.* at § 1798.185(b).

⁹ *Id.* at § 1798.185(a)(6).

In lieu of requiring businesses to provide specific pieces of personal information in such circumstances, the Attorney General could clarify that businesses may provide reasonable summaries or aggregated compilations of the personal information that the businesses have collected, which would enable consumers to reasonably assess the business's processing of personal information.

(2) Permit automakers to share personal information with third-party emergency response and roadside assistance providers to provide services to consumers who have opted out of the sale of personal information

If consumers have opted out of the sale of their personal information, the broad CCPA concept of sale could needlessly endanger vehicle occupants, potentially causing death or exacerbating injuries by preventing automakers from providing prompt emergency response or roadside assistance services following an accident. Many automakers share personal information with third-party entities that provide emergency response or roadside assistance services. Such services may include mechanical, medical, or security services. Some of the entities providing such services may be for-profit entities that retain and use the information for their own purposes (e.g., independent repair services that may use personal information to maintain relationships with consumers after the provision of services).

When automakers share personal information with such entities, some arrangements could be viewed as sales under the CCPA.¹⁰ To dispatch services to remote areas, automakers may need to engage providers with which they have no prior relationship. Or it may be that the providers of vital emergency services are not willing to position themselves as mere service providers given their direct interactions with consumers and the pricing they offer by virtue of knowing they will have such interactions. If a consumer opts out of an automaker's sale of personal information and subsequently requests emergency response or roadside assistance, the prior opt out could potentially prevent the sharing of personal information with the assistance providers absent the consumer's express authorization.¹¹ However, in many scenarios, such as emergency or late-night situations, it may not be feasible to obtain express authorization for the sale. Disrupting the sharing of personal information that is needed to support the provision of emergency response or roadside assistance

¹⁰ *Id.* at § 1798.140(t).

¹¹ *Id.* at § 1798.120(d) ("A business that has received direction from a consumer not to sell the consumer's personal information ... shall be prohibited ... from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.").

services (e.g., sharing precise location, name, and nature of the incident) may adversely affect the delivery of such services.

The Alliance therefore requests that the Attorney General, pursuant to its authority to issue rules and procedures for compliance with a consumer's opt-out request,¹² clarify that automakers may, in response to a consumer's request for emergency or roadside assistance services, or based on an automated crash notification, share personal information with emergency response or roadside assistance providers and other entities providing similar services even after an opt-out request has been received. Although the consumer may not be able to provide a traditional, express authorization for the sharing, the triggering of crash notification or similar trigger should be deemed an express authorization in such circumstances.

(3) Establish rules and procedures clarifying that only vehicle owners have rights to request access to and the deletion of vehicle data

As discussed in Section (1) above, automakers may retain vehicle-level data tied to VINs or other identifiers. Vehicle data may include information relating to the use of a vehicle by non-owners—potentially many non-owners. Spouses, children, other family members, and valets may be among the many users of a vehicle. The CCPA grants consumers the right to request access to and the deletion of personal information the business has collected about the consumer.¹³

Allowing guest users to exercise access and deletion rights with regard to vehicle data may affect the rights of other individuals, particularly the vehicle owner. A guest driver who misuses a vehicle may wish to delete evidence of such misuse. The vehicle owner may have paid for certain services (e.g., geofencing or vehicle history services) specifically to identify such misuse. In providing guest users with vehicle data, automakers risk divulging information about another user's interactions with the vehicle. An employee driving a fleet vehicle might request access to vehicle data in order to track colleagues' movements. Or the employee, seeking to launch a business competing with the current employer, could request vehicle data in order to obtain proprietary information revealed by vehicle data (e.g., delivery routes and client visits).

Further complicating these issues is the fact that automakers, as discussed above, may have no information identifying who used a vehicle at a specific time. To comply with requests from non-owners, therefore, automakers might need to collect and process personal information beyond that needed to provide vehicle

¹² *Id.* at § 1798.185(a)(4)(B).

¹³ *Id.* at § 1798.105.

services. Moreover, as described further in Section (1) above, access rights may be used in ways that harm others' rights and freedoms.

The Alliance therefore requests that the Attorney General, pursuant to its authority to establish rules and procedures governing responses to consumer requests,¹⁴ clarify that only the registered vehicle owner may request access to or the deletion of data tied to the vehicle. Permitting guest drivers or occupants to exercise rights over the data may adversely affect the owner, and the mere fact that someone uses a device should not establish rights relating to information associated with the device.

(4) Establish robust verification standards for access and deletion requests related to vehicle data

The CCPA authorizes the Attorney General to establish rules and procedures governing how businesses should determine whether a consumer request is a verifiable consumer request.¹⁵ In the automobile context, insufficiently verified requests could create safety risks or disrupt services. As discussed in Section (1), above, vehicle data may be associated with multiple consumers, including owners, guest drivers, and occupants. Disclosing vehicle data to an unauthorized person, or to a person who has used but does not own a vehicle, risks compromising the safety and privacy interests of vehicle owners and other users of the vehicle. As discussed in Section (3), above, vehicle owners have a substantial interest in maintaining vehicle data to support the provision of desired services. Deleting vehicle data in response to a request from someone other than the vehicle owner could adversely affect the owner's ability to obtain desired services, for example, vehicle health reports or diagnostics that rely on longitudinal histories of vehicle performance.

Because of the risks associated with complying with access or deletion requests from unauthorized individuals, the Alliance requests that the Attorney General establish rules and procedures that enable automakers to apply robust standards when assessing whether a consumer request to access or delete vehicle data is verifiable. At minimum, consumers should have to provide proof of vehicle ownership (or owner authorization) and proof of identity in support of any deletion or access requests.

¹⁴ *Id.* at § 1798.185(a)(7).

¹⁵ *Id.*

(5) Permit businesses to retain personal information for research, including research to support the development of life-saving technologies, particularly where consistent with privacy notices

The CCPA provides consumers with the right to request that businesses delete personal information businesses have collected from the consumers.¹⁶

Automakers use vehicle-level data they collect for analysis related to motor vehicle safety, performance, and security, including for future security improvements and to assess how historical vehicle use may affect safety and performance. This data, including information that vehicles may collect regarding the external environment (e.g., road conditions), is particularly crucial to the development, training, implementation, and assessment of automated vehicle technologies. These technologies include crash avoidance technologies, such as blind spot detection, adaptive cruise control, automatic emergency breaking, and lane assist. In many cases, automakers may need to analyze the information over time, as longitudinal assessments enable automakers to assess how past use may affect future safety, security, and performance. The data collected for research and development of such technologies is frequently tied to VINs or other vehicle identifiers and could, in certain circumstances, be viewed as personal information in that it may be possible to link the information to the owner or a registered user of a vehicle or vehicle services.

Automakers recognize that deleting information that is directly tied to a consumer may be a reasonable means of protecting privacy. However, deletion is not practicable in all circumstances. If, automakers are required, in response to a deletion request, to delete all information that could reasonably be linked to a vehicle, that would result in depriving automakers and automotive researchers from using the information to develop, test, and deploy vehicles and technologies that promise to deliver substantial life-saving, environmental, and societal benefits.

The CCPA enumerates a number of circumstances under which a business need not comply with a deletion request. Such exceptions include when the information is necessary to:

(7) . . . enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.
[. . .]

¹⁶ *Id.* at § 1798.105(a).

(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.¹⁷

The Alliance asks the Attorney General, pursuant to its authority under the CCPA to establish rules and procedures governing responses to consumer requests,¹⁸ to clarify that where a business has disclosed in its privacy notice how vehicle data will be processed for research purposes related to motor vehicle safety, performance, efficiency, convenience, or security, such research will be deemed internal uses reasonably aligned with the expectations of the consumer or otherwise compatible with the context in which the consumer provided the information.

(6) Clarify that information will be considered deidentified so long as it cannot reasonably be used to identify a consumer—the mere possibility of reidentification should not be sufficient to demonstrate that information is not deidentified

Section 1798.145(a)(5) states that the CCPA "shall not restrict a business's ability to . . . [c]ollect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information."¹⁹ The Alliance requests that the Attorney General, pursuant to its authorization to adopt regulations as necessary to further the purposes of the CCPA,²⁰ issue regulations clarifying that data that does not reasonably identify a specific person will be considered "deidentified" data. In doing so, the Attorney General would enhance the ability of automakers and other organizations to analyze data for socially beneficial uses while also protecting consumer privacy.

The CCPA definition of "deidentified" could be interpreted to mean that any information maintained at the individual level (i.e., any information not aggregated across multiple users) would be considered personal information. Establishing such a standard would render the concept of deidentified data superfluous. And the standard would impose substantial and unnecessary compliance burdens on companies that seek to engage in beneficial uses of individual-level data, like research and product improvement, while mitigating privacy risk by using deidentified data.

The CCPA defines "deidentified" information as "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or

¹⁷ *Id.* at § 1798.105(d).

¹⁸ *Id.* at § 1798.185(a)(7).

¹⁹ *Id.* at § 1798.145(a).

²⁰ *Id.* at § 1798.185(b).

be linked, directly or indirectly, to a particular consumer," so long as the business using the deidentified information implements technical and administrative safeguards to prevent reidentification and makes no attempt to reidentify the information.²¹ If "reasonably" is interpreted to apply only to "identify" in the definition of "deidentified" information, then deidentification of individual-level data is impossible. With sophisticated techniques or additional data sets, almost any information is "capable" of being associated with a particular consumer. For individual-level data, there may frequently be a mathematical possibility that a researcher devoting substantial time and resources could associate information with the consumer to whom it relates. If deidentification is assessed without reference to the reasonableness of identification, including internal company safeguards, "deidentified information" would be a class without any members—all individual-level data would be personal information.

The Alliance therefore requests that the Attorney General clarify that "reasonably" qualifies all of the terms that follow it in the defining sentence and not just the term "identify." In doing so, the Attorney General will clarify that the CCPA should not be interpreted to render the category of deidentified data a nullity and establish that the CCPA approach to deidentification will be consistent with the well-established FTC approach discussed below. To further the clear purpose of the CCPA in establishing a definition of "deidentified information," the Alliance requests that the Attorney General clarify that information is deidentified so long as it is maintained and used in a manner that does not reasonably support identification and so long as the appropriate safeguards are in place.

For example, automakers may collect vehicle-level data for research and development purposes related to motor vehicle safety, security, or product improvement and efficiency. Automakers may need to track vehicle-level data over time to understand system performance or wear and tear, or for other socially beneficial purposes such as better understanding environmental impacts. Vehicle-level data may be needed for government programs such as California's new Clean Fuel Rewards Program, which mandates that automakers track where electronic vehicles are charged. And automakers may need to conduct vehicle-level analysis by tying vehicle data to VINs or unique, internal identifiers that allow longitudinal tracking. Where automakers do not maintain or link this data to customer relationship management ("CRM") databases; do not otherwise associate it with traditional identifiers such as name, address, phone number, email address, etc.; have technical and administrative safeguards reasonably designed to prevent reidentification of the information; and prohibit and make no attempt to identify the individuals associated with the information, such vehicle-specific information should be considered deidentified.²²

²¹ *Id.* at § 1798.140(h).

²² *See id.*

Treating all vehicle-specific data as personal information would perversely create no incentive for automakers to implement deidentification safeguards, such as disabling links between vehicle-specific data and traditional identifiers in CRM databases. The vehicle-specific information would be deemed personal information, subject to the full range of CCPA obligations, regardless of its link to CRM data. In fact, if all vehicle-specific data were considered personal information, automakers would have strong incentives to maintain links between the vehicle data and the traditional identifiers in CRM databases, therefore increasing privacy risk. Further, if all vehicle-specific information were to be deemed personal information, that could require automakers to divert significant resources from safety and product improvement research to support identifying, tracking, and producing or deleting such information in response to a consumer's access or deletion request.

Confirming a reasonableness standard for deidentification would reflect the guidance issued by the FTC in its 2012 privacy report. The FTC recognized that data that is not reasonably linkable to a specific consumer or device, taking into account internal and contractual safeguards, does not need to be subject to the same privacy protections as personal information.²³ Moreover, the FTC Staff Report regarding the Internet of Things notes that deidentification of data that persists in an individual-level manner is valuable in that it can promote beneficial uses of information while establishing reasonable privacy protections.²⁴

By clarifying that deidentification is assessed based on the reasonableness of identifying individuals, rather than on the hypothetical potential for reidentification, the Attorney General would enable automakers to engage in valuable motor vehicle safety, security, and efficiency research while taking reasonable steps to protect consumer privacy in regard to identifiable information.

(7) Permit automakers to continue sharing personal information with authorized dealers and suppliers to support services that benefit consumers and motor vehicle safety after receiving opt-out requests

The CCPA provides consumers the right to opt out of "sales" of their personal information.²⁵ The definition of "sale" captures the sharing of personal information with unaffiliated third parties for consideration, which is potentially

²³ See FTC, Protecting Consumer Privacy in an Era of Rapid Change 20-22 (2012), available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

²⁴ See FTC Staff, Internet of Things: Privacy and Security in a Connected World 37-39 (2015), available at <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>.

²⁵ Cal. Civ. Code § 1798.120(a)-(b).

subject to a broad interpretation that might impact complicated, decades-long relationships.

Automakers, independent dealerships, and suppliers share information for purposes that benefit consumers and the public. Sharing vehicle information enables dealerships to access full repair histories for vehicles, makes it easier for consumers to obtain services from multiple dealerships, enables suppliers to use vehicle-level data to improve safety, security, and performance for vehicle parts and systems, and allows suppliers and dealers to share vehicle- or part-related information with automakers for safety, security, warranty, or other purposes. These sharing relationships could be viewed as sales as automakers, dealers, and suppliers generally are not affiliated, and the recipients may be authorized to use the information for their own purposes.

As such, a request to opt-out of the sale of personal information may disrupt the sharing of information between automakers, suppliers, and authorized dealers and may complicate automakers' efforts for compliance with other laws such as auto franchise laws. Such disruption may be contrary to consumer interests.

Due to the common branding shared by automakers and their authorized dealers, consumers may expect that they share information with each other to support vehicle purchases, service, warranty, recall, rebate, financing, marketing, service communications, discounts, and other operations. However, such sharing may, in certain circumstances, be considered a sale under the CCPA.²⁶ For example, dealers may be contractually required to share vehicle repair information with automakers for warranty purposes. Such sharing generally involves the disclosure of vehicle-specific information. Although automakers and their authorized dealers share common branding, they generally are not affiliated entities. So, the sharing could be viewed as a sale of personal information under the CCPA. Consumers who request that dealers or automakers not sell their personal information may not recognize that their request will disrupt the sharing of information between their automakers and their trusted dealers.

Similarly, automakers may have agreements with suppliers to share information about the failures of specific parts or systems to enable the suppliers to assess and potentially improve design or production processes. That information may be tied to the vehicles in which the parts or systems were installed so that the analysis is supported by a fuller understanding of the circumstances of deployment. While consumers may wish to opt out of traditional sales of

²⁶ "Sale" is defined as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration" with certain enumerated exceptions. *Id.* at § 1798.140(t).

personal information, where identifying information is shared with unaffiliated third parties for marketing purposes, they may not wish to disrupt the sharing of vehicle data with suppliers for purposes of improving parts and systems for the automotive industry at large.

The Attorney General is authorized to issue rules and procedures for compliance with a consumer's opt-out request.²⁷ The Alliance requests that the Attorney General issue rules and procedures permitting businesses to continue exchanging information with business partners of the types described above for reasonably expected purposes even after receiving an opt-out request. If the Attorney General is not willing to grant that request, the Alliance requests that businesses be permitted, but not required, to: (1) provide consumers with granular choices regarding their opt-out requests (i.e., permitting some sales while opting out of others); and (2) provide consumers with accurate disclosures regarding the potential impact of complying with a comprehensive opt-out request before implementing the opt-out.

(8) Permit businesses to use reasonable summaries or aggregate reports in response to access requests where disclosing specific pieces of personal information would compromise trade secrets or intellectual property rights, would likely be unintelligible to consumers, or would be unduly burdensome

Automakers have invested substantial resources into developing connected and highly automated vehicle technologies. The specific information that vehicles collect and transmit, as well as the timing of collection and transmission, may, in many instances, reveal trade secrets or other proprietary information regarding vehicle design and configuration or service offerings. For example, highly automated technologies rely on the collection of technical vehicle and environmental information that automakers use to further develop and improve the technologies. There is often a need to tie the information to specific vehicles to assess performance over time and across various environments. Much of this data may be maintained in a manner that would be a trade secret in that it could, for example, reveal the specific types or combinations of information that automakers are processing to develop highly automated systems.

The sophisticated, technical nature of certain data may also complicate compliance with access requests. Vehicle data may be restricted due to U.S. Export Control regulations, and require a specific license from the U.S. Department of State or U.S. Department of Commerce prior to release to non-U.S. persons. The information may be maintained in highly technical formats that would be unintelligible to all or most consumers. And there may be types of

²⁷ *Id.* at § 1798.185(a)(4)(B).

data that would be unduly burdensome to provide due to the nature of the data collection and storage. For example, businesses may monitor certain areas (e.g., vehicle showrooms) through closed-circuit television. Such data may be continuously collected and deleted at regular intervals, and not maintained in a manner facilitating the isolation of a particular consumer's information. To provide an individual a complete record of his/her own information, businesses may be required to analyze recordings in order to identify when the individual appears within frame, isolate the relevant video segments, and manually blur the images of other individuals in the recording to protect others' privacy.

The CCPA authorizes the Attorney General to establish exceptions to CCPA obligations as necessary in relation to "trade secrets and intellectual property rights"²⁸ and as necessary to further the purposes of the CCPA.²⁹ The Alliance asks the Attorney General to issue regulations clarifying that automakers and other businesses are not required to provide specific pieces of personal information in response to an access request where doing so would compromise trade secret or other intellectual property protections, where the information might be virtually meaningless to consumers, or where disclosure would be unduly burdensome. The Attorney General could clarify that automakers and other businesses may comply with access requests by providing consumers with reasonable summaries or aggregate compilations of the information collected in such circumstances.

(9) Clarify that businesses may enforce reasonable terms of financial incentive programs following a consumer's opt out of the program

Automakers are innovating new business models to address the increased interest in highly automated vehicles, car sharing, ride sharing, and other mobility offerings. Some of these business models may involve financial incentive programs, such as offering consumers discounts on vehicles or mobility services in exchange for consumers agreeing to the collection, use, and sharing of certain vehicle data. Such arrangements can help defray what would otherwise be higher-cost services to consumers. If a consumer opts-out of a sale or collection of information that is fundamental to an incentive program, businesses should be permitted to enforce reasonable terms of the program.

²⁸ *Id.* at § 1798.185(a)(3).

²⁹ *Id.* at § 1798.185(b).

The CCPA permits the use of such incentive programs as long as consumers provide opt-in consent after receiving the material terms of the financial incentive program.³⁰ And consumers have the right to revoke their consent to financial incentive programs at any time.³¹

Where consumers affirmatively agree to and are presented with clear terms and conditions for financial incentive programs, the intuitive and reasonable consequence for revoking consent to the programs is that businesses may exercise and enforce reasonable terms of the agreement. For example, if an automaker sold a vehicle to a consumer at a discount based on the consumer's agreement to share personal information with certain third parties, it would be reasonable for the automaker to require that the consumer refund the discount, or a pro-rated portion thereof, to the automaker if the consumer subsequently opts out of the financial incentive agreement. This is a reasonable and intuitive consequence where consumers affirmatively accept reasonable terms and conditions for a service.

When a consumer opts out of a financial incentive program, however, the consumer is exercising a right under the CCPA.³² If a business enforces reasonable, material terms associated with the opt-out, that could result in charging the consumer a different price or providing a different level or quality of goods or services to the consumer as a result of the opt out. As a consequence, enforcing the terms of the agreement could be viewed as a form of discrimination under the CCPA.³³ The Alliance therefore requests that the Attorney General, pursuant to its authority to establish rules and guidelines regarding financial incentive offerings,³⁴ establish rules and procedures clarifying that businesses may lawfully exercise and enforce reasonable, just, and nonusurious terms and conditions of financial incentive programs when consumers opt out of such programs. Absent such rules and procedures, automakers and other businesses may refrain from offering financial incentive programs, which likely would result in consumers paying higher costs for goods and services than they would pay under reasonable financial incentive programs.

³⁰ *Id.* at § 1798.125(b)(3).

³¹ *Id.*

³² *Id.*

³³ *Id.* at § 1798.125(a).

³⁴ *Id.* at § 1798.185(a)(6).

(10) Clarify that a business does not collect personal information merely by manufacturing for consumer use devices that store personal information on the devices where such information is not transmitted to the business

The CCPA establishes requirements for businesses that collect personal information. "Collect" is defined as "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means."³⁵

In the automotive context, much of the data that vehicles collect and store remains on vehicle systems. For example, data regarding vehicle systems status and data collected to support the operation of adaptive cruise control, lane assist, and other automated systems may reside only on the vehicle until actively retrieved by authorized dealers or other entities for repair or other services. Although it may be possible, in certain circumstances, for automakers to retrieve the data, in many circumstances they do not.

The Alliance therefore requests that the Attorney General, pursuant to its authorization to issue regulations as necessary to further the purposes of the CCPA,³⁶ clarify that personal information that is stored on devices owned by consumers, including vehicles, does not constitute personal information that a business has collected unless the business actually retrieves the information from the device. The mere potential to remotely retrieve personal information from a device should not be considered collection.

(11) Permit businesses to deidentify personal information in response to deletion requests

The CCPA requires businesses to comply with deletion requests by deleting personal information from the records they hold and by directing service providers to delete consumer's personal information, unless specific exceptions apply.³⁷ The CCPA does not apply to deidentified data.³⁸

The Alliance requests that the Attorney General, pursuant to its authority to adopt regulations as necessary to further the purposes of the CCPA,³⁹ clarify that

³⁵ *Id.* at § 1798.140(e).

³⁶ *Id.* at § 1798.185(b).

³⁷ *Id.* at § 1798.105.

³⁸ See *id.* at § 1798.145(a) ("The obligations imposed on businesses by [the CCPA] shall not restrict a business's ability to . . . [c]ollect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.").

³⁹ *Id.* at § 1798.185(b).

deidentification constitutes a form of deletion. When businesses deidentify personal information, they are no longer processing personal information. As discussed further in Section (6) above, deidentification allows businesses to engage in valuable processing activities while protecting consumer privacy. The CCPA recognizes that deidentified information should not be subject to the statute's deletion rights.⁴⁰ To further the purposes of the CCPA, the Attorney General should clarify that deidentifying personal information is a form of deletion in that it removes personal information from a business's systems.

(12) Clarify that personal information under the CCPA does not extend to employee information

As others have noted,⁴¹ the CCPA's definition of "personal information" potentially applies to employees and contractors, as some employees and contractors are California residents.⁴² However, many provisions of the CCPA are ill-suited for the employment context. For example, the CCPA requires publishing privacy notices on public-facing websites. The public distribution of employee privacy notices risks exposing confidential information, and providing an employee privacy notice on a business's public-facing website differs from the standard practice of providing such disclosures in employee handbooks or via intranet resources.

Although employment-related information is expressly mentioned as an example of personal information, neither the statutory language nor the legislative findings use the terms "employer" or "employee." And the anti-discrimination provision of the CCPA describes only consumer-related actions, not termination of employment or other labor-related issues. As a result of the CCPA's apparent legislative intent to focus on consumer privacy issues and the counterintuitive results of treating employees or contractors as consumers, the Alliance requests that the Attorney General, pursuant to its CCPA authority to issue regulations as necessary to further the purposes of the CCPA,⁴³ adopt regulations clarifying that the CCPA does not apply to information collected and processed in the context of employment relationships.

⁴⁰ *Id.* at § 1798.145(a).

⁴¹ See, for example, the testimony of Tanya Forsheit before the California state legislature. Audio and video of the hearing is available at <https://www.assembly.ca.gov/media/assembly-committee-privacy-consumer-protection-20190220/video>, and a third party's written summary of the testimony is available at <https://blog.ericgoldman.org/archives/2019/02/recap-of-the-california-assembly-hearing-on-the-california-consumer-privacy-act.htm>.

⁴² The CCPA defines "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," where "consumer" is further defined as "a natural person who is a California resident, as defined in [the tax code] however identified, including by any unique identifier." Cal. Civ. Code § 1798.140.

⁴³ *Id.* at § 1798.185(b).

Conclusion

Innovative vehicle technologies hold great promise to deliver substantial environmental, safety, consumer, and societal benefits. As illustrated by its voluntary adoption of the Principles, the Alliance and its members recognize the importance of implementing reasonable privacy protections to foster consumer trust and engagement.

The Alliance appreciates the Attorney General's consideration of these comments. Please feel free to contact us if you have any questions about the Alliance's position or would like to discuss any aspect of these comments.

A handwritten signature in black ink, reading "Jessica L. Simmons", is displayed on a light blue rectangular background.

Jessica L. Simmons
Assistant General Counsel



Message

From: McArthur, Webb [REDACTED]
Sent: 3/8/2019 3:26:08 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Eric Ellman [REDACTED]
Subject: Comments on CCPA
Attachments: CDIA CCPA Rulemaking Comment Letter.pdf

Privacy Regulations Coordinator:

On behalf of the Consumer Data Industry Association (CDIA), I submit the attached comment letter regarding the Department of Justice's anticipated rulemaking on the California Consumer Privacy Act.

Webb McArthur

Associate | Admitted in the District of Columbia, Maryland, and Virginia

Hudson Cook, LLP

[REDACTED] | [REDACTED]

1909 K St., NW | 4th Floor | Washington, DC 20006

**HUDSON
COOK**

The information contained in this transmission may be privileged and may constitute attorney work product. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact Webb McArthur at [REDACTED] or [REDACTED] and destroy all copies of the original message and any attachments.

* * * *



Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

CDIAONLINE.ORG

March 8, 2019

Via Electronic Delivery to privacyregulations@doj.ca.gov

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

RE: California Consumer Protection Act Rulemaking

The Consumer Data Industry Association submits this comment in response to the California Department of Justice's anticipated rulemaking for the California Consumer Privacy Act ("CCPA").

The Consumer Data Industry Association (CDIA) is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk.

Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers' access to financial and other products suited to their unique needs. They help people meet their credit needs. They ease the mortgage and employment processes; they help prevent fraud; they get people into homes, jobs, and cars with quiet efficiency. CDIA members locate crime victims and fugitives; they reunite consumers with lost financial assets; they keep workplaces and apartment buildings safe. CDIA member products are used in more than nine billion transactions each year.

CDIA members have been complying with laws and regulations governing the consumer reporting industry for decades. Members have complied with the Fair Credit Reporting Act ("FCRA"), which has been called the original federal consumer privacy law. The FCRA governs the collection, assembly, and use of consumer report information and provides the framework for the U.S. credit reporting system. In particular, the FCRA outlines many consumer rights with respect to the use and accuracy of the information contained in consumer reports. Under the FCRA, consumer reports may be accessed only for permissible purposes, and a consumer has the right to dispute the accuracy of any information included in his or her consumer report with a consumer reporting agency ("CRA"). Accordingly, CDIA members have been at the forefront of consumer privacy protection. Fair, accurate, and permissioned use of consumer information is necessary for any CDIA member client to do business effectively.

CDIA members have also complied with an array of state laws for decades, including the California Consumer Credit Reporting Agencies Act (“CCRAA”), the California Investigative Consumer Reporting Agencies Act (“ICRAA”), and the California Commercial Credit Reporting Act.

CDIA appreciates the California State Assembly and the Department of Justice, through the Office of the Attorney General (“AG”), for their work on the cutting edge of consumer privacy issues in the CCPA. It is in this spirit that CDIA offers the following comments to improve the clarity and effectiveness of the CCPA for its intended purposes.

To assist your office in crafting a rule that meets consumer expectations and allows businesses to best support customers and consumers, we offer this comment on a number of AG rulemaking directives. This comment addresses the following issues:

- I. Rulemaking Directive: Update Categories of Personal Information (§ 1798.185(a)(1))
Household information – Clarification that it does not include information that is only linked to an address.
- II. Rulemaking Directive: Furthering the Purposes of Sections 1798.110 and 1798.115 (§ 1798.185(a)(7))
Third party notice requirement – Clarification that a third party can rely on notice provided by the business with the relationship with the consumer.
- III. Rulemaking Directive: Adopt Additional Regulations as Necessary to Further the Purposes of the CCPA (§ 1798.185(b))
Fraud Prevention Services – Clarification that information maintained for fraud prevention purposes is exempt from the law.
Deidentified information – Clarification that even if a company possesses information that could be used to reidentify, information is still considered “deidentified” so long as the company employs proper safeguards against reidentification.
Service Provider Exception – Clarification that “necessary to perform a business purpose” includes outsourcing those tasks that are more efficient or less expensive for a service provider to perform.
Definition of “Consumer” – Clarification that the term “consumer” does not include individuals who have an employment or business relationship with the business.
FCRA Exemption – Clarification that the FCRA exemption covers information transferred without valuable consideration or never included in a consumer report.
Commercial Credit Reporting – Clarification that commercial credit reporting agencies are not subject to the CCPA.

- I. Rulemaking Directive: Update Categories of Personal Information (§ 1798.185(a)(1))

ISSUE: Household information – Clarification that it does not include information that is only linked to an address.

The term “personal information” includes information that is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular household. Cal. Civ. Code § 1798.140(o)(1). The term “household” is not defined.

CRA and data analytics providers may collect data that is specific to an address without being specific to one consumer. Nevertheless, such information may be “capable of” being associated with a consumer, and may therefore be “personal information” under the CCPA, as the business may possess other information that a consumer has lived at the address at issue or a consumer, when submitting a verifiable consumer request, may provide the address. The CCPA, at sections 1798.110 and 1798.115, requires a business to disclose personal information “about the consumer.” Because personal information may be linkable not only to a particular consumer but also to a household, the CCPA arguably may require CRAs to disclose all information associated with an address with which a consumer has been associated (or with which the consumer associates himself or herself).

The CCPA does not require a business to reidentify or otherwise link any data that is not maintained in a manner that would be considered personal information. Cal. Civ. Code § 1798.145(i); *see also* Cal. Civ. Code § 1798.110(d)(2). However, because data linked to an address but not to a particular individual may be considered “personal information,” this exception would not protect businesses from being required to disclose address-specific information to any consumer who has ever been associated with that address.

Requiring businesses to disclose personal information to any consumer who shares or has shared the same address undermines the privacy rights set out in the CCPA and may increase the incidence of identity theft. An increase in the incidence of identity theft may increase the risk of data breaches or other security incidents, as the availability of sensitive information in the public domain would permit criminals to buy and sell such information for nefarious purposes.

PROPOSED SOLUTION: The AG is authorized to update additional categories of personal information by section 1798.185(a)(1). Accordingly, the AG should clarify that information that is linked only to an address—but not linked to a specific consumer—is not linked to a “household” and is therefore not “personal information” under the CCPA. Additionally, the AG should use its section 1798.185(b) authority to address the risk of disclosure to individuals other than the consumer directly. The AG should state that a business is not required to disclose to a consumer personal information that is linked to the consumer’s address but is not otherwise linked to the consumer. The AG should also state that a business is not required to disclose to a consumer personal information that is linked to an individual other than the requesting consumer, even one that may share the same address. Section 1798.185(b) is an appropriate avenue for this clarification, as without clarification on this issue, the CCPA may require businesses to disclose sensitive personal information to individuals who are not the requesting consumer and thereby undermine the privacy rights conferred by the CCPA.

II. Rulemaking Directive: Furthering the Purposes of Sections 1798.110 and 1798.115
(§ 1798.185(a)(7))

ISSUE: Third party notice requirement – Clarification that a third party can rely on notice provided by the business with the relationship with the consumer.

Section 1798.115(d) prohibits a third party from selling personal information that has been sold to the third party by a business unless the consumer to whom the information relates has received “explicit notice” and is provided an opportunity to exercise her or his right to opt out.

Third parties may not have a relationship with the consumer in order to provide these notice and opt-out rights. Specifically, CRAs and other data analytics providers seldom have direct relationships with consumers to ensure that these requirements have been complied with before selling information. If CRAs or data analytics providers were required to provide these notice and opt-out rights, the CRAs or data analytics providers would have to obtain up-to-date contact information for the consumer from the business from which it obtained the information and initiate a relationship in order to provide them these rights. Such a process would not only be extremely burdensome, but the legally-required dissemination of contact information might compromise consumer privacy.

This provision also presents two other issues. First, it is also not clear what the law means by “explicit notice,” as the CCPA only requires notice on a business’ website and privacy policies. See Cal. Civ. Code § 1798.135(a). Second, by applying directly to any “third party,” this provision expands the scope of the CCPA from California businesses as defined by the law effectively to any entity anywhere.

PROPOSED SOLUTION: Under its section 1798.185(a)(7) authority, the AG should permit a third party to rely on the business from which it obtained the personal information to provide these notice and opt-out rights. To do so, the AG should provide a safe harbor or a limitation of liability for third parties when relying on a transferring business’ online privacy policies or specified attestations made by the business in connection with the transfer of personal information.

III. Rulemaking Directive: Adopt Additional Regulations as Necessary to Further the Purposes of the CCPA (§ 1798.185(b))

ISSUE: Fraud Prevention Services – Clarification that information maintained for fraud prevention purposes is exempt from the law.

Section 1798.105(a) permits consumers to request the deletion of any personal information about the consumer which the business has collected from the consumer. However, the law provides an exception for businesses or service providers where it is “necessary” for businesses or service providers to maintain the personal information to “[d]etect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity.” Cal. Civ. Code § 1798.105(d)(2).

Thus, the fraud exception to the deletion obligation applies only where it is necessary for a business to keep the personal information to detect fraud. It is unclear under what circumstances it would be necessary for a business to retain personal information to detect fraud. This is of concern to CRAs and other data analytics providers that provide fraud detection and prevention services which leverage personal information to protect consumers and businesses. CDIA members provide these services by comparing information submitted on an individual against other information held by the fraud prevention services provider to detect inconsistencies and other red flags.

Furthermore, this exception only contemplates that a business may retain information to prevent fraud on itself. It does not contemplate one business using personal information in order to detect and prevent fraud on another business. CDIA members are in a position to provide, and do provide, fraud detection services to customer businesses because they have access to a larger universe of information than one merchant or creditor.

Finally, fraud detection is only an exception to the CCPA's deletion obligation and not the other obligations, like the opt-out requirement. The lack of an exception for the detection of fraud or other illegal activity to other business obligations means that fraud detection products may be less effective. For example, an opt-out right might mean that less information will be available for fraud detection. This would affect not only the consumer who requested opt-out, but all consumers, as effective fraud detection requires a large volume of data. For example, a consumer's removal of her phone number from this information stream might not only affect a criminal attempting to open a credit account in *her* name in the future, but also another consumer where a fraudster provides that phone number when applying for credit.

The CCPA's goal of protecting consumer privacy underlines the importance—and the *growing* importance—of fraud detection products. Fraud detection products protect not only businesses against fraud by criminals, but they also protect consumers from identity fraud. These products work by utilizing a large volume of data, and removing one consumer's data from the universe of available data would affect not only that consumer, but all consumers.

PROPOSED SOLUTION: Section 1798.185(b) authorizes the AG to adopt additional regulations as necessary to further the purposes of the CCPA. The CCPA is intended to protect consumer privacy, and the OAG should clarify that the CCPA does not impede a business' ability to detect and prevent fraud or other illegal activity. Issuing such a rule would further consumer privacy and promote the purposes of the CCPA. Therefore, CDIA strongly urges the AG to clarify that the fraud detection exception to the right of deletion covers the processing of personal information for a third party's fraud prevention purposes, as well as a business' own purposes. Additionally, CDIA strongly urges the AG to adopt a regulation that provides that businesses are not subject to the CCPA's opt-out and other disclosure obligations with regard to personal information collected, retained, or disclosed for fraud detection and prevention purposes.

ISSUE: Deidentified information – Clarification that even if a company possesses information that could be used to reidentify, information is still considered “deidentified” so long as the company employs proper safeguards against reidentification.

The CCPA clarifies that the obligations imposed on businesses do not restrict a business' ability to collect, use, retain, sell, or disclose consumer information that is deidentified or aggregated. Cal. Civ. Code § 1798.145(a)(5). “Deidentified” means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information implements certain specified safeguards. Cal. Civ. Code § 1798.140(h) (emphasis added). The CCPA does not define what it means to be “capable of being associated with” or “could reasonably be linked.”

It is not clear, based on the structure of the definition of “deidentified,” whether information for which a business has implemented the safeguards specified by section 1798.140(h) is necessarily considered deidentified, or if the law separately requires that the personal information be, in fact, not reasonably capable of being associated with or linked to, directly or indirectly, a particular individual. This problem arises from the fact that the definition includes the words “provided that,” which may imply that the safeguards are not enough to make information deidentified. The definition of

“deidentified” therefore may be ineffectual except to impute a reasonableness requirement to the definition of “personal information.”

CRA and other data analytics providers work with deidentified data regularly, including for data analytics research purposes, development of new scores, etc. When working with deidentified data, these companies implement appropriate safeguards to prevent the identification of the data. However, it is not clear whether such data would be considered “deidentified” under the CCPA, as CRAs or other data analytics providers may have identified data sets which, if combined with a non-identified set, might permit the re-identification of the non-identified data set. Although these businesses may implement the safeguards described in the definition of “deidentified,” it is not clear that the implementation of these safeguards necessarily means that the data is “deidentified” for the reasons described above.

This issue is particularly problematic for CRAs and other data analytics providers with regard to personal information inferences. “Personal information” includes, when capable of being associated with, or could be reasonably linked, directly or indirectly, inferences drawn from any personal information to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. Cal. Civ. Code § 1798.140(o)(1)(K). A company may create data sets by inferring characteristics about a consumer from other data sets. Because of the lack of clarity in the definition of “deidentified,” it is not clear whether inferences drawn from deidentified information are “personal information” under the CCPA. Data analytics research may be undertaken to improve the delivery of business services, including a CRA’s delivery of fraud prevention services, which furthers consumer privacy rights.

PROPOSED SOLUTION: The AG should clarify that data sets for which a business has implemented the section 1798.140(h) safeguards are necessarily “deidentified.” The AG should also clarify that any inferences drawn from information deidentified by way of implementing the section 1798.140(h) safeguards are also “deidentified.”

ISSUE: Service Provider Exception – Clarification that “necessary to perform a business purpose” includes outsourcing those tasks that are more efficient or less expensive for a service provider to perform.

The term “sale” does not include a business’ use or sharing of personal information with a service provider “that is necessary to perform a business purpose” if certain conditions are met. Cal. Civ. Code § 1798.140(t)(2)(C). The law does not clarify what it means by “necessary to perform a business purpose.”

CRAs and other data analytics providers may regularly engage service providers for business purposes to gain those service providers’ efficiencies or expertise. Service providers may collect data or process data for businesses when offering non-FCRA products like fraud prevention tools. However, engaging a service provider should be considered necessary to perform a business purpose when a business gains efficiencies or expertise through the arrangement even if it is possible for the business to undertake those tasks individually.

PROPOSED SOLUTION: The AG should clarify by rule that sharing data with an engaged service provider is not a “sale” of personal information where the conditions under section 1798.140(t)(2)(C) are met.

ISSUE: Definition of “Consumer” – Clarification that the term “consumer” does not include individuals who have an employment or business relationship with the business.

The term “consumer” means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier. Cal. Civ. Code § 1798.140(g). Because of the breadth of this definition, it arguably includes all California residents, even when they are employees of the business or have only a business (and not a consumer) relationship with the business. As a result, the CCPA regulates as “personal information” information relating to an individual with an employment or business relationship with the business, extending to such individuals rights including those related to disclosure and deletion.

Nevertheless, the CCPA’s anti-discrimination provisions make it clear that the law is meant to protect individuals who have a consumer relationship with a business, not individuals who have an employment relationship or a business relationship (e.g., a sole proprietor or business owner) with a business, as these provisions protect consumers against being denied goods or services, being charged different rates for goods or services, or being given different quality goods or services. *See* Cal. Civ. Code § 1798.125.

Extending the CCPA to individuals with employment or business relationships with a business may cause conflict with existing California law. For example, the California Labor Code already regulates employee rights to disclosure of personal records. *See* Cal. Lab. Code § 1198.5.

Additionally, extending the CCPA to individuals with employment or business relationships with the business may put consumer privacy rights in jeopardy. For example, without correction, the CCPA might allow an employee to request deletion of records of allegations of harassing conduct in the workplace. Although the CCPA permits a business to decline to delete information necessary to comply with a legal obligation, businesses regularly retain personnel records to protect the business and other employees and not to comply with specific legal document retention requirements.

Finally, extending the CCPA to individuals with business relationships may complicate, if not make impossible, compliance with due diligence requirements under know-your-customer, anti-corruption, or anti-money laundering laws, as the CCPA may permit individuals related to businesses to request deletion of information about them. Lack of compliance with these requirements would likely also compromise consumer privacy.

PROPOSED SOLUTION: Because extending the CCPA to individuals that have employment or business relationships with a business may jeopardize consumer privacy rights, the AG would be authorized to provide clarification under its section 1798.185(b) authority. Therefore, the AG should adopt a rule clarifying that the term “consumer” does not include individuals with an employment or business relationship with a business.

ISSUE: FCRA Exemption – Clarification that the FCRA exemption covers information transferred without valuable consideration or never included in a consumer report.

The CCPA does not apply to “the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined by subdivision (d) of Section 1681a of Title 15 of the United States Code, and use of that information is limited by the federal Fair Credit Reporting Act.” Cal. Civ. Code § 1798.145(d).

However, as currently written, this exemption does not cover all information regulated by the FCRA and may pose new consumer risks to consumers, government agencies, law enforcement, volunteer organizations, and businesses.

First, the current FCRA exemption extends only to the “sale” of personal information, to the extent that its use is limited by the FCRA. The term “sale” under the law requires “monetary or other valuable consideration.” Cal. Civ. Code § 1798.140(t)(1). Because “other valuable consideration” is not defined in the CCPA, there is some risk that the FCRA exemption may not cover transfers of personal information that are critical to the provision of consumer reports, including the transfer of data from furnishers, which provide information to CRAs for free. If the FCRA exception was interpreted as not applying to such data, the requirements of the CCPA would threaten the accuracy and completeness of consumer reports and the overall integrity, reliability, and predictability of the credit reporting system.

Second, the current FCRA exemption extends only to information that “is to be reported in, or used to generate, a consumer report.” However, CRAs often maintain information that may never be reported in, or used to generate, a consumer report. Such information may be information furnished by a creditor on a consumer on whom a consumer report may never be ordered, information the CRA obtains but about which it has accuracy concerns, or information that is not reportable under the law or otherwise (because it is obsolete or on a deceased consumer). Nevertheless, CRAs may retain such information to verify that a consumer is who they say they are and for other research purposes to improve the CRAs’ accuracy. Allowing CRAs to improve their matching techniques and to ensure that data they provides on consumers is accurate benefits consumers and furthers the purposes of the CCPA, not only because it allows consumers to obtain products and services more easily and at lower costs, but because it protects against the release of sensitive personal information to individuals who are not the consumer in question.

PROPOSED SOLUTION: The AG is authorized to provide clarification under its section 1798.185(b) authority because it would further consumer privacy to allow CRAs to provide complete and accurate information on consumers in compliance with the FCRA. Accordingly, the AG should provide clarification on the “sale of” language in the current FCRA exemption, stating that the exemption extends to transfers of information that are not made for monetary consideration but are made as part of the U.S. consumer reporting system. Additionally, the AG should provide clarification that the exemption covers information that may be used to generate a consumer report, even if such information is never actually included in such a report.

ISSUE: Commercial Credit Reporting – Clarification that commercial credit reporting agencies are not subject to the CCPA.

California law regulates a category of entities that are not regulated by the federal FCRA or the California CCRAA or ICRAA, namely "commercial credit reporting agencies." Commercial credit reporting agencies provide reports "relating to the financial status or payment habits of a commercial enterprise." See Cal. Civ. Code §§ 1785.41 *et seq.* A "commercial enterprise" may include a sole proprietor, necessarily involves owners, principals, etc., and as a result, a "commercial credit report" may include information that is "personal information" as defined and regulated by the CCPA.

Additionally, because of the broad sweep of the definition of "personal information," commercial credit reports may include information on business employees, as a commercial credit report may contain information on the financial status or payment habits of a commercial enterprise that are able to be linked to an individual. If such information is linked to a particular individual, that individual would have the right under the CCPA to obtain sensitive business information to which it does not otherwise have access, and that individual may also have such information deleted. These rights would exist even though such information would bear no cognizable privacy risk to these individuals. Additionally, because it would be difficult to determine the individual to whom the information relates, requiring the disclosure of this information may increase the risk of identity theft. Finally, deletion rights would impede the availability, accuracy, and usefulness of commercial credit reports made available under California law.

PROPOSED SOLUTION: Because the disclosure of information may impose risks to consumer privacy without furthering the privacy of other consumers, the AG is authorized to provide clarification on this issue under section 1798.185(b). Therefore, the AG should adopt an exemption for "commercial credit reporting agencies" as defined by California law.

CDIA thanks the California Department of Justice for the opportunity to share its views on the CCPA rulemaking process. Please contact us if you have any questions concerning the above comments or need additional information.

Sincerely,

A handwritten signature in blue ink, appearing to read 'E. Ellman', with a long horizontal flourish extending to the right.

Eric J. Ellman
Senior Vice President, Public Policy & Legal Affairs

Message

From: Debbie Schwarzer [REDACTED]
Sent: 1/15/2019 4:53:59 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA - Aeris Communications

Greetings.

Aeris Communications, Inc. is a company headquartered in San Jose, CA with global operations. Like a huge number of companies doing business in this state, we sell services solely to other businesses (meaning we are a “B2B”, or business-to-business, company). Our services include cellular connectivity to allow customer devices to send data to a customer endpoint (imagine a solar panel that sends data about usage and performance to a company server over cellular, or a medical device that connects to the cellular network each morning to upload patient data) or to allow the business customer to manage the devices (e.g., sending a firmware update to the device). We also sell device and data management services to businesses, including usage-based insurance companies, fleet managers and automotive OEMs. The vast majority of this data is spectacularly boring and is in no way “personal”, or is not transmitted in a way that would allow a hacker to associate the data with a living natural person.

In each of these situations, Aeris has no relationship with a consumer. In many cases, we do not know who the consumer is (whose house the solar panel is attached to, who is using the medical device, etc.). If we do know, such as for “connected vehicle” services that automotive OEMs provide to their vehicle owners (think of a mobile app that allows you to unlock your car from your phone, or set a speed alert, etc.), we are prohibited by contract from interacting with vehicle owners, and we take pains to store data in ways that minimize the association with named persons (we use non-public device identifiers, for example). Is Aeris subject to CCPA? Do we “collect” the data? We technically enable collection, but we are not the company that decides what data to collect or what to do with it, or enters into a contract with the consumer. We sometimes hold it in our production or archival database in accordance with contractual commitments, but we have no consumer-facing websites where an individual could request actions with respect to their data.

In GDPR language, we are a data processor, not a data controller. It is an enormously helpful distinction, and it is missing completely from the CCPA.

California businesses that do business with consumers in Europe, or that do business with companies that do business with consumers in Europe, just went through a massive two year exercise to understand what GDPR requires and to revise business and IT processes. It would be exceptionally helpful if the CCPA could be amended to adopt some of the core concepts that were introduced through GDPR and that have become de facto global standards in other countries adopting privacy regulations (e.g., India). I would include in this group the following:

- The distinction between data controllers and data processors in terms of obligations
- The concept of informed consent, and the purposes for which data collection and processing are permitted
- The concept of “organizational and technical measures” that can be adopted by a business using risk-based analysis to protect data (as distinct from specifying specific standards, such as ISO 27001)
- The idea of “privacy by design” as a guiding principle for designing applications that collect data
- Procedures for regulating the use of data processors, including transfer of personal data to new processors

I don't think a single one of these reduces protections for consumers. What they do is clarify for businesses what their obligations are, and as the lead attorney for a California business, that is of utmost importance to me. I would be happy to assist with an effort to incorporate these ideas into CCPA and am certain that our CEO would support me in using my time in that way.

Please let me know if you have any questions or if you would like to discuss my proposals.

Best,

Debbie Schwarzer

[Deborah R. Schwarzer](#) | General Counsel

[Aeris Communications, Inc.](#)

[REDACTED]

[REDACTED] | [REDACTED]

The information in this message may be confidential and legally privileged. If you are not the intended recipient of this message, please inform the sender of the error immediately. The review, use, distribution or copying of any message not intended for you is prohibited, and we ask that you permanently delete the message along with any copies and attachments.

Message

From: [REDACTED]
Sent: 2/24/2019 12:03:58 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA - Submitting and Complying with Requests - Agent requirement
Flag: Follow up

The law needs to allow agents to be able to submit requests on behalf of consumers.

I haven't heard this discussed much, but it is CRITICALLY important!

Since there are hundreds of companies that have consumer's data, an agent must be allowed to submit these requests on a consumers behalf. Otherwise the individual consumer would have to go to each company's website to submit a request and there would be hundreds of companies the typical consumer would never know exist to submit their request.

So the language needs to look something akin to: "Companies must respond to requests submitted by consumers, or their authorized agent(s)."

Thanks!

Jonathan Broder

Message

From: [REDACTED]
Sent: 3/11/2019 8:44:31 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA

I was the named plaintiff in a major class action lawsuit against TD Ameritrade, as documented in the national press ([links, etc. here](#) on my Caring About Security site)

You ask,

Number seven: How can consumer or their agents submit a request for information to a business and how should a business reasonably verify these requests?

Please do NOT allow a business to do this:

- 1)When a consumer sends an email requesting information, reply only via US mail. Instead, require the company reply substantively, by email, to the email, and in addition reply in other appropriate ways.
- 2)When a consumer sends an email requesting information, reply only with just a request for additional information or documentation not asked for initially. Instead, if the business is allowed to require such (e.g. a notarized request, require that the business document all requirements at the outset, wherever it notifies the consumer of their right to request information.

Make sure you understand what deanonymization is.

-Matthew

SF, CA 94102

Message

From: Anne Kimbol [REDACTED]
Sent: 3/8/2019 10:55:22 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Carl Anderson [REDACTED]
Subject: Comments on CCPA rulemaking
Attachments: HITRUST Comments on California privacy law.pdf

Attached please find comments from HITRUST's Senior Vice President of Governmental Affairs on the CCPA rulemaking. We appreciate the opportunity to provide these comments. Thank you, Anne Kimbol



Anne Kimbol
Asst. General Counsel and Chief Privacy Officer
[REDACTED]

CONFIDENTIALITY NOTICE: The contents of this email message and any attachments may contain confidential, proprietary or legally privileged information and/or may be subject to copyright or other intellectual property protection and be legally protected from disclosure. This information is intended only for use of the addressee or addressees named above for its intended purpose. If you are not the intended recipient of this message or their agent, or if this message has been addressed to you in error, please immediately alert the sender by reply email and then delete this message and any attachments. If you are not the intended recipient, you are hereby notified that any use, dissemination, copying, or storage of this message or its attachments is strictly prohibited.

March 8, 2019

Xavier Becerra
California Department of Justice
Attn: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, California 90013

Sent via email: PrivacyRegulations@doj.ca.gov

Re: Comments on Assembly Bill 375, the California Consumer Privacy Act of 2018

Dear Mr. Becerra:

On behalf of HITRUST, I thank you for the opportunity to provide comment on the California Consumer Privacy Act of 2018 (CCPA) and feedback as part of the rulemaking process. HITRUST supports suggestions made at public meetings you have held on the CCPA in support of a safe harbor option for entities that complete recognized certification programs. Such a safe harbor is consistent with the CCPA's safe harbors for encrypted data and reasonable security safeguards, since such a program would review the entity for those exact measures. However, specific recognition by the Office of Attorney General of such actions would allow more certainty and comfort among entities when devoting sufficient resources to their programs and having them assessed.

HITRUST believes California should recognize the work of entities that have had a third party assessment based on certifiable privacy and security standards and should encourage more entities to take that step. Third party assessment and certification is the best way to ensure entities have good programs in place that are well implemented. The private sector has strong programs in this arena already, and it would empower the California government and entities seeking to test and improve their programs to take advantage of pre-existing systems.

Founded in 2007, HITRUST Alliance is a not-for-profit standards organization whose mission is to champion programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security and risk management leaders from both the public and private sectors, HITRUST develops, maintains and provides broad access to its widely adopted common risk and compliance management and de-identification frameworks; related assessment and assurance methodologies; and initiatives advancing cyber sharing, analysis, and resilience.

The foundation of all HITRUST® programs and services is the HITRUST CSF®, a certifiable framework that provides organizations with a comprehensive, flexible and efficient approach to regulatory compliance and risk management. Developed in collaboration with information

security professionals, the HITRUST CSF rationalizes relevant regulations and standards into a single overarching privacy and security framework.

The HITRUST CSF is a risk-based controls framework that incorporates the HIPAA Privacy and Security Rules and the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, or Cybersecurity Framework. The most recent edition of the CSF also includes privacy controls based on internationally recognized privacy frameworks, including the Fair Information Practice Principles (FIPPs), the Organization for Economic Cooperation and Development (OECD) Privacy Principles, and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.

The HITRUST CSF Assurance Program is just one of the methods entities can use to seek certification against strong privacy and security standards. As with the HITRUST CSF, many of these programs have aided entities in detecting and mitigating issues in their own practices as well as allowing them to mitigate third party risk by only contracting with service providers who have also been certified or accredited. By recognizing such programs, the CCPA would be encourage entities to ensure their programs are well developed and implemented while also acknowledging that the private sector has existing recognized programs that could assess an entity against national and international laws as norms as well as its compliance with the CCPA.

Additionally, such programs can be used to monitor business partners. As we have seen, auditing third party vendors and other data sharing partners for compliance with data protection requirements is essential to protect data and consumers. Entities generally do not have the resources in terms of time, personnel, and finances to perform such audits on a regular basis, particularly of each data sharing partner. Allowing entities to rely on certifications from recognized certification bodies would reduce the resources entities need to devote to auditing business partners, while also ensure that such partners have and are maintaining strong data protection programs.

For these reasons, HITRUST supports recommendations for a safe harbor for entities with data protection certifications. No system is breach-proof, and those who have developed, implemented, and maintained appropriate policies and procedures should receive recognition that they have done the right thing, even if a breach occurs. In addition, California should rely on existing frameworks and recognize that the private sector has responded to data protection concerns and offers appropriate methods of measuring the strength of data protection programs.

I thank you again for the opportunity to provide these comments.

Very truly yours,



Carl A. Anderson
Chief Legal Officer and Senior Vice President for Government Affairs

Message

From: Aleecia McDonald [REDACTED]
Sent: 3/8/2019 8:35:20 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA

With apologies I do plan to submit comments, but I will not have something worth reading tonight. I hope you will be able to accept late comments early next week.

Aleecia

Assistant Professor Aleecia M. McDonald // Carnegie Mellon' s Information Networking Institute //

[REDACTED]

Message

From: Johnny Ryan [REDACTED]
Sent: 3/8/2019 2:22:53 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on preliminary rulemaking for the California Consumer Privacy Act
Attachments: Brave letter to California Department of Justice regarding the CCPA, March 8 2019.pdf

Dear colleagues,

Please find attached a letter from Brave Software, regarding the CCPA.

Johnny Ryan

--

Dr Johnny Ryan FRHistS

Chief Policy & Industry Relations Officer
Brave Software

Twitter: https://urldefense.proofpoint.com/v2/url?u=http-3A__www.twitter.com_johnnyryan&d=DwIFaQ&c=uASjV29gZuJt5_5J5CPRuQ&r=kXcUIWCJFJC3Y7A6WP15oNx0wEUzL_7MxjOspe9bxxI&m=t0t-YBTzpSmNGE128nYxDq36_djSAZ-Ho8wnabShw8&s=VsB_6dsF1Taez8w_-souZkHdh1VLss6-q_3oR7dk5r0&e=

Praise for 'A History of the Internet and the Digital Future'

"Consider this book your road map" - Marc Benioff (CEO of Salesforce)

"An immensely important book" -Kevin O'Sullivan (Editor of The Irish Times)

"Engrossing" -Cory Doctorow (BoingBoing)

"Enormously useful" -Prof Tim Wu (Columbia Law School)



Privacy Regulations Coordinator
California Department of Justice
300 S. Spring Street
Los Angeles, CA 90013

8 March 2019

Comments on preliminary rulemaking for the California Consumer Privacy Act

Dear colleagues,

I represent Brave, a rapidly growing Internet browser based in San Francisco. Brave is at the cutting edge of the online media industry. Its CEO, Brendan Eich, is the inventor of JavaScript, and co-founded Mozilla/Firefox. Brave is headquartered in San Francisco and innovates in areas such as online advertising, machine learning, blockchain, and security.

We are heartened to see the potential increase in the level of privacy protection in the California Consumer Protection Act. We write to raise four matters, and suggest how to further protect individuals' privacy in a manner that is compatible with innovation and economic growth.

1. "Personal information"

First, we are concerned by the fact that the definition of "personal information" does not not include publicly available information. This is only partly remedied by the caveat that

"Information is not 'publicly available' if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained."

We suggest that it would be simpler and easier for business to understand, and for the Attorney General to enforce, a definition of personal information that includes all



personal information, irrespective of whether the information is public or not. From our perspective as a business that also operates in Europe under the GDPR, we have experienced no ill effect from the GDPR's definition of personal data, which include both public and non-public information. As a general principle, it is the information's relationship to a person that makes it "personal", and this applies whether or not that information happens to also be also public.

We commend the legislator for including "capable of being associated with" within the definition. This is of critical importance.

2. Deletion requests

There is a risk that the CCPA allows a business to deny a deletion request if the data concerned are - in it's own judgement - useful for "security", "debugging", or to provide a good or service "reasonably anticipated within the context of a business's ongoing business relationship with the consumer".

We suggest that this is too a wide spectrum of reasons to not comply with a person's request for deletion of information about themselves.

In particular, we are troubled by the exception concerning "a business's ongoing business relationship with the consumer". Why would a person request the deletion of data that would negatively affect the service they receive, unless they are aware of that fact? If, however, they are not aware of the consequences, then surely all that is necessary is to inform them, and ask if they wish to proceed. We believe that limiting a person's right to have data about them deleted in such a circumstance run counter to logic. We are deeply concerned that this may undermine intention of the Act.

3. "Business purposes" exception

We are troubled by the Act's exception for personal information to be used or shared when necessary to perform a "business purpose". A business purpose can include:

"...providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider."

We suggest that this requires more thought in the light of successive privacy scandals in advertising. Permitting personal information to be used for a business purpose that includes advertising may, we fear, open the door to widespread abuse by the



advertising technology industry. As participants in this industry, we urge you to engage in rulemaking that mitigates this grave threat.

4. "Sale"

We are concerned that the concept of the "sale" of personal information may be too permissive. One company can share personal information with one or more other companies and benefit from this sharing without there being a formally defined valuable consideration. This occurs, for example, in the "real-time bidding" online ad auction system, where personal information is shared among thousands of companies. We fear that this activity would not be captured by the concept of "selling". This is a grave concern, because real-time bidding currently broadcasts what every person in California reads, watches, and listens to online billions of times a day. Therefore, we urge a broadening of the definition of "sale" so that this activity, and similar activities, are captured.

We commend you for your work on this Act so far, and are ready to help you if we can.

Sincerely,

A handwritten signature in black ink, appearing to be "Dr. Johnny Ryan", with a long, sweeping horizontal line extending from the end of the signature.

Dr Johnny Ryan FRHistS
Chief Policy & Industry Relations Officer



Message

From: Scott Buchanan [REDACTED]
Sent: 3/8/2019 2:16:21 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on Rulemaking for the CCPA - Student Loan Servicing Alliance
Attachments: SLSA_CCPACommentLetter_3-8-19_SUBMITTED.pdf; SLSA_CCPACommentsAnalysis_3-8-19_SUBMITTED.pdf

Privacy Regulations Coordinator,

On behalf of the Student Loan Servicing Alliance I respectfully submit the following comments on rulemaking for the California Consumer Privacy Act of 2018, and request their consideration in the process. Please let me know if you have any questions, or if I and our membership can be helpful during this process.

Regards,

Scott

C. Tapscott Buchanan

Executive Director

Student Loan Servicing Alliance

1100 Connecticut Avenue, NW

Suite 1200

Washington, DC 20036

[REDACTED]

[REDACTED]



Student Loan Servicing Alliance
1100 Connecticut Avenue, NW
Suite 1200
Washington, DC 20036

March 8, 2019

VIA EMAIL: privacyregulations@doj.ca.gov

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

Re: Comments on Rulemaking for the California Consumer Privacy Act of 2018

The Student Loan Servicing Alliance (SLSA) appreciates the opportunity to provide feedback on the California Consumer Protection Act (CCPA) in advance of proposed rulemaking. SLSA is a non-profit trade association that represents federal and private student loan servicers, who collectively service over 90% of all student loans in the country. Members of SLSA are committed to handling consumer data with care and transparency, and the CCPA is an important tool understanding expectations for processing data protecting consumer privacy rights. SLSA believes that continued focus on privacy is critical, and we hope the rulemaking on CCPA will allow for harmonization with existing federal and CA state law to ensure implementation recognizes the complexity of the issues as we all work to better protect consumers.

Enclosed are annotated copies of the CCPA that identify provisions we hope will be further clarified and defined in the CCPA's rulemaking process. We would also like to bring attention to the following issues, which are applicable to the broader statute.

Implementation Timeframe

The CCPA's effective date is January 1, 2020, and compliance with CCPA will require significant IT development and investment for SLSA members. It is imperative that these compliance efforts are driven by a complete understanding of the CCPA and its implementing regulations. While the enforcement date is currently scheduled to be after the effective date, given the fact implementing regulations for the CCPA have not yet been proposed, SLSA requests that enforcement of the CCPA be assessed for further adjustment based on the timing of the final CCPA regulations and their complexity. SLSA members anticipate that IT development efforts will take between six (6) and twelve (12) months after the issuance of final CCPA regulations depending upon the nature of those final regulations. This is especially critical as insufficient time to properly implement and validate these processes could expose consumers to further privacy concerns.

Data Owners vs. Data Processors

Several provisions and disclosures required under CCPA are most appropriate for businesses that collect data directly from consumers. Data processors (i.e. service providers) are neither well-positioned to provide the disclosures required under CCPA, nor delete data in response to a consumer's request. SLSA recommends creating a distinction between data owners and data processors, as well as clarifying which requirements apply to each business type. While the statute reflects intent as it relates to data owners, there are third-party data processors or servicers – such as our members – who have unique circumstances and relationships with the underlying data and its control that differ from those of data owners, and therefore need to be fully contemplated in any rulemaking.

Data Deletion and Applicable Record Retention Requirements

The CCPA requires businesses to delete data upon receipt of a request from the consumer unless the business is processing the data under an exception in CCPA. The regulations should clarify that businesses are not required to delete consumer data if doing so would violate other retention requirements under the law. SLSA also requests further clarification regarding complying with CCPA and GLBA, in order to avoid direct and unreconcilable conflict with various laws to which an entity must comply.

Beyond these three broad areas of clarification, we have also highlighted in the annotated statute areas that include defining “verifiable consumer request,” guidance on how to determine residency in a way that can be practically implemented, and other considerations. SLSA looks forward to continuing to partner with California on protecting consumer privacy rights. We are happy to provide additional information, examples specific to the unique market of third-party student loan servicing, or examples to facilitate rulemaking. If you would like to discuss the comments provided, please contact me at [REDACTED] or [REDACTED].

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'C. Tapscott Buchanan', with a large, stylized flourish at the end.

C. Tapscott Buchanan
Executive Director

**STUDENT LOAN SERVICING ALLIANCE
COMMENTS ON RULEMAKING FOR THE CCPA
MARCH 8, 2019**

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS

SECTION 1.

This measure shall be known and may be cited as “The California Consumer Privacy Act of 2018.”

SEC. 2.

The Legislature finds and declares that:

- (a) In 1972, California voters amended the California Constitution to include the right of privacy among the “inalienable” rights of all people. The amendment established a legal and enforceable right of privacy for every Californian. Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information.
- (b) Since California voters approved the right of privacy, the California Legislature has adopted specific mechanisms to safeguard Californians’ privacy, including the Online Privacy Protection Act, the Privacy Rights for California Minors in the Digital World Act, and Shine the Light, a California law intended to give Californians the ‘who, what, where, and when’ of how businesses handle consumers’ personal information.
- (c) At the same time, California is one of the world’s leaders in the development of new technologies and related industries. Yet the proliferation of personal information has limited Californians’ ability to properly protect and safeguard their privacy. It is almost impossible to apply for a job, raise a child, drive a car, or make an appointment without sharing personal information.
- (d) As the role of technology and data in the every daily lives of consumers increases, there is an increase in the amount of personal information shared by consumers with businesses. California law has not kept pace with these developments and the personal privacy implications surrounding the collection, use, and protection of personal information.
- (e) Many businesses collect personal information from California consumers. They may know where a consumer lives and how many children a consumer has, how fast a consumer drives, a consumer’s personality, sleep habits, biometric and health information, financial information, precise geolocation information, and social networks, to name a few categories.
- (f) The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm.
- (g) In March 2018, it came to light that tens of millions of people had their personal data misused by a data mining firm called Cambridge Analytica. A series of congressional hearings highlighted that our personal information may be vulnerable to misuse when shared on the Internet. As a result, our desire for privacy controls and transparency in data practices is heightened.

(h) People desire privacy and more control over their information. California consumers should be able to exercise control over their personal information, and they want to be certain that there are safeguards against misuse of their personal information. It is possible for businesses both to respect consumers' privacy and provide a high level transparency to their business practices.

(i) Therefore, it is the intent of the Legislature to further Californians' right to privacy by giving consumers an effective way to control their personal information, by ensuring the following rights:

(1) The right of Californians to know what personal information is being collected about them.

(2) The right of Californians to know whether their personal information is sold or disclosed and to whom.

(3) The right of Californians to say no to the sale of personal information.

(4) The right of Californians to access their personal information.

(5) The right of Californians to equal service and price, even if they exercise their privacy rights.

SEC. 3.

Title 1.81.5 (commencing with Section 1798.100) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.5. California Consumer Privacy Act of 2018

1798.100.

(a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

SLSA requests that the CCPA regulations explicitly define "categories of personal information" and "categories of sources", as both terms are referenced throughout the statute. We also request that the regulation further define "verifiable consumer request" in order to clarify expectations of consumers and businesses related to such requests. As written, the provision is vague and could create additional frivolous complaints which, in turn, may make it more difficult for businesses to address consumers who are exercising legitimate privacy rights.

(b) A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

SLSA requests that CCPA clarify the timing of this requirement. Student loan servicers are unable to provide the required information "at or before the point of collection" because the information is collected from a prior servicer or a loan holder, and loan holders have a contractual relationship with the consumer. Additionally, student loan servicers' use of information is limited to the provisions of the loan holder's annual Gramm-Leach-Bliley-Act privacy notice. Providing additional disclosures is likely to confuse consumers, rather than empower them to exercise their privacy rights. SLSA recommends an exemption to this

requirement for businesses that comply with Gramm-Leach-Bliley Act initial and annual privacy notice requirements.

(c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.

(d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

SLSA requests that the requirement to make information accessible “without hindrance” be further defined to ensure that data produced in accordance with (d) is accessible to other entities. Because student loan servicers process data provided by loan holders, options for ensuring other entities can use consumer data are limited.

(e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

SLSA recommends further defining “one-time” transaction to clarify which transactions are in-scope (e.g. check cashing, defined loan applications, general inquiries, etc.). Additionally, SLSA requests that (e) be clarified as follows, “This section shall not require a business to retain any personal information collected for a single, one-time transaction, (i) if such information is not sold or retained by the business, or (ii) to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.”

1798.105.

(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

Businesses may collect information about the same consumer for multiple purposes. In this scenario, the data is partially excluded from this requirement under 1798.145(c), but also partially subject to this requirement. SLSA requests clarification on whether businesses in this scenario are required to delete all data, or whether they are able to keep the parts of the data that are excluded under 1798.145(c).

(b) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (A) of paragraph (5) of subdivision (a) of Section 1798.130, the consumer’s rights to request the deletion of the consumer’s personal information.

Businesses handling data solely as described under (d) of this Section will ultimately deny all consumer requests under this provision. To reduce confusion among consumers, SLSA

recommends an exemption to this disclosure requirement for businesses handling data solely as described in (d).

(c) A business that receives a verifiable request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.

(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

(6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(8) Comply with a legal obligation.

(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

1798.110.

(a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

(1) The categories of personal information it has collected about that consumer.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) The specific pieces of personal information it has collected about that consumer.

SLSA requests clarification of what constitutes "specific pieces of personal information the business has collected"? For example, is it sufficient to disclose that a business collected the consumer's IP address, or does the business also need to disclose the particular IP address?

- (b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable request from the consumer.
- (c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:
- (1) The categories of personal information it has collected about that consumer.
 - (2) The categories of sources from which the personal information is collected.
 - (3) The business or commercial purpose for collecting or selling personal information.
 - (4) The categories of third parties with whom the business shares personal information.
 - (5) The specific pieces of personal information the business has collected about that consumer.

(d) This section does not require a business to do the following:

- (1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.
- (2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information

SLSA recommends clarifying the timeline in which information for single one-time transactions must be deleted in order to fall under the exemption in (d).

1798.115.

(a) A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

- (1) The categories of personal information that the business collected about the consumer.
- (2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.
- (3) The categories of personal information that the business disclosed about the consumer for a business purpose.

(b) A business that sells personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to paragraph (4) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable request from the consumer.

(c) A business that sells consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

- (1) The category or categories of consumers' personal information it has sold, or if the business has not sold consumers' personal information, it shall disclose that fact.
- (2) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out pursuant to 1798.120.

1798.120.

(a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt out.

(b) A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the right to opt out of the sale of their personal information.

(c) A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited, pursuant to paragraph (4) of subdivision (a) of Section 1798.135, from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.

(d) Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt in."

SLSA recommends explicit exemption from the requirements in Section 1798.120 for businesses that do not sell data. It is unclear whether businesses are required to honor consumer opt-out requests when data is shared for a legitimate purpose other than sale.

1798.125.

(a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer's rights under this title.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data.

(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data.

(2) A business that offers any financial incentives pursuant to subdivision (a), shall notify consumers of the financial incentives pursuant to Section 1798.135.

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.135 which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.

(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

SLSA requests clarification on distinguishing legitimate value that can be tied to financial incentives under 1798.125(b) from the improper incentives prohibited in 1798.125(a), what it means to derive value from data, and the definition of "financial incentive".

1798.130.

(a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, in a form that is reasonably accessible to consumers, a business shall:

(1) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.

(2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable request, but this shall not extend the business's duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business's receipt of the verifiable request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business shall not require the consumer to create an account with the business in order to make a verifiable request.

SLSA requests guidance on complying with 1798.130 in the following scenarios:

- The business is unable to locate the consumer's information based on the content of the consumer's request. For example, if the consumer is making a request pursuant to Sections 1798.10 and 1798.115, but the business did not collect the consumer's name or demographic information that the consumer is providing in their request, the regulations should clarify that the business is not required to provide the information requested.

- The consumer's data has already been deleted at the time of the consumer's request. Businesses typically do not keep records of data that have already been deleted and may be unable to comply with 1798.130 absent additional clarification.

(3) For purposes of subdivision (b) of Section 1798.110:

(A) To identify the consumer, associate the information provided by the consumer in the verifiable request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its Internet Web site, and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.

(B) For purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact.

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in

subdivision (c) that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Sections 1798.110, 1798.115, 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business's verification of the consumer's request solely for the purposes of verification.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.110 and 1798.115 shall follow the definition of personal information in Section 1798.140.

1798.135.

(a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

(2) Include a description of a consumer's rights pursuant to Section 1798.120, along with a separate link to the "Do Not Sell My Personal Information" Internet Web page in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers' privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer.

(5) For a consumer who has opted out of the sale of the consumer's personal information, respect the consumer's decision to opt out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information.

SLSA requests guidance on obtaining authorization for the sale of personal information after the expiration of the 12-month period. Specifically, must the authorization be explicit or written?

Are implied authorizations acceptable? For example, if a business provides the disclosures required under 1798.120 in order to resume the sale of the consumer's data and provides a deadline for opt-out, can the business resume the sale of data if the consumer has not responded?

(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(b) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes

reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

(c) A consumer may authorize another person solely to opt out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General.

SLSA requests clarification on whether consumers may authorize another person to opt in to the sale of personal data on the consumer's behalf.

1798.140.

For purposes of this title:

(a) "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been de-identified.

(b) "Biometric information" means an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) "Business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) Has annual gross revenues in excess of twenty-five million dollars (\$25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the

management of a company. “Common branding” means a shared name, servicemark, or trademark.

(d) “Business purpose” means the use of personal information for the business’ or a service provider’s operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are:

- (1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.
- (2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.
- (3) Debugging to identify and repair errors that impair existing intended functionality.
- (4) Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer’s experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.
- (5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.
- (6) Undertaking internal research for technological development and demonstration.
- (7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

(e) “Collects,” “collected,” or “collection” means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer’s behavior.

(f) “Commercial purposes” means to advance a person’s commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. “Commercial purposes” do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

(g) “Consumer” means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

SLSA requests rulemaking clarification that a consumer’s state of residence may be determined by the address provided to the business. Clearly, residency as defined under the law, is not an

attribute that most businesses would be aware of, and providing a clarification that consumer provision of mailing address shall suffice for determination purposes is needed. The regulations should also clarify expected treatment of consumers who were not California residents at the time of collection, but subsequently become California residents and submit requests under the CCPA.

(h) “Deidentified” means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(2) Has implemented business processes that specifically prohibit reidentification of the information.

(3) Has implemented business processes to prevent inadvertent release of deidentified information.

(4) Makes no attempt to reidentify the information.

(i) “Designated methods for submitting requests” means a mailing address, email address, Internet Web page, Internet Web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

(j) “Device” means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.

(k) “Health insurance information” means a consumer’s insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer’s application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.

(l) “Homepage” means the introductory page of an Internet Web site and any Internet Web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application’s platform page or download page, a link within the application, such as from the application configuration, “About,” “Information,” or settings page, and any other location that allows consumers to review the notice required by subdivision (a) of Section 1798.145, including, but not limited to, before downloading the application.

(m) “Infer” or “inference” means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(n) “Person” means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(o) (1) “Personal information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following:

- (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
 - (B) Any categories of personal information described in subdivision (e) of Section 1798.80.
 - (C) Characteristics of protected classifications under California or federal law.
 - (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
 - (E) Biometric information.
 - (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
 - (G) Geolocation data.
 - (H) Audio, electronic, visual, thermal, olfactory, or similar information.
 - (I) Professional or employment-related information.
 - (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
 - (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
- (2) "Personal information" does not include publicly available information. For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. "Publicly available" does not include consumer information that is deidentified or aggregate consumer information.
- SLSA recommends narrowing the scope of personal information in alignment with existing federal law.**

(p) "Probabilistic identifier" means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(q) "Processing" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.

(r) "Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(s) "Research" means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business' service or device for other purposes shall be

- (1) Compatible with the business purpose for which the personal information was collected.
- (2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.
- (3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
- (4) Subject to business processes that specifically prohibit reidentification of the information.
- (5) Made subject to business processes to prevent inadvertent release of deidentified information.
- (6) Protected from any reidentification attempts.
- (7) Used solely for research purposes that are compatible with the context in which the personal information was collected.
- (8) Not be used for any commercial purpose.
- (9) Subjected by the business conducting the research to additional security controls limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

- (i) (1) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.
- (2) For purposes of this title, a business does not sell personal information when:
 - (A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.
 - (B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.
 - (C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purposes if both of the following conditions are met: services that the service provider performs on the business' behalf, provided that the service provider also does not sell the personal information.
 - (i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135
 - (ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.
 - (D) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business provided that information is used or shared consistently with Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and

Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(u) “Service” or “services” means work, labor, and services, including services furnished in connection with the sale or repair of goods.

(v) “Service provider” means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

(w) “Third party” means a person who is not any of the following:

(1) The business that collects personal information from consumers under this title.

(2) A person to whom the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract:

(A) Prohibits the person receiving the personal information from:

(i) Selling the personal information.

(ii) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.

(iii) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

(B) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

A person covered by paragraph (2) that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by paragraph (2) in compliance with paragraph (2) shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.

(s) “Unique identifier” or “Unique personal identifier” means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, “family” means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

(y) “Verifiable consumer request” means a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer’s behalf.

SLSA recommends that the regulations specify parameters for a verifiable consumer request, specifically what data or matches would verify the specific consumer. This clarification is essential to protect the consumer from the privacy risks of unverified requests, but also to provide the practical threshold for entities to be able to determine consumer data in scope since there may be data collected actively or passively that cannot be validated to be related to a consumer depending on levels of verification described.

In addition, SLSA recommends a safe harbor in the event fraud is committed due to an individual other than the consumer requesting data where that individual provides enough information to fraudulently verify as the specific consumer and obtaining personal information. In this scenario, the business should be held harmless if it has taken reasonable efforts to comply with the verification parameters.

1798.145.

(a) The obligations imposed on businesses by this title shall not restrict a business’s ability to:

- (1) Comply with federal, state, or local laws.
- (2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.
- (3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.
- (4) Exercise or defend legal claims.
- (5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.
- (6) Collect or sell a consumer’s personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer’s personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

Given the fact that online services are becoming the primary means by which business interact with consumers, SLSA requests clarification on identifying residents of California in the absence of a postal address. Without postal address, the rulemaking should address how to determine

residency or what safe harbor an entity may rely upon to determine whether this law is applicable.

(b) The obligations imposed on businesses by Sections 1798.110 to 1798.135, inclusive, shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c) This act shall not apply to protected or health information that is collected by a covered entity governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56 of Division 1)) or governed by the privacy, security, and breach notification rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Availability Act of 1996. For purposes of this subdivision, the definition of "medical information" in Section 56.05 shall apply and the definitions of "protected health information" and "covered entity" from the federal privacy rule shall apply.

(d) This title shall not apply to the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined by subdivision (d) of Section 1681a of Title 15 of the United States Code, and use of that information is limited by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

(e) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, if it is in conflict with that law.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.), if it is in conflict with that act.

(g) Notwithstanding a business' obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to any verified consumer request may be extended by up to 90 additional days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.

SLSA requests that “repetitive character” be defined as more than twice in a 12-month period, consistent with 1798.100(d).

(h) A business that discloses personal information to a service provider shall not be liable under this title if the service provider receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title.

(i) This title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(j) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.

1798.150.

(a) (1) Any consumer whose nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’ violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant’s misconduct, and the defendant’s assets, liabilities, and net worth.

These damages provisions appear to conflict with those of California’s data breach law (Section 1798.84), which specifies damages and requirements for customers impacted by a security breach under Section 1798.82. SLSA strongly recommends that the CCPA and regulations be updated to explicitly incorporate California’s existing data breach law to resolve the conflict.

(b) Actions pursuant to this section may be brought by a consumer if all of the following requirements are met:

(1) Prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer shall provide a business 30 days’ written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide

statutory damages may be initiated against the business. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

(2) A consumer bringing an action as defined in paragraph (1) of subdivision (c) shall notify the Attorney General within 30 days that the action has been filed.

(3) The Attorney General, upon receiving such notice shall, within 30 days, do one of the following:

(A) Notify the consumer bringing the action of the Attorney General's intent to prosecute an action against the violation. If the Attorney General does not prosecute within six months, the consumer may proceed with the action.

(B) Refrain from acting within the 30 days, allowing the consumer bringing the action to proceed.

(C) Notify the consumer bringing the action that the consumer shall not proceed with the action.

(c) Nothing in this act shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

1798.155.

Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title.

(a) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be liable for a civil penalty as provided in Section 17206 of the Business and Professions Code in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.

(b) Notwithstanding Section 17206 of the Business and Professions Code, any person, business, or service provider that intentionally violates this title may be liable for a civil penalty of up to seven thousand five hundred dollars (\$7,500) for each violation.

(c) Notwithstanding Section 17206 of the Business and Professions Code, any civil penalty assessed pursuant to Section 17206 for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (a), shall be allocated as follows:

(1) Twenty percent to the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.109, with the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with this title.

(2) Eighty percent to the jurisdiction on whose behalf the action leading to the civil penalty was brought.

(d) It is the intent of the Legislature that the percentages specified in subdivision (c) be adjusted as necessary to ensure that any civil penalties assessed for a violation of this title fully offset any costs incurred by the state courts and the Attorney General in connection with this title, including a sufficient amount to cover any deficit from a prior fiscal year.

1798.160.

(a) A special fund to be known as the “Consumer Privacy Fund” is hereby created within the General Fund in the State Treasury, and is available upon appropriation by the Legislature to offset any costs incurred by the state courts in connection with actions brought to enforce this title and any costs incurred by the Attorney General in carrying out the Attorney General’s duties under this title.

(b) Funds transferred to the Consumer Privacy Fund shall be used exclusively to offset any costs incurred by the state courts and the Attorney General in connection with this title. These funds shall not be subject to appropriation or transfer by the Legislature for any other purpose, unless the Director of Finance determines that the funds are in excess of the funding needed to fully offset the costs incurred by the state courts and the Attorney General in connection with this title, in which case the Legislature may appropriate excess funds for other purposes.

1798.175.

This title is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers’ personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80). The provisions of this title are not limited to information collected electronically or over the Internet, but apply to the collection and sale of all personal information collected by a business from consumers. Wherever possible, law relating to consumers’ personal information should be construed to harmonize with the provisions of this title, but in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

1798.180.

This title is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers’ personal information by a business.

1798.185.

(a) On or before January 1, 2020, the Attorney General shall solicit broad public participation to adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

- (1) Updating as needed additional categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (o) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.
- (2) Updating as needed the definition of unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and additional categories to the definition of designated methods for submitting requests to facilitate a consumer’s ability to obtain information from a business pursuant to Section 1798.130.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter

(4) Establishing rules and procedures for the following, within one year of passage of this title and as needed thereafter.

(A) To facilitate and govern the submission of a request by a consumer to opt out of the sale of personal information pursuant to paragraph (1) of subdivision (a) of Section 1798.145.

(B) To govern business compliance with a consumer's opt-out request.

(C) The development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt out of the sale of personal information.

(5) Adjusting the monetary threshold in subparagraph (A) of paragraph (1) of subdivision (b) of Section 1798.106 in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter.

(7) Establishing rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business' determination that a request for information received by a consumer is a verifiable request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business' authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

(b) The Attorney General may adopt additional regulations as necessary to further the purposes of this title.

1798.190.

If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title.

1798.192.

Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable

This section shall not prevent a consumer from declining to request information from a business, declining to opt out of a business' sale of the consumer's personal information, or authorizing a business to sell the consumer's personal information after previously opting out.

1798.194.

This title shall be liberally construed to effectuate its purposes.

1798.196.

This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the California Constitution.

1798.198.

(a) Subject to limitation provided in subdivision (b), this title shall be operative January 1, 2020.

(b) This act shall become operative only if initiative measure No. 17-0039, The Consumer Right to Privacy Act of 2018, is withdrawn from the ballot pursuant to Section 9604 of the Elections Code.

SEC. 4.

(a) The provisions of this bill are severable. If any provision of this bill or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.

Message

From: Bomberg, Jared A. [REDACTED]
Sent: 3/8/2019 1:30:39 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Jaffe, Dan [REDACTED]; Christopher Oswald [REDACTED]; dcstaff [REDACTED]; Potashnik, Tara
Sugiyama [REDACTED]; Ingis, Stuart [REDACTED]
Subject: Comments on the CCPA
Attachments: ANA CCPA Comments.pdf

Please find attached comments on the CCPA submitted on behalf of the Association of National Advertisers. Please contact Dan Jaffe, Group Executive Vice President, at [REDACTED] or [REDACTED] with any questions regarding these comments.

Jared Bomberg

Jared A. Bomberg, Esq. | Venable LLP

[REDACTED]
600 Massachusetts Avenue, NW, Washington, DC 20001

[REDACTED] | www.Venable.com

This electronic mail transmission may contain confidential or privileged information. If you believe you have received this message in error, please notify the sender by reply transmission and delete the message without copying or disclosing it.



LEADERSHIP AND
MARKETING EXCELLENCE

**Before the
California Department of Justice
Los Angeles, CA 90013**

COMMENTS
of the
ASSOCIATION OF NATIONAL ADVERTISERS
on
The California Consumer Privacy Act

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
2020 K Street, NW
Suite 660
Washington, DC, 20006
[REDACTED]

Counsel:
Stu Ingis
Tara Potashnik
Jared Bomberg
Venable LLP
600 Massachusetts Ave., NW
Washington, DC 20001
[REDACTED]

March 8, 2019

California Consumer Privacy Act Comments

The Association of National Advertisers (“ANA”) provides these comments in response to the California Attorney General’s (“CA AG”) request for public comment on the California Consumer Privacy Act (“CCPA”).

ANA is the advertising industry’s oldest trade association. ANA’s membership includes nearly 2,000 companies and marketing solutions providers, with 25,000 brands that engage almost 150,000 industry professionals and collectively spend or support more than \$400 billion in marketing and advertising annually. Nearly every advertisement in print, online, or on TV is connected in some way to ANA members’ activities. In California, advertising helps generate \$767.7 billion (16.4% of the state’s economic activity) and helps produce 2.7 million jobs (16.8% of all jobs in the state). ANA’s members include a broad range of major national advertisers, leading marketing data science and technology suppliers, ad agencies, law firms, consultants, and vendors. We also count among our membership a large number of nonprofit organizations and charities that, while ostensibly exempted from the provisions of the CCPA, in fact, are significantly impacted by the CCPA, as they rely heavily on data and marketing to reach donors and carry out their missions. Many of ANA’s members are headquartered in California or carry out significant business in the state.

ANA strongly supports the underlying goals of the CCPA. Privacy is an extraordinarily important value that deserves meaningful protections in the marketplace. As an industry, advertisers and marketers have taken a number of major steps to put these values into practice—investing multi-millions of dollars providing consumers greater control over data, transparency with respect to the collection, use and transfer of data, and implementing strong self-regulatory bodies and codes including the highly lauded Digital Advertising Alliance (“DAA”) program to help ensure accountability in regard to privacy and fair practices in the marketplace.

As our members prepare to implement the CCPA, additional clarity regarding various provisions would help ensure compliance with the law and enhance consumer privacy. Such clarifications and interpretations fall specifically within the CA AG’s regulatory authority provided under the law.¹ We urge the CA AG to issue regulations on the following matters:

Priority Issues for the California Attorney General to Address

1. Preserve Loyalty Discount Programs
2. Clarify the Rules for Consumer Requests by Authorized Representatives to Ensure that Consumers are Protected
3. Allow “Third Parties” to Rely on Written Attestations of “Explicit Notice”
4. Enable Granular Choices for Consumers Exercising CCPA Rights
5. Prevent the Need to Create an Ever-Expanding Multiplicity of Individualized Privacy Policies
6. Clarify “Household” in the Definition of “Personal Information”

¹ Cal. Civ. Code § 1798.185.

7. Clarify “Professional or Employment Related Information” in the Definition of “Personal Information”
8. Distinguish “Pseudonymized” Data from “Personal Information”
9. Clarify the “Cure” Requirement for Security Breaches

Key Additional Issues for the California Attorney General to Address

1. Clarify that Businesses Have Flexibility When Verifying Consumer Requests
2. Preserve Ad Measurement and Attribution Activities
3. Clarify the Scope of the “Publicly Available” Information Exclusion
4. Clarify the 12-Month Look-Back Provision
5. Limit the CCPA’s Unintended Impact on Nonprofit Organizations, Including Charities
6. Preserve the Ability to Provide Expected Marketing Messages to Consumers
7. Ensure the Viability of the Fraud Exception
8. Clarify the Definition of “Business Purpose”
9. Clarify the Operative Ages in the Opt-In Requirement Related to Minors
10. Remove Backup Information from the Scope of a Deletion Request
11. Ensure that Businesses Do Not Have to Collect Extra Data to Comply with CCPA Requirements

I. Priority Issues for the California Attorney General to Address

This section identifies priority areas within the CCPA that would benefit from the CA AG’s clarification, describes the real-world impacts of these issues, cites the CA AG’s statutory authority for addressing such issues through regulation, and provides suggestions for the content of such rules.

1. Preserve Loyalty Discount Programs

The CCPA prohibits price and service “discrimination,” among other practices, against consumers who have exercised their CCPA rights, but it creates these prohibitions with imprecise drafting that could be interpreted to prohibit traditional loyalty discount programs.² Loyalty discount programs could be considered a discriminatory practice under the CCPA because these programs create different price levels between consumers. Consumers who make deletion or opt-out requests of their data restrict the very data that allows them to participate in a loyalty program. As a result, those consumers who choose not to participate in a loyalty program will automatically be treated differently than other consumers in the program. This difference in treatment could run afoul of the ambiguous wording in the law, which states in one section that

² The CCPA states: “A business shall not discriminate against a consumer because the consumer exercised any of the consumer’s rights under this title, including... by:... [c]harging different prices or rates for goods or services, including through the use of discounts or other benefits imposing penalties.... Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer’s data.” Cal. Civ. Code §§ 1798.125(a)(1)-(2).

these programs must be “reasonably related” to the value provided to the consumer, while the law states in another section that these programs must be “directly related” to the value provided to the consumer.³ Confusion exists as to which standard applies, and the law provides no additional guidance on how to measure whether a program is reasonably or directly related to the value provided to consumers.

Without clarification, many loyalty programs could cease altogether when the CCPA becomes effective. Loyalty programs allow businesses to maintain and foster positive relationships with consumers. They provide consumers significant benefits in the form of lower prices and access to special offers. The vast number of consumers, including a broad range of California consumers, who have and are voluntarily participating in loyalty programs over many years demonstrates the popularity and value these programs provide. ANA therefore asks the CA AG to permit a business to offer loyalty-based discount programs that consumers value and expect without the program constituting discrimination under the CCPA. For instance, we ask that the CA AG interpret “reasonably related” and “directly related” to the value provided to consumers to include the collection, use, and sharing of any data that is needed to provide a loyalty discount program and other consumer benefits.⁴ Consumers that provide such data to participate in a loyalty program would obtain value through the loyalty program that is reasonably and directly related to the value of the consumer’s data because without the consumer’s data, the loyalty program would not be possible. Such clarification would help ensure the continued use of loyalty programs under the CCPA.

2. Clarify the Rules for Consumer Requests by Authorized Representatives to Ensure that Consumers are Protected

The CCPA allows individuals and entities to make access, deletion, or opt-out requests on behalf of consumers, so long as such parties’ actions constitute a “verifiable consumer request” under the law.⁵ However, the CCPA is silent on whether these authorized representatives of consumers must inform consumers of the implications and outcomes of exercising their CCPA choices with respect to the personal information held by a particular business. As such, a third-party requestor could choose not to provide relevant information to a

³ Compare Cal. Civ. Code § 1798.125(a)(2) (“reasonably related”) with Cal. Civ. Code § 1798.125(b)(1) (“directly related”).

⁴ The CA AG has authority to issue regulations to “further the purposes of [the] title.” Cal. Civ. Code §§ 1798.185(a), (b). The clarification we seek would further the purposes of the title because the current provision related to discrimination and the acceptable uses of customer incentives is: (a) vague and (b) may conflict with Section 1798.145 of the law, which states “[t]he rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.” Cal. Civ. Code § 1798.145(j). Without the clarification we propose or a similar clarification, many loyalty programs would cease altogether, which would adversely affect the rights of other consumers who wish to participate in and receive the benefits of such programs.

⁵ The CCPA states: “Verifiable consumer request” means a request that is made by a consumer... or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can reasonably verify, pursuant to regulations adopted by the CA AG pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information.” Cal. Civ. Code § 1798.140(y).

consumer concerning the implications of exercising CCPA rights, which would impede the consumer's ability to make an informed choice because the consumer would not have necessary information. Furthermore, the CCPA is silent on whether authorized representatives must have any particular qualifications or make any representations about the use(s) they will make of the consumer data they receive. It is possible that an authorized representative with no relevant qualifications for handling consumer requests could make a request on behalf of a consumer without fully informing the consumer of the implications of making such a request. Such authorized representatives could also manipulate information presented to consumers to attempt to influence a consumer's decision on whether to make a request. This is not a theoretical concern—ANA members have had to combat unauthentic consumer requests by third parties allegedly acting on behalf of consumers under current privacy standards—but a present challenge that will increase significantly without guidance from the CA AG. Consumer choice works when the choice by consumers is informed. When businesses stand in between the consumer and the business that must carry out the request, the choice model is placed at risk because it is not clear what information will be presented to the consumer to trigger their choice and whether they effectively communicate those choices.

To serve as an authorized representative for a consumer request under the CCPA, we suggest that the CA AG issue a rule that the authorized representative must properly inform a consumer of their choices and the implications of exercising such choices (*e.g.*, no longer receiving new offers from the business).⁶ This notification requirement is important because the business that ultimately must comply with the request may not be able to directly discuss potential impacts of the request with the consumer. For a business to obtain verifiable consumer consent, a consumer must be properly informed of choices. We also request that the CA AG issue a rule creating specific requirements for authorized representatives who gather and facilitate consumer CCPA requests and consider whether the business is serving the public interest or is manipulating consumers, or not effectuating their choices. For instance, the rule would require an authorized representative to obtain a consumer's written authorization detailing what requests will be made what the implications of those requests are, and how any data collected from the consumer will be used; the CA AG would conduct oversight over these entities.

3. Allow "Third Parties" to Rely on Written Attestations of "Explicit Notice"

The CCPA prevents a third party that has received consumer personal information from a business (and not consumers directly) from selling such personal information unless the consumer has received "explicit notice" and is provided an opportunity to exercise the right to opt out.⁷ The CCPA does not define "explicit notice" or clarify how third-party companies that do not have a direct relationship with consumers must provide such notice. As a result, if the law

⁶ The CA AG has authority to issue this clarification pursuant to Cal. Civ. Code § 1798.185(a)(7), which allows him to establish "rules and procedures... to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130...." By clarifying the meaning of a verifiable consumer request, the CA AG would facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to the regulatory authority listed in the law.

⁷ Cal. Civ. Code § 1798.115(d).

is interpreted to require third parties to provide direct notice to consumers before selling covered information, third parties may not be able to do so and would be prevented from selling such data. This outcome could impact sales of data that have no privacy implications and that are necessary to deliver products and services that consumers value, or that would protect against fraud. In these circumstances, third parties ought to be able to rely on their data providers to ensure the CCPA-required “explicit notice” is given, as those data providers have a direct relationship with consumers or should have knowledge of whether legal obligations have been met. The law should recognize that written assurances from the provider of the data, along with explicit notice on a website by the receiver of the data, is a sufficient compliance approach under the circumstances.

We urge the CA AG to clarify the “explicit notice” requirement for third parties to ensure that a third party can rely on written attestations of compliance when receiving data from other businesses.⁸ Businesses that rely on written attestations of compliance also should be required to make the same disclosures to consumers in their online privacy policy representations. With this interpretation of the statute, consumers will have better access to the information contemplated in the explicit notice requirement because contractual representations and warranties mandated by this interpretation will help ensure that appropriate disclosures are provided to consumers. Also, requiring businesses that receive information down the chain to place consumer disclosures in their online privacy policies would advance the intent behind the “explicit notice” requirement. Without this interpretation, third parties will be forced to operate as first parties in the digital ecosystem, which may be impossible for many third parties that have no direct relationship with consumers and no clear way to create such a relationship. As a result, many third parties may no longer be able to operate, which could substantially unravel the seamless nature of the Internet that consumers rely upon. In particular, many products and services in the digital economy that consumers value, including anti-fraud products that rely on consumer data to identify fraudulent activity, could be jeopardized because the data transfers by third parties without a direct consumer relationship needed to create or deliver those products would be prohibited.

4. Enable Granular Choices for Consumers Exercising CCPA Rights

The CCPA allows consumers to access all of their personal information, entirely opt out of the sale of their data, or entirely delete their data from businesses’ systems.⁹ The law, however, does not explicitly state that a business may allow a consumer the choice to access, delete, or opt out from the sale of *some, but not all*, of their data. As a result, a consumer request may be interpreted to cover all of the consumer’s data even though a consumer only wants part of their data deleted or restricted from further sharing. This issue is especially challenging when

⁸ The CA AG has authority to interpret the “explicit notice” provision pursuant to Cal. Civ. Code § 1798.185(a)(7), which contemplates rules to “facilitate a consumer’s or the consumer’s authorized agent’s ability to obtain information pursuant to Section 1798.130.” Third parties should be required to provide an online opt-out notice and be allowed to ensure through contractual commitments from data providers that proper CCPA disclosures were made to consumers. Such activities will help ensure that opt-out notices and instructions are provided to consumers by the entities that have a direct relationship with them. The CA AG also has authority to interpret this provision pursuant to his general authority to issue rules “as necessary to further the purposes of [the] title.” Cal. Civ. Code §§ 1798.185(a), (b).

⁹ Cal. Civ. Code §§ 1798.100, 105(c), 110, 115, 120(a).

a company has multiple products or services with consumer information or multiple subsidiaries that interact with the same consumer. Determining what data sets a consumer refers to in a consumer request can be complex, and this job is made harder by vague consumer requests and by third parties acting as authorized representatives who may not know exactly what the consumer wishes to be deleted or restricted from sharing.

We ask that the CA AG clarify that consumers may have the option to choose the types of sales they want to opt out of or the types of data they want deleted instead of mandating one all-or-nothing opt-out or deletion requirement.¹⁰ Consumers may wish to make granular choices regarding the use and maintenance of their data, and a regulation clarifying that such granularity is permissible should be issued. Paradoxically, failure to take this step may undermine privacy protections because a consumer may decide not to restrict any use of his data by a company if the consumer is only concerned about specific limited uses of his information.

5. Prevent the Need to Create an Ever-Expanding Multiplicity of Individualized Privacy Policies

Imprecise drafting in the CCPA may require privacy policies to disclose the “specific pieces of personal information the business has collected about that consumer.”¹¹ Because data differs from one consumer to another, to comply with this provision, a business would need to create personalized privacy policies for each consumer that visits their website. This process would be incredibly burdensome, costly and could raise the likelihood of inadvertent disclosures of specific consumer information to wrong recipients. This requirement also is found in the part of the law describing consumer access rights, which suggests that the provision could be meant to cover specific consumer access requests, not the content of required privacy policies.

We ask that the CA AG clarify that a business should not be required to create individualized privacy policies for each consumer to comply with the CCPA’s privacy policy provisions and that specific pieces of information should only be provided in response to a

¹⁰ The CA AG has authority to clarify this issue with respect to the opt-out right pursuant to Cal. Civ. Code § 1798.185(a)(4)(A), which directs him to establish rules “[t]o facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information.” The CA AG also has authority to interpret CCPA’s access and deletion rights pursuant to regulatory authority to “further the purposes of [the] title” in Cal. Civ. Code §§ 1798.185(a), (b). To create a consistent experience for consumers that reflects their expectations, the CA AG should clarify in rulemaking that consumers may have the same granular options with respect to access, deletion, and opt-out requests.

¹¹ Cal. Civ. Code § 1798.110(c) (“A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130: (5) The specific pieces of personal information the business has collected about that consumer.”); Cal. Civ. Code § 1798.130(a)(5)(B) (“In order to comply with [Section]... 1798.110... a business shall, in a form that is reasonably accessible to consumers... [d]isclose... in its online privacy policy... [f]or purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.”).

verifiable consumer access request.¹² By clarifying that individualized privacy policies are not required, the CA AG would prevent inadvertent disclosure of specific consumer personal information and facilitate the actual consumer's (or the consumer's authorized agent's) ability to obtain specific pieces of personal information through an access request separate from a general privacy policy disclosure, which could be viewed by multiple individuals and lead to unwanted privacy invasions.

6. Clarify "Household" in the Definition of "Personal Information"

"Personal information" under the CCPA "means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or *household*."¹³ The CCPA requires that a business provide "specific pieces of personal information it has collected about [a] consumer," in response to a consumer request.¹⁴ Because the law creates an access right for personal information and the law's definition of personal information includes both consumer and household data, the CCPA could require that a business disclose information about a consumer within a household to another consumer in the same household through the course of a consumer access request.¹⁵ This interpretation, however, would effectively read out the specific language in the consumer access right provision that a consumer is entitled to personal information "about that consumer," not about the consumer's household.¹⁶ If the CCPA is interpreted to require that all household information associated with a consumer be provided in response to each consumer access request, this interpretation would result in major privacy and safety concerns as personal information may be provided to a household member such as an abusive spouse or a dishonest and self-serving roommate who should not have such information.

The CA AG should clarify that access requests are limited to the personal information known about the individual consumer making the request or about others in the household only if the individual making the request is an authorized representative of those other persons in the household.¹⁷ Specifically, the rulemaking should recognize that the term "about that consumer" in Section 1798.110 refers to only the personal information known about the individual consumer making the access request or the personal information that can be provided to the consumer as an authorized representative of other consumers in the same household.

¹² The CA AG has authority to interpret this provision pursuant to Cal. Civ. Code § 1798.185(a)(7), which directs him to establish "rules and procedures... to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130..."

¹³ Cal. Civ. Code § 1798.140(o)(1) (emphasis added).

¹⁴ Cal. Civ. Code § 1798.110(a)(5).

¹⁵ Cal. Civ. Code §§ 1798.110; 140(o)(1).

¹⁶ Cal. Civ. Code § 1798.110(a)(5).

¹⁷ The CA AG has authority to issue this clarification pursuant to Cal. Civ. Code § 1798.185(a)(7), which allows him to "[e]stablish rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's...ability to obtain information..." The CA AG can carry out this directive by establishing rules that clarify when household information should be provided to a consumer.

7. Clarify “Professional or Employment Related Information” in the Definition of “Personal Information”

“Personal information” under the CCPA “means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household [including]... [p]rofessional or employment-related information.”¹⁸ As such, consumer access, deletion, and opt-out rights apply to the undefined concept of professional or employment-related information. Without further clarification, any employee of a business can potentially request that another business or the company by whom they are employed that has information on file or in a business-to-business context delete such data as well as any business information capable of being associated with the data.¹⁹ These deletion rights could create supply chain concerns and competitive concerns since the removal of business data could make due diligence on potential business partners or oversight of business partners impossible to carry out. Although professional and employment-related data in the CCPA could be interpreted to include employment information posted on social media or data used for marketing to individuals in their personal capacity, this data should not cover information on persons acting as a representative of an employer or business.

The phrase “professional or employment-related information” should be clarified to make clear it does not include information on persons acting as a representative of their employer or business such as business representatives and sole proprietors.²⁰ When a person is acting in the marketplace on behalf of an employer or business, the data that is captured is business data, not consumer data. Without a rule recognizing this distinction, an overly broad reading of the definition of personal information could allow employees to improperly access business information (thereby, potentially compromising confidential business data) or inappropriately take advantage of deletion and opt-out rights afforded to consumers under the CCPA. The CCPA is directed to consumer protection and this provision, if not clarified, would expand the law’s reach far beyond that scope.

8. Distinguish “Pseudonymized” Data from “Personal Information”

The CCPA’s definition of “personal information,” means any data that “is capable of being associated with... a particular consumer or household,” and a “consumer” is defined to include unique identifiers.²¹ Because pseudonymized data is associated with a unique identifier, and a “consumer” includes unique identifiers, pseudonymized data could be captured by the definition of personal information. However, the CCPA also creates a separate definition for “pseudonymize,” which suggests that pseudonymized data may be a distinct category of data

¹⁸ Cal. Civ. Code § 1798.140(o)(1)(I).

¹⁹ “Personal information” under the law includes “[p]rofessional or employment-related information.” *Id.*

²⁰ The CA AG has specific authority to adopt rules to “updat[e] as needed additional categories of personal information.” Cal. Civ. Code § 1798.185(a)(1). The clarification we propose aligns with this authority because the byproduct of the clarification is an additional category of personal information covering professional and employment-related information about an individual in his or her personal capacity and not their business capacity.

²¹ Cal. Civ. Code § 1798.140(o)(1); 140(g).

apart from personal information. According to the CCPA, pseudonymized data is rendered in a manner that does not directly identify a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that it is not attributed to an identified or identifiable consumer.²² Also, the CCPA's only reference to pseudonymized data is in the definition of research, where the CCPA lists pseudonymized data in the same category as de-identified data – data excluded from the definition of the term “personal information.”²³ As such, the CCPA does not explicitly resolve whether pseudonymized data is personal information or if pseudonymized data falls outside the definition of personal information.

If pseudonymized data is considered personal information under the law, the CCPA has the potential to force businesses to collect substantially more data about consumers so that they can individually identify a specific person that makes a CCPA request. For example, to effectuate consumer rights such as the rights to access, delete, or opt out of the sale of personal information under the CCPA, a business that does not have identifying information such as a name or email address could be forced to associate this data from the requester with non-identifiable device data that the business holds. This approach would remove existing data privacy protections enjoyed by California residents pursuant to self-regulatory codes such as the Digital Advertising Alliance's (“DAA”) Self-Regulatory Principles for Online Behavioral Advertising by forcing businesses to reidentify data in order to verify a consumer's request.²⁴

To help ensure consumer privacy is appropriately protected by pseudonymized data, the CA AG should clarify that pseudonymized data is not covered within the definition of personal information when the data is governed by the pseudonymized data controls listed in the CCPA (*i.e.*, the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that it is not attributed to an identified or identifiable consumer).²⁵ If such a clarification is not made, we request that the CA AG issue a rule that states that a business need not link pseudonymized data to personally identifiable information (such as a name or email address) to effectuate a consumer request when the company does not maintain any personally identifiable information. To effectuate the request, a consumer should provide only the pseudonymized information that the business maintains through a recognized opt-out tool such as the opt-out provided by the Digital Advertising Alliance. Such a rule would ensure that

²² Cal. Civ. Code § 1798.140(r).

²³ Cal. Civ. Code § 1798.140(s); 140(o).

²⁴ See DAA, *Self-Regulatory Principles for Online Behavioral Advertising* (Jul. 2009), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/seven-principles-07-01-09.pdf.

²⁵ The CA AG has the authority to make this clarification based on CCPA's directive to the CA AG adopt rules to “further the purposes of this title.” Cal. Civ. Code §§ 1798.185(a), (b). Such an interpretation would further the purposes of this title because when pseudonymized data is considered personal information, businesses may need to collect more information from consumers in order to effectuate CCPA requests. The collection of this identifiable information creates privacy concerns including increased risks to personal data and identity theft that did not previously exist.

companies that have made the choice not to link pseudonymized data to personally identifiable data are not forced to do so to comply with the CCPA.²⁶

9. Clarify the “Cure” Requirement for Security Breaches

Under the CCPA, no action for statutory damages may be initiated against a business for an alleged data security failure if the business actually *cures* the noticed data security violation within 30 days.²⁷ The CCPA, however, does not define “cure,” and as a result there is a risk that a strict interpretation of the term would mean that any data that was lost, corrupted, or subject to unauthorized access due to the breach must be retrieved or restored in order to constitute a “cure” of the violation. Such an overly restrictive interpretation of “cure” would be difficult, if not impossible, in many cases to attain and would essentially render moot the law’s cure option.

The CA AG should clarify that the “cure” requirement refers to curing the security procedures and practices that may be found to be deficient under the statute, and the term “cure” does not require that a company retrieve or restore data that may have been lost, corrupted, or subject to unauthorized access where no consumer harm has occurred.²⁸ In cases where demonstrable harm has occurred, “curing” the breach would be to cure the security procedures and practices that may be deficient under the statute and providing a process to reasonably reimburse consumers for any actual loss that a consumer suffered as a direct result of the breach and providing such reimbursement within a reasonable period. Such an interpretation is consistent with the CA AG’s authority to further the purposes of the CCPA, as it would incentivize companies to implement and maintain reasonable security procedures and practices.

II. Key Additional Issues for the California Attorney General to Address

This section identifies key additional issues within the CCPA that would benefit from the CA AG’s clarification.

1. Clarify that Businesses Have Flexibility When Verifying Consumer Requests

Generally speaking, the CCPA affords consumers rights to access, delete, and opt out from the sale of personal information but, despite affording consumers these expansive rights, the CCPA provides little guidance on how businesses should comply with these rights. Specifically, no guidance exists on the steps a business must take when a consumer does not provide enough information to identify the data the business holds about him or her. Currently, the only validated method for confirming consumer identities is dependent on the consumer having an account with the entity to whom the request is directed.²⁹ Under this provision, a request submitted through a password-protected account maintained by the consumer is

²⁶ *Id.*

²⁷ Cal. Civ. Code § 1798.150(b).

²⁸ The CA AG may clarify this issue based on his authority to adopt rules to “further the purposes of [the] title.” Cal. Civ. Code §§ 1798.185(a), (b).

²⁹ Cal. Civ. Code § 1798.185(a)(7).

considered a verifiable consumer request.³⁰ This method of verification, however, may have limited utility for businesses that do not offer consumers the ability to create consumer accounts in the normal course of business. Also, the CCPA does not address the format or level of detail businesses should provide in response to consumer access requests.

The CA AG should clarify how a business should comply with vague or incomplete requests. In particular, we request that the CA AG clarify that: (1) a business may use commercially reasonable methods to verify a consumer request before effectuating an access, opt-out, or deletion request under the law; (2) the process of verifying consumer requests may take many different forms; and (3) businesses may ask consumers for necessary information to ensure the request can be addressed.³¹ Additionally, businesses should be permitted to respond to consumer access requests in any commercially reasonable way, provided the response is complete and given in a consumer-friendly and portable format. The CA AG can make this interpretation pursuant to its specific authority to adopt rules related to verifiable consumer requests as articulated in the CCPA's definition of a "verifiable consumer request."³²

2. Preserve Ad Measurement and Attribution Activities

The CCPA does not create explicit exceptions for ad measurement and attribution activities, which involve the analysis of advertising practices to help refine advertising tactics, mediums, and content so it is more appropriate and enjoyable for consumers. As a result, a consumer potentially could delete data or restrict the sharing of data that would prevent the ability to carry out ad measurement and attribution. Without the ability to use information for these purposes, consumers would view less relevant ads as businesses would have a much more difficult time improving ad content and placement, gauging ad effectiveness, and understanding consumer preferences.

The CA AG should clarify that: (1) personal information strictly used for ad measurement and attribution activities constitute an internal use of personal information exempt from the deletion right under the law; and (2) ad measurement and attribution activities constitute "analytic services"³³ within business purposes exempt from the definition of "sale" under the

³⁰ *Id.*

³¹ The CA AG has authority to issue this clarification with respect to the access and deletion provisions pursuant to Cal. Civ. Code § 1798.185(a)(7), which allows him to establish "rules and procedures... to facilitate a consumer's... ability to obtain information pursuant to Section 1798.130...." The CA AG can use Cal. Civ. Code § 1798.185(a)(4)(B) to interpret the opt-out right, as it allows him to issue regulations "[t]o govern business compliance with a consumer's opt out request." Alternatively, the CA AG can use his general authority to issue rules "as necessary to further the purposes of this title." Cal. Civ. Code §§ 1798.185(a), (b).

³² Cal. Civ. Code § 1798.140(y) ("Verifiable consumer request" means a request that... the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information.")

³³ Cal. Civ. Code §§ 1798.140(d); 140(t).

law.³⁴ This interpretation would allow for internal, analytic uses of data that are contemplated by already existing exemptions to the deletion right and the “sale” definition.

3. Clarify the Scope of the “Publicly Available” Information Exclusion

Publicly available information is excluded from the CCPA’s definition of personal information, but the law is unclear with respect to what constitutes publicly available information.³⁵ In particular, the law states that information is not publicly available unless it is used for the purpose for which it was made available in a government record, even though these records often do not fully identify the purposes for which the information was released.³⁶ Publicly available information is for public use. To say data is not publicly available unless it is used for the purpose for which it was made available in a government record is a departure from the general notion that publicly available information is for public use. It also defies the common sense understanding of the term “public” and is an unintended consequence of the way the publicly available information exemption is currently drafted. The law’s terms should reflect the exclusion as it is typically featured in state and federal privacy statutes throughout the country.

The definition of “publicly available” information should be clarified so that information made available by government disclosures can be used unless the government specifically prohibits a certain use.³⁷

4. Clarify the 12-Month Look-Back Provision

The CCPA imposes a 12-month look-back provision that requires businesses to “[d]isclose and deliver the required information to a consumer... [which] shall cover the 12-month period preceding the business’s receipt of the verifiable consumer request....”³⁸ The law is unclear if this 12-month look-back provision: (1) imposes a 12-month data retention requirement on businesses, even though no specific retention requirement is created by the law; or (2) creates an affirmative requirement for businesses to retain data held as of January 1, 2019, even though the law becomes effective on January 1, 2020 and compliance mechanisms will not be built until the CA AG completes the rulemaking process.

³⁴ The CA AG can clarify that ad measurement and attribution activities are not subject to the opt-out to sale right pursuant to his authority to issue rules “[t]o facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information.” Cal. Civ. Code § 1798.185(a)(4)(A). For the deletion right, the CA AG has authority to interpret this provision pursuant to his general regulatory authority to further the purposes of the CCPA, which already envisions the use of data for similar analytic purposes regardless of a consumer deletion request. Cal. Civ. Code §§ 1798.185(a), (b).

³⁵ Cal. Civ. Code § 1798.140(o)(2).

³⁶ *Id.*

³⁷ The CA AG can clarify this definition under the Attorney General’s authority to adopt rules to update additional categories of personal information and the general authority to adopt rules to further the purposes of the CCPA. Cal. Civ. Code §§ 1798.185(a)(1), (b).

³⁸ Cal. Civ. Code § 1798.130(a)(2).

We request that the CA AG clarify that: (1) there is no data retention requirement; and (2) the 12-month look-back provision takes effect 12 months *after* the CA AG's rulemaking is complete.³⁹ Regarding the data retention request that would clarify that no data retention requirement exists, we ask the AG to clarify this point so that the law does not inadvertently create new rules that require the retention of data, creating new privacy concerns. Regarding the effective timeline for access requests, the CCPA already anticipates that some consumer access requests will not be fulfilled (where requests are “manifestly unfounded” or “excessive”).⁴⁰ As such, it would not be inconsistent for the CA AG to take the position that providing access rights before the implementing regulations interpreting the CCPA are written would be manifestly unfounded, since there is no sufficient clarity on the scope of data involved. Moreover, providing access rights to data before the rules on the scope of data involved or how to verify a consumer request are promulgated creates risks of fraud and privacy violations. As a result, clarifying the 12-month look-back via regulation would further the purposes of the CCPA by minimizing such risks of fraud and privacy violations and increasing the ability of businesses to comply with the CCPA in privacy-conscious and privacy enhancing ways.

5. Limit the CCPA's Unintended Impact on Nonprofit Organizations, Including Charities

The CCPA is unclear if businesses subject to the CCPA must delete or refrain from selling consumers' personal data when such data will be provided to nonprofit organizations, including charities. The CCPA was not intended to impact charities and nonprofits, as the law applies to “for profit” businesses and does not explicitly create rules for nonprofits.⁴¹ Nonprofit activities and charitable giving are reliant on smart, informed data sources. Using data from businesses for charitable purposes is foundational to the operations of legitimate nonprofit organizations. Charities use such data to communicate with donors, potential supporters, and new contacts about vitally important missions that help Californians. Requiring compliance with CCPA rules for businesses that provide data to charities and nonprofits would cripple such entities' ability to access information in order to further their nonprofit missions. The CCPA creates a risk that nonprofits will be able to access few legitimate data resources, which could jeopardize the future growth of charities, their missions, and charitable giving in California.

The CA AG should clarify that consumer personal information maintained by a business strictly to provide such data to nonprofits, including charities, is exempt from the CCPA's deletion and opt-out rules.⁴² This interpretation would further the purposes of the CCPA, which is designed to cover businesses, not nonprofit organizations and charities.

³⁹ As further described in this section, the CA AG may clarify this issue based on his authority to adopt rules to “further the purposes of [the] title.” Cal. Civ. Code §§ 1798.185(a), (b).

⁴⁰ Cal. Civ. Code § 1798.145(g)(3).

⁴¹ Cal. Civ. Code § 1798.140(c).

⁴² As further described in this section, the CA AG may clarify this issue based on his authority to adopt rules to “further the purposes of [the] title.” Cal. Civ. Code §§ 1798.185(a), (b).

6. Preserve the Ability to Provide Expected Marketing Messages to Consumers

The CCPA states that a business or a service provider shall not be required to comply with a consumer's deletion request if: (1) it is necessary for the business or service provider to maintain the consumer's personal information in order to provide a good or service requested by the consumer; or (2) if maintaining such information would be reasonably anticipated within the context of a business's ongoing business relationship with the consumer.⁴³ However, the CCPA is unclear with respect to whether expected marketing messages, such as subscription renewal reminders, are reasonably anticipated and can be provided within the context of a business's ongoing business relationship with the consumer.

We ask the CA AG to clarify that the deletion exception for providing a service requested by the consumer or reasonably anticipated by the consumer can include expected marketing messages (*i.e.* subscription renewal reminders).⁴⁴ Because consumers expect and value these messages from their ongoing commercial activities, including them in the scope of the aforementioned deletion exception would further the purposes of the title by preserving consumer expectations in a specific area that consumers value.

7. Ensure the Viability of the Fraud Exception

The CCPA creates a deletion right and an exception to this right for business activities related to combatting fraud, such as: detecting security incidents; protecting against malicious, deceptive, fraudulent, or illegal activity; and prosecuting those responsible for such activity.⁴⁵ However, the CCPA is unclear as to whether the fraud exception to a consumer's deletion right covers businesses that collect and use data to create anti-fraud products and services. If the exception does not cover these activities, the CCPA could jeopardize the availability of the anti-fraud tools the law already recognizes should be protected. Also, under the CCPA, a consumer may authorize a third party to delete information on the consumer's behalf, which could allow a cottage industry to develop for offering deletion services for anti-fraud databases and other identity verification and fraud detection networks. Some of the areas that could be impacted by an incomplete fraud exception include: anti-terrorism efforts (ensuring people on terrorist watch lists do not have access to financing), anti-money laundering efforts, locating persons of interest in criminal investigations, verification of identities, and officer safety measures, such as the identification of the occupants of an address.

The deletion exception for fraud should be clarified to include the collection and use of personal information to create and sell anti-fraud tools. Such an interpretation by the CA AG would further the purposes of the CCPA by helping businesses access robust tools, products, and

⁴³ Cal. Civ. Code § 1798.105(d)(1).

⁴⁴ As further described in this section, the CA AG may clarify this issue based on his authority to adopt rules to "further the purposes of [the] title." Cal. Civ. Code §§ 1798.185(a), (b).

⁴⁵ Cal. Civ. Code § 1798.105(d)(2).

services for fighting fraud.⁴⁶ These tools, products, and services enhance consumer privacy by allowing businesses to employ reliable efforts to combat fraudulent practices in order to protect consumer identities and personal information.

8. Clarify the Definition of “Business Purpose”

The CCPA definition of “sale” excludes the sharing of personal information with a service provider if such sharing “is necessary to perform a business purpose.”⁴⁷ As a result, a business that shares a consumer’s personal information with a service provider for a business purpose will not constitute a sale of information from which a consumer can opt out. According to the CCPA, a “business purpose” means the use of personal information for the business or a service provider’s operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed, or for another operational purpose that is compatible with the context in which the personal information was collected.⁴⁸ The CCPA also lists seven permissible “business purposes.”⁴⁹ Specifically, the CCPA states, “Business purposes are:” and then lists the seven permissible purposes.⁵⁰ Because the CCPA stated that business purposes “are” instead of business purposes “include,” the CCPA could be read to limit the general definition of “business purpose” to those seven examples, which is too narrow for consumers and businesses alike. For instance, undertaking research for retail store site selection or product placement is a business purpose that should be included in the definition but is not specifically mentioned in the CCPA’s seven enumerated examples of business purposes.

We believe that the CA AG can reasonably conclude that the purposes identified in Section §1798.140(d)(1)-(7) are not exhaustive, and should clarify that the general definition of “business purpose” is still operative and the seven categories are examples rather than the full extent of the definition.⁵¹ Although the purposes are introduced using the term “are” (which may suggest an exhaustive list), the overarching definition of a “business purpose” is functional. Ensuring that the seven categories are examples rather than the full extent of the definition would further the purposes of the title by maintaining the existing narrow, yet flexible, definition of “business purpose” without limiting the definition to the seven examples that are not fully reflective of the definition.

⁴⁶ As further described in this section, the CA AG may clarify this issue based on his authority to adopt rules to “further the purposes of [the] title.” Cal. Civ. Code §§ 1798.185(a), (b).

⁴⁷ Cal. Civ. Code § 1798.140(i)(2)(C).

⁴⁸ Cal. Civ. Code § 1798.140(d).

⁴⁹ Cal. Civ. Code §§ 1798.140(d)(1)-(7).

⁵⁰ *Id.*

⁵¹ The CA AG may clarify this issue based on his authority to adopt rules to “further the purposes of [the] title.” Cal. Civ. Code §§ 1798.185(a), (b). Clarifying the scope of the fraud exception would ensure that data is maintained to combat fraud and any resulting unwanted privacy intrusions.

9. Clarify the Operative Ages in the Opt-In Requirement Related to Minors

As written, the CCPA requires businesses to refrain from selling the personal information of consumers they know to be “less than 16 years of age” without opt-in consent.⁵² The effect of this rule is that businesses must receive opt-in consent to sell the personal information of children aged 15 or younger. However, the law also allows minors aged 16 (not *less* than 16) to consent on their own behalf even though age 16 is beyond the age where opt-in consent is required.”⁵³ As such, the inconsistencies in descriptions of ages create confusion around the ages when opt-in consent is required.

The CA AG should clarify that the rule requiring opt-in consent to sell personal information of children relates to children aged 15 or younger.⁵⁴ This would help educate consumers on their rights and promote compliance with the CCPA by setting forth a definitive rule regarding the age at which opt-in consent is necessary.

10. Remove Backup Information from the Scope of a Deletion Request

The CCPA states that a consumer has the right to request that a business delete any personal information about the consumer which the business has collected from the consumer; however, the law is silent on whether those data requests cover data held in backup storage when the data is not used for other purposes.⁵⁵ Data held in backup storage is kept for a finite period of time and typically only to restore systems in the event of a data failure. As a result, the CA AG should issue a rule exempting data held on backup tapes from the scope of the deletion right under the CCPA.

In particular, we request that the CA AG interpret Section 1798.145(g)(3) of the CCPA (providing exceptions to consumer requests that are excessive or manifestly unfounded) to include requests related to data in backup storage.⁵⁶ If consumers’ deletion requests could reach the data held on backup systems, businesses’ ability to rebound from data failures and technological problems would be severely limited. Removing backup storage data from the scope of the deletion right would further the purposes of the CCPA by continuing to enable businesses to mitigate data loss issues without having to contact the consumer for assistance in restoring necessary information.

⁵² Cal. Civ. Code § 1798.120(c).

⁵³ *Id.*

⁵⁴ As further described in this section, the CA AG may clarify this issue based on his authority to adopt rules to “further the purposes of [the] title.” Cal. Civ. Code §§ 1798.185(a), (b).

⁵⁵ Cal. Civ. Code § 1798.105(a).

⁵⁶ As further described in this section, the CA AG may clarify this issue based on his authority to adopt rules to “further the purposes of [the] title.” Cal. Civ. Code §§ 1798.185(a), (b).

11. Ensure that Businesses Do Not Have to Collect Extra Data to Comply with CCPA Requirements

The CCPA does not explain how a business should comply with a vague consumer request or a request that does not provide sufficient information to locate personal information maintained by the business about the consumer. Accordingly, an overbroad interpretation of the CCPA would mandate that a business collect additional information about a consumer sufficient to locate records maintained by the business. However, the law also states that businesses do not need to “reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.”⁵⁷ As such, there is ambiguity as to whether additional consumer information must be sought by a business to effectuate a consumer request.

The CA AG should clarify that businesses are not required (but may attempt) to collect additional information about a consumer to comply with a vague consumer request or a request that does not provide sufficient information to locate the personal information maintained by the business about the consumer.⁵⁸ This interpretation would further the purposes of the CCPA by refraining from mandating the transfer of additional information by consumers to businesses while simultaneously allowing the business to access the information it needs to comply with a consumer request.

* * *

The ANA appreciates this opportunity to comment on the California Consumer Privacy Act and looks forward to continuing to work with the CA AG on these issues.

Please contact Dan Jaffe, Group Executive Vice President, at [REDACTED] or [REDACTED] with any questions regarding these comments.

⁵⁷ Cal. Civ. Code § 1798.145(i).

⁵⁸ As further described in this section, the CA AG may clarify this issue based on his authority to adopt rules to “further the purposes of [the] title.” Cal. Civ. Code §§ 1798.185(a), (b).

Message

From: Stephen Dwyer [REDACTED]
Sent: 3/7/2019 1:59:52 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Stephen Dwyer [REDACTED]
Subject: Comments re: California Consumer Privacy Act Forthcoming Proposed Regulations
Attachments: ASA CCPA Comments March 2019.pdf

To Whom It May Concern: Attached for your consideration are the American Staffing Association's comments with respect to any forthcoming proposed California Consumer Privacy Act regulations.

Should you have any questions, please do not hesitate to contact me. Thank you.

Stephen C. Dwyer
General Counsel
American Staffing Association
277 S. Washington St., Suite 200
Alexandria, VA 22314-3675



americanstaffing.net

This electronic message contains information that may be legally confidential or privileged or both. The information is intended solely for the individual or entity named above, and access by anyone else is unauthorized. If you are not the intended recipient, any disclosure, copying, distribution, or use of this information is prohibited and may be unlawful. If you have received this electronic message in error, please reply immediately to the sender that you have received the message in error, and delete it.

American Staffing Association

277 South Washington Street, Suite 200 • Alexandria, VA 22314-3675



VIA ELECTRONIC SUBMISSION THROUGH
privacyregulations@doj.ca.gov

703.253.2053 fax

americanstaffing.net

March 7, 2019

California Department of Justice
Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, California 90013

Re: California Consumer Privacy Act Forthcoming Proposed Regulations

To Whom It May Concern:

The American Staffing Association ("ASA") provides these comments in response to the California Attorney General's ("AG") request for input on regulations that will interpret provisions of the California Consumer Privacy Act ("CCPA"). ASA is a national trade association that represents the interests of the staffing, recruiting, and workforce solutions industry across the country. The staffing industry, comprised of more than 20,000 firms and nearly 15 million employees, contributes \$150 billion to the U.S. economy through temporary and contract staffing, recruiting and permanent placement, outsourcing and outplacement, and human resource consulting.¹ Our members' impact in California is substantial. In 2017, ASA-member staffing companies placed over 2.6 million Californians in jobs in a wide variety of industries.²

ASA members place workers in temporary and contract jobs and help businesses fulfill their workforce needs. A natural component of our members' work requires them to share individuals' personal information with businesses so they may be considered for job opportunities. The CCPA's broad applicability threatens our members' business model and the staffing industry as a whole. Although the CCPA was enacted to empower consumers, it fails to cabin its effects to individuals engaged in consumer transactions. As written, the CCPA's definition of "consumer" broadly includes any California resident, no matter the context in which the resident is acting.³ However, the interactions between job candidates, who are looking for employment to support themselves and their families, and staffing firms, whose purpose is to put people to work, are not consumer-business transactions. Individuals do not pay staffing firms for finding and placing them in jobs, so staffing firms process individuals' information in the employment, rather than the consumer, context.

We therefore ask the AG to issue a rule clarifying that job applicants, candidates, and employees do not constitute "consumers" under the CCPA, as further described in Section I below. Without this clarification, workers will be adversely affected and, as described in Section II, a number of other provisions in the CCPA will also require clarification.

I. Clarify that Job Applicants, Candidates, and Employees are Not Consumers Under the CCPA

¹ ASA, *Introduction: A Vital Workforce That Supports the Economy*, available at <https://americanstaffing.net/staffing-industry/workforce-solutions/>.

² ASA, *Fact Sheet: Staffing Firms Employed 2,613,500 Workers in California*, available at <https://d2m21dzi54s7kp.cloudfront.net/wp-content/uploads/2018/06/ASA-2018StateFactSheets-CA.pdf>.

³ See Cal. Civ. Code § 1798.140(g).

We ask the AG to clarify that job applicants, candidates, and employees are not “consumers” subject to the CCPA (hereinafter the “Proposed Clarification”). The CCPA broadly defines “consumer” as “a natural person who is a California resident... however identified, including by any unique identifier.”⁴ Nowhere in the law does it state that it only applies to information collected in the course of a consumer transaction or explicitly exclude information collected for employment purposes, and thus the broad definition could be construed to apply to job applicants, candidates, and employees (in possible contravention of legislative intent).

The definition of “consumer” does not account for the fact that certain exchanges of personal information take place wholly outside of the consumer context. The common understanding of a “consumer” is an individual who buys goods or services. In the staffing industry, job applicants, candidates, and employees do not pay the staffing firm to be placed in jobs. The CCPA’s purpose is to give rights to consumers, protect their personal information, and prevent it from being shared or sold without notice and an opportunity to exercise choice. These purposes center on consumer transactions; they seek to prohibit businesses’ use of consumers’ information in ways that are outside the realm of their expectations and authorizations.

In the staffing context, individuals provide their personal information to firms with the desire and expectation that such firms will share their personal information with businesses for job opportunities. The information our members process and share pertains to individuals in their employment capacities. Interpreting the CCPA to apply to all California residents, regardless of their purpose for providing information or their role as a non-consumer, would frustrate job-seekers’ desires and expectations. A rule stating that the CCPA does not apply to job applicants, candidates, and employees would therefore further the purposes of the CCPA by more clearly focusing its effects on consumer transactions and information.

ASA therefore urges the AG to issue the Proposed Clarification. The AG is authorized to issue such a rule pursuant to his authority to promulgate regulations “to further the purposes of [the CCPA.]”⁵ Without the Proposed Clarification, the staffing industry would be faced with a significant compliance burden that would impede the industry’s ability to place people in jobs. In brief, it would be bad for job growth and for Californians looking for job opportunities.

II. Without the Proposed Clarification, Various Other Clarifying Regulations Will Be Necessary

A number of provisions in the CCPA will need to be addressed if the Proposed Clarification is not issued. The following list sets forth CCPA interpretations ASA requests the AG to promulgate if he does not make the Proposed Clarification described in Section I above:

- *Clarify that the exception to “sale” under Section 1798.140(t)(2)(A) applies to the staffing industry.* Although the definition of “sale” is broadly defined as “making available” a consumer’s personal information, the CCPA exempts from the definition any sharing of personal information when “[a] consumer uses or directs the business to intentionally disclose personal information... to a third party... provided the third party does not also sell the personal information...”⁶ If the AG does not issue the Proposed Clarification, we ask the AG to clearly state that this exemption applies when job-seekers share their personal information with staffing firms for the purpose of being placed in jobs. This exemption fits the staffing context, because job candidates use and expect staffing firms to disclose information to potential third-party employers, who do not further sell applicants’

⁴ *Id.*

⁵ Cal. Civ. Code §§ 1798.185(a), (b).

⁶ Cal. Civ. Code §§ 1798.140(t)(1), (2)(A).

personal information. Interpreting “sale” so staffing firms fall within the exception to the definition would confirm that our industry can continue to share information with employers in order to help Californians find jobs and fulfill businesses’ workforce needs.

- *Clarify that staffing firms need not characterize their sharing of information as a “sale.”* The CCPA requires covered businesses to notify individuals of the “sale” of their information and provide a “clear and conspicuous link” consumers can click titled “Do Not Sell My Personal Information.”⁷ However, ASA members’ sharing of individuals’ personal information for employment purposes does not constitute a “sale”. Requiring such a disclosure could therefore confuse candidates who may want to take advantage of staffing industry services, and could unnecessarily dissuade them from doing so, thus impacting job opportunities. We therefore ask the AG to clarify that staffing firms must only disclose that they share information with potential employers to further the individual’s job prospects and need not use the term “sale” when making such disclosures.
- *Clarify the applicability of the CCPA’s non-discrimination provision to the staffing industry.* The CCPA prohibits businesses from “imposing penalties” or providing a different level of quality of services to Californians who exercise their CCPA rights.⁸ We ask the AG to clarify that a staffing firm that refrains from providing services to a Californian who asks to delete or opt out of the sharing of personal information is not instituting a “penalty” or imposing a different level of services on the consumer. Staffing firms simply cannot provide their services if they are prohibited from sharing personal information with businesses for employment purposes. We also ask the AG to issue a rule stating that wages or compensation paid to a worker by a staffing firm does not constitute a “financial incentive program” that the staffing firm must allow the worker to revoke at any time.⁹
- *Clarify the requirement to make consumer disclosures “at or before the point of collection.”* The CCPA requires businesses to notify consumers of the categories of personal information to be collected and the purposes for which such information shall be used “at or before the point of collection.”¹⁰ This requirement poses significant challenges for the staffing industry, as staffing firms routinely collect information regarding job candidates from public sources such as LinkedIn. These individuals have voluntarily made such information public by publishing it online or disseminating it in some other publicly available form, and requiring privacy notices to be issued every time staffing firms collect information from these sources would only serve to overwhelm and confuse job seekers. The CCPA’s definition of “publicly available,” however, is narrow and limited to government disclosures of information,¹¹ and thus does not address the sourcing of prospective employee information from public sources. Therefore, we ask the AG to clarify that staffing firms can satisfy this requirement by making a privacy policy generally available.

The Proposed Clarification would adequately address all of the issues raised in this Section II so that the staffing industry can continue to provide its beneficial services to California’s workers and California

⁷ Cal. Civ. Code §§ 1798.110, 115, 135.

⁸ Cal. Civ. Code § 1798.125(a)(1).

⁹ Cal. Civ. Code § 1798.125(b)(3).

¹⁰ Cal. Civ. Code § 1798.100(b).

¹¹ Cal. Civ. Code § 1798.140(o)(2).

American Staffing Association

March 7, 2019

Page 4

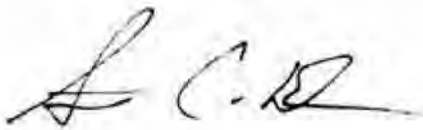
businesses. However, without the Proposed Clarification, a number of terms in the CCPA will have a significant negative impact on individuals who use staffing firms to find jobs. The Proposed Clarification constitutes a blanket fix that would ensure that job applicants, candidates, and employees are not subject to the CCPA, which, as noted above, was intended to apply to personal information collected from consumers in their consumer capacities.

We therefore ask the AG to issue the Proposed Clarification, and if not, the clarifications set forth in this Section II so that staffing firms can continue to find and place Californians in jobs.

Thank you for your consideration.

Very truly yours,

AMERICAN STAFFING ASSOCIATION

A handwritten signature in black ink, appearing to read "S. C. Dwyer", written in a cursive style.

Stephen C. Dwyer
General Counsel

Message

From: Brett Chamberlin [REDACTED]
Sent: 3/8/2019 3:01:29 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments re: CCPA
Attachments: The Story of Stuff Project – Public Comment re_ CCPA.pdf

To whom it may concern,

I am writing today to submit comments with regard to the California Consumer Privacy act of 2018. Please find my comments attached as a PDF, and, for your convenience, included inline below.

Thank you,
Brett Chamberlin

To whom it may concern,

I am writing today on behalf of the nonprofit Story of Stuff Project to submit comments regarding the California Consumer Privacy Act of 2018 (CCPA). Our interest in this law relates to a service called Catalog Choice which is operated by our organization.

Catalog Choice (www.catalogchoice.org) is a free-to-use, web-based service which allows individuals to reduce their volume of unwanted catalogs and other forms of junk mail by submitting "opt-out" requests to direct mail marketers. Catalog Choice has over 2.2 million registered accounts and has processed over 31 million opt-out requests since its launch in 2007. According to calculations made with the Environmental Paper Calculator, these opt-outs represent a diversion of over 200,000 tons of paper waste by preventing the printing, distribution, and disposal of unwanted paper mail. We estimate that 275,000 of these accounts and 3.7 million of these opt-outs are associated with California residents. Catalog Choice is the only free service of its kind.

Functionally, Catalog Choice is comprised of a database of nearly 9,000 direct mail marketers including retailers, credit card providers, nonprofits, and other entities ("merchants"). Catalog Choice allows individuals to search our database for a merchant from whom they are receiving unwanted mail; users are then provided with steps to submit their opt-out request. In some cases, users are redirected to the relevant web form on the company's website or provided with the appropriate phone number for that company. In other cases, users are able to complete their opt-out request on the Catalog Choice website by entering their name and address onto a form on the site; that information is then used to generate an opt-out request which is delivered to the company by the method of the company's choosing. In some cases, this means that a user's opt-out request is delivered to an email address designated by the merchant; in other cases, the merchant can access and download a file of opt-outs on a periodic basis.

From the perspective of an individual user, Catalog Choice makes it significantly faster and easier to opt out of unwanted mail from our central platform by obviating the need to comb through companies' websites and privacy policies. We frequently receive positive feedback from Catalog Choice users who appreciate the ease and effectiveness of the site, which has helped them save time, reduce clutter, and divert waste by putting a stop to unwanted junk mail. The most touching messages have come from individuals who have used our service to stop a flood of fraudulent and malicious offers targeting elderly parents, or to stop mail addressed to a deceased loved one.

From the perspectives of direct mail marketers who are listed on our site, there is functionally no difference between opt-outs submitted via Catalog Choice and opt-outs submitted directly to the merchant via web form or email. Whether an individual uses their personal email to submit an opt-out request directly to a company or uses Catalog Choice to generate an opt-out request that is delivered to the merchant, the effect is the same. In fact, some merchants have expressed that they prefer receiving opt-outs via Catalog Choice because our standardized format for opt-out requests reduces the staff

time required to compile and process those requests. All the same, when merchants do ask to be removed from our directory, that request is honored – though in over two years of managing the program, fewer than a dozen merchants have requested removal while many more have been enrolled.

The greatest challenge for Catalog Choice is maintaining merchant compliance with opt-out requests. Although the majority of merchants included in our database are happy participants in the program, some bad actors seem to wish to make it as difficult as possible for individuals to opt out of direct mail marketing and the sharing of their personal information. In some cases, there is no publicly listed method for an individual to opt out of such programs, and requests submitted via Catalog Choice are simply ignored.

It is our hope that rules developed under CCPA will assert individuals' rights to opt out of unwanted direct mail marketing and information sharing; and to protect Catalog Choice's efforts to help individuals exercise that right. In so doing, the state of California will be helping residents protect their privacy, avoid fraud, reduce waste, and preserve natural resources.

I would be happy to answer any follow-up questions or to provide further information about Catalog Choice, its function, impact, and relationships with our users and merchants. I can be contacted at [REDACTED] by email at [REDACTED].

--

Brett Chamberlin
Community Engagement Manager
The Story of Stuff Project
www.storyofstuff.org
[REDACTED]

Join the conversation: [Facebook](#) | [Twitter](#) | [Pinterest](#) | [Instagram](#)

The Story of Stuff Project
1442 A Walnut St.
Berkeley, CA 94709

March 8, 2018

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

To whom it may concern,

I am writing today on behalf of the nonprofit Story of Stuff Project to submit comments regarding the California Consumer Privacy Act of 2018 (CCPA). Our interest in this law relates to a service called Catalog Choice which is operated by our organization.

Catalog Choice (www.catalogchoice.org) is a free-to-use, web-based service which allows individuals to reduce their volume of unwanted catalogs and other forms of junk mail by submitting "opt-out" requests to direct mail marketers. Catalog Choice has over 2.2 million registered accounts and has processed over 31 million opt-out requests since its launch in 2007. According to calculations made with the Environmental Paper Calculator, these opt-outs represent a diversion of over 200,000 tons of paper waste by preventing the printing, distribution, and disposal of unwanted paper mail. We estimate that 275,000 of these accounts and 3.7 million of these opt-outs are associated with California residents. Catalog Choice is the only free service of its kind.

Functionally, Catalog Choice is comprised of a database of nearly 9,000 direct mail marketers including retailers, credit card providers, nonprofits, and other entities ("merchants"). Catalog Choice allows individuals to search our database for a merchant from whom they are receiving unwanted mail; users are then provided with steps to submit their opt-out request. In some cases, users are redirected to the relevant web form on the company's website or provided with the appropriate phone number for that company. In other cases, users are able to complete their opt-out request on the Catalog Choice website by entering their name and address onto a form on the site; that information is then used to generate an opt-out request which is delivered to the company by the method of the company's choosing. In some cases, this means that a user's opt-out request is delivered to an email address designated by the merchant; in other cases, the merchant can access and download a file of opt-outs on a periodic basis.

From the perspective of an individual user, Catalog Choice makes it significantly faster and easier to opt out of unwanted mail from our central platform by obviating the need to comb through companies' websites and privacy policies. We frequently receive positive feedback from Catalog Choice users who appreciate the ease and effectiveness of the site, which has helped them save time, reduce clutter, and divert waste by putting a stop to unwanted junk mail. The most touching messages have come from individuals who have used our service to stop a flood of fraudulent and malicious offers targeting elderly parents, or to stop mail addressed to a deceased loved one.

From the perspectives of direct mail marketers who are listed on our site, there is functionally no difference between opt-outs submitted via Catalog Choice and opt-outs submitted directly to the merchant via web form or email. Whether an individual uses their personal email to submit an opt-out request directly to a company or uses Catalog Choice to generate an opt-out request that is delivered to the merchant, the effect is the same. In fact, some merchants have expressed that they prefer receiving opt-outs via Catalog Choice because our standardized format for opt-out requests reduces the staff time required to compile and process those requests. All the same, when merchants do ask to be removed from our directory, that request is honored – though in over two years of managing the program, fewer than a dozen merchants have requested removal while many more have been enrolled.

The greatest challenge for Catalog Choice is maintaining merchant compliance with opt-out requests. Although the majority of merchants included in our database are happy participants in the program, some bad actors seem to wish to make it as difficult as possible for individuals to opt out of direct mail marketing and the sharing of their personal information. In some cases, there is no publicly listed method for an individual to opt out of such programs, and requests submitted via Catalog Choice are simply ignored.

It is our hope that rules developed under CCPA will assert individuals' rights to opt out of unwanted direct mail marketing and information sharing; and to protect Catalog Choice's efforts to help individuals exercise that right. In so doing, the state of California will be helping residents protect their privacy, avoid fraud, reduce waste, and preserve natural resources.

I would be happy to answer any follow-up questions or to provide further information about Catalog Choice, its function, impact, and relationships with our users and merchants. I can be contacted at [REDACTED] by email at [REDACTED].

Sincerely,

Brett Chamberlin
Catalog Choice Program Manager
The Story of Stuff Project

Message

From: Andrew Madden [REDACTED]
Sent: 3/8/2019 3:55:03 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments re: CCPA
Attachments: ACA CCPA Comments 3-5-19.docx

Please accept these comments from ACA International.



Andy Madden, VP, Government & State Affairs
ACA International, 509 2nd Street, N.E., Washington, DC 20002



Helping Members Succeed!



March 8, 2019

VIA ELECTRONIC DELIVERY TO PRIVACYREGULATIONS@DOJ.CA.GOV

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.,
Los Angeles, CA 90013

Dear Sir/Madam:

ACA International ("ACA"), the Association of Credit and Collection Professionals, submits these comments in response to the Attorney General's notice of preliminary rulemaking activity and series of public forums on the California Consumer Privacy Act (CCPA).

I. BACKGROUND ON ACA INTERNATIONAL

ACA International (ACA) is the leading trade association for credit and collection professionals. Founded in 1939, and with offices in Washington, D.C. and Minneapolis, Minnesota, ACA represents approximately 2,500 members, including credit grantors, third-party collection agencies, asset buyers, attorneys, and vendor affiliates in an industry that employs more than 230,000 employees worldwide including and over 20,000 in California. Given its longstanding history and broad membership, ACA is uniquely positioned to comment on the California Consumer Privacy Act of 2018.

ACA members include the smallest of businesses that operate within a limited geographic range of a single state, and the largest of publicly held, multinational corporations that operate in every state. The majority of ACA member companies, however, are small businesses. According to a recent survey, 44 percent of ACA member organizations (831 companies) have fewer than nine employees. Additionally, 85 percent of members (1,624 companies) have 49 or fewer employees and 93 percent of members (1,784) have 99 or fewer employees. Even though a majority of our members are small businesses, it is unclear how many of them will be impacted by the thresholds set forth in the CCPA given the diverse clients they serve.

MINNEAPOLIS OFFICE
4040 WEST 70TH STREET 55435
P.O. BOX 390106, MINNEAPOLIS, MN 55439-0106
FAX (952) 926-1624

WASHINGTON OFFICE
800 2ND STREET NE, WASHINGTON, D.C. 20002
FAX (202) 547-2671

As part of the process of attempting to recover outstanding payments, ACA members are an extension of every community's businesses ACA members work with these businesses, large and small, to obtain payment for the goods and services already received by consumers. In years past, the combined effort of ACA members has resulted in the annual recovery of billions of dollars for the economy. This savings is returned to and reinvested by businesses. This allows small businesses and large employers to limit losses on the financial statements of those businesses. Without an effective collection process, the economic viability of these businesses and, by extension, the American and California economy is threatened. Recovering rightfully-owed consumer debt enables organizations to survive, helps prevent job losses, keeps credit, goods, and services available, and reduces the need for tax increases to cover governmental budget shortfalls. Importantly, ACA members are committed to fair, reasonable, and respectful practices and take their obligations in collecting debt and protecting consumers privacy very seriously. As legitimate credit and collection professionals, ACA members play a key role in helping consumers fulfill their financial goals and responsibilities while facilitating broad access to the credit market.

II. COMMENTS OF ACA INTERNATIONAL

The CCPA is a robust state law, which many members of the accounts receivables management industry have argued is overly complex and burdensome. Notably, it also touches many businesses outside of California if personal information of California consumers is collected making its reach potentially much more than California collection agencies. ACA members have testified at hearings in San Francisco, San Diego, Inland Empire/Riverside, Los Angeles, Sacramento, Fresno, and Stanford discussing the law across California and submitted comments outlining industry concerns. We appreciate your consideration of this important input from our members.

ACA members strongly support the overarching goal of the CCPA of protecting the privacy of consumers and their data. However, as the Attorney General moves forward in implementing the CCPA, it is critical to ensure legitimate businesses are provided crystal clear guidelines and not faced with insurmountable regulatory burdens.

It is currently unclear how the CCPA will be harmonized with federal laws like HIPAA, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, Gramm Leach Bliley Act, and the Family Educational Rights and Privacy Act of 1974. Furthermore, the General Data Protection Regulation went into effect in the European Union in May 2018 and impacts certain ACA members in the U.S., as well as international accounts receivable management agencies.

The accounts receivable industry does not collect consumers' information for any purposes other than those permitted by privacy and consumer financial protection laws. However, because of the breadth of the law and the lack of clarity surrounding exemptions certain practices of the accounts receivables management could be swept under the law. We are seeking further clarity on questions such as how skip-tracing may be impacted. Additionally, as outlined below there are several areas where the CCPA has overly broad

definitions or requirements that may conflict with other requirements such as the Fair Debt Collections Practices Act (FDCPA).

III. AREAS OF CONCERN

Safe harbor language

The industry is already very restricted in what information and how information can be communicated to consumers under the FDCPA. This raises issues when communicating with consumers that have requested access to all personal information a business has collected within 45 days. The industry requests that a standardized format of communications and safe harbor language be provided to allow a safe and compliant way for the industry to communicate with these consumers.

Clarification on the definition of a consumer

Under the CCPA, "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations." This definition of consumer is broader in scope than the traditional definition of consumer and would likely include employees of a business as well as the actual consumers a business serves.

High risk of third-party disclosure

The CCPA contains no guidance regarding information requests businesses receive from an agent of the consumer. This puts members of the accounts receivables management industry in a high-risk situation for third party disclosure. The debt collection industry cannot disclose to a third party the existence of a debt. Without clear guidance on how handle requests from a third-party agent such as an attorney, spouse or guardian the industry is at risk.

Clarification regarding email delivery

ACA request additional clarification regarding email verifications sent to consumers. The CCPA provides that a business can deliver information to consumers "in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option."

The industry appreciates the option for electronic or email and would like to embrace this option however there are concerns regarding third party disclosure issues that must be addressed through further guidance.

The accounts receivable industry is required to protect consumers against unintentionally sharing their information or the fact that they have a debt with a third party. Sending information to a consumer through email creates the risk that a consumer could provide an employer's email account or a joint email account which would subject the information to third-party disclosures.

What is the impact of the private right of action provision?

The CCPA would "provide for its enforcement by the Attorney General, as specified, and would provide a private right of action in connection with certain unauthorized access and exfiltration, theft, or disclosure of a consumer's nonencrypted or nonredacted personal

information, as defined. The bill would prescribe a method for distribution of proceeds of Attorney General actions.... The bill would authorize a business, service provider, or 3rd party to seek the Attorney General's opinion on how to comply with its provisions. The bill would void a waiver of a consumer's rights under its provisions. The bill would condition its operation on the withdrawal of a specified initiative from the ballot."

What is the statute of limitation on bringing a private right of action? How will this affect the rules of civil procedure when filing with a court?

ACA appreciates the opportunity to provide comments.

Submitted by:



Andrew Madden
Vice President of Government and State Affairs
ACA International



Message

From: Alan Chapell [REDACTED]
Sent: 3/7/2019 2:25:48 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments RE: Implementing Regulations for the California Consumer Privacy Act of 2018
Attachments: Chapell CCPA comments to Xavier Becerra.pdf

Good Afternoon – Thanks for the opportunity. Please see attached.

Cheers,

Alan Chapell

Chapell & Associates

[REDACTED]

March 7, 2019

The Honorable Xavier Becerra
Attorney General
CA Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

RE: Implementing Regulations for the California Consumer Privacy Act of 2018

Dear Mr. Becerra:

My name is Alan Chapell. I am an attorney licensed in New York and certified as an information privacy professional by the International Association for Privacy Professionals. I have a legal consulting practice that works primarily with advertising technology and marketing technology platforms. I am pleased to offer the following commentary in response to the Department of Justice's request for comments regarding implementing regulations it may promulgate under the California Consumer Privacy Act of 2018 ("CCPA").

I believe that it will be difficult for adtech and martech businesses to implement the CCPA without additional clarification. These implementation challenges are particularly noteworthy given the push towards ensuring a private right of action and/or local government enforcement under CCPA.

Please clarify the definitions of third party and service provider

First, it is unclear whether adtech companies are considered "third-parties" or "service providers" under CCPA. This distinction is particularly important given that transfers of data to third parties and businesses are considered a "sale" under CCPA and therefore subject to notice and choice requirements. (Specifically, CCPA requires notice and choice each time data is transferred. Section 1798.100 stipulates that the notice provided must be "at or before the point of collection.") If adtech companies adopt a conservative view and assume they are third-parties, that means that a separate notice and choice must be offered each time data is transferred. The nature of digital ad serving typically involves multiple entities. So in the context of a single digital ad being served on a single web page; when a website publisher transfers data to an ad exchange, notice and choice must be provided. And when the ad exchange transfer data to an ad server or demand side platform, a separate notice and choice must be provided. And when the demand side platform transfers data to an ad verification partner, an additional notice and choice is required. And when the demand side platform transfers data to a data management platform – an additional notice and choice is required. So a single ad in this example would necessitate the provision of notice and choice four separate times. And if that publisher has more than one ad appearing on that page, notice and choice would need to be provided for each ad under CCPA. As such, the act of visiting a single ad supported newspaper website would require multiple notice and choice instances each time a web page is refreshed. It would be difficult to imagine how California consumers will respond to being inundated with such requests.

I believe there are a few clarifications which may address this issue: 1) clarify when an entity is a service provider versus a third-party; 2) clarify what constitutes a “business purpose” under CCPA; and 3) clarify that sales of data conducted in near-real time would only necessitate the provision of a single notice and choice.

Please Clarify the Do Not Sell My Data Button Requirements

The digital media space would benefit with some clarification regarding the choice requirements. The CCPA requires businesses to post a Do Not Sell My Data button on their websites. I think I understand the intent here, but without clarification this Do not Sell button will be difficult to implement in part because those requirements as currently worded are at odds with the way the digital media marketplace operates.

By way of background - ad targeting opt-outs in digital media are set at the vendor level, not the advertiser or publisher level. Conversely, the opt-out requirements under CCPA are imposed upon the entity “selling” the data, and that might be an adtech vendor when not working as a service provider. But it would just as commonly be a business under CCPA – in this context, an advertiser or publisher.

So, if CCPA requires that the Do Not Sell button must be placed by the business that might “sell” the data, that business would presumably need to scope their opt-out to cover all of their possible data transfers across multiple third-party partners. That approach is practical when dealing with personal information such as an email or postal addresses. However, the unique nature of the way ads are served, the multiple entities involved and the use of pseudonymous identifiers such as cookie IDs may make this process difficult to manage under CCPA.

Therefore, I’m asking the AG’s office to clarify how a Do Not Sell Button would work in practice. It doesn’t seem reasonable for the Do Not Sell functionality to stop all data collection with the press of a single button. Rather, I think the intent under CCPA is for the Do Not Sell Button to take the data subject to a page that enables her or him to exercise the myriad choices available from that business. To that end, in the context of transfers for digital advertising, it would be helpful to clarify whether taking the data subject to a page that includes a link to the industry opt-outs offered by the Network Advertising Initiative (“NAI”) and Digital Advertising Alliance (“DAA”) are sufficient. Similarly, it would be helpful if the AG’s office created a safe harbor so that third parties operating in accordance with the NAI or DAA would obtain the presumption they are in compliance with the CCPA’s choice requirements.

Clarify what a “verifiable” access or deletion request is in the context of pseudonymous data.

My third point pertains to data subject access and deletion requests under CCPA. It would be helpful to have some guidance around what it means to be a “verifiable” access or deletion request. This is particularly important for businesses and third-parties that may process only pseudonymous personal information. For example, what are the steps that a business or third-party may take to verify a request? Are there types of requests that a business or third-party are allowed to ask for additional information in order to ascertain the validity of a request? What about a business or third-party that is unable to verify whether pseudonymous personal information is owned or controlled by the person making the request? I believe there are risks to providing personal information to data subjects when there is no way to verify their identity. It’s probably worth noting

that representatives from the group “Californians for Consumer Privacy” appear to be aligned with industry on this point based upon the comments at the March hearing at Stanford Law School.

Please consider pushing back the enforcement date of the CCPA

At the March hearing at Stanford Law School, representatives from the CA Department of Justice noted that they may not have a first draft of implementation guidance until fall of 2019. Given that the implementation guidance may significantly impact how businesses need to comply with the CCPA, businesses will need at least a year to build out our compliance programs. I’d respectfully request that the enforcement date for CCPA be pushed to one year after publication of final guidance from the CA Department of Justice.

Thank you for the opportunity to share my views.

A handwritten signature in black ink, appearing to read "Alan Chapell". The signature is fluid and cursive, with the first name "Alan" and last name "Chapell" clearly distinguishable.

Alan Chapell

Message

From: Tracy Rosenberg [REDACTED]
Sent: 12/27/2018 2:55:41 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments/Recommendations on CCPA Implementation
Attachments: Media Alliance Comments on CCPA Pay For Privacy Regulation.pdf
Flag: Follow up

Greetings,

Please find enclosed organizational comments on CCPA's financial incentives portion.

Thank you.

Respectfully,

Tracy Rosenberg
Media Alliance

--
Tracy Rosenberg
Executive Director
Media Alliance
2830 20th Street Suite 102
San Francisco, CA 94110
www.media-alliance.org

[REDACTED]
[REDACTED]
Text via Signal

MEDIA ALLIANCE

December 27, 2018

California Department of Justice
Attn: Privacy Regulations Coordinator
300 South Spring Street
Los Angeles CA 90013

Re: Implementation of California Consumer Privacy Act of 2018

The regulatory framework for the 2020 implementation of the California Consumer Privacy Act of 2018 is a significant task for the CAL-DOJ. Since no other state has passed as ambitious and comprehensive a consumer privacy framework as California's CCPA, the DOJ must flesh out an innovative and expansive protocol to implement this law, while grappling with some inconsistencies in the existing text related to the speedy approval process in the CA Legislature and a raft of competing interests. We do not envy your task.

Our comments today are narrowly focused on the pay for privacy implications¹ of the law's current text and the implementation choices that the CAL-DOJ must make. We will discuss some potential problems and concerns and then provide some recommendations for what we believe to be the best possible protocol within the constraints of the current legislative language. Nothing stated here is intended to forestall modifications/improvements to the existing language via the Sacramento legislative process in 2019. To whatever extent the DOJ finds the issues raised here compelling, we would hope for your institutional support for some consumer-protective additions.

Media Alliance is working in partnership with numerous other privacy advocates on the implementation of CCPA. We believe our comments here are consistent with the views of many other privacy groups at least in the broad scope of our concerns, but these recommendations are solely those of our particular organization and should not be taken as a summary of the views of any other privacy advocacy organization.

Media Alliance is a Bay Area democratic communications advocate. Our members include professional and citizen journalists and community-based media and communications professionals who work with the media and on various digital platforms powered by the Internet. As an organization, we particularly focus our advocacy on communications by and for marginalized communities and alternative points of view, with an understanding of how resource inequities affect the nature of the public dialogue on an ongoing basis and the challenges faced by consumers of limited or inadequate means.

1

1 <https://www.akingump.com/en/news-insights/california-passes-landmark-consumer-privacy-act-what-it-means.html>

While the much-publicized “privacy problems” of the past few years including Cambridge Analytica² and Equifax³, have had broad impacts on all consumers, there is no doubt consumers of limited means often get the double whammy of the most impact and the least ability to mitigate those impacts through services like credit monitoring, attorneys and the court system, and online assistance in the form of software fixes and jargon-filled guides.⁴ Among others, SUNY-Albany professor Virginia Eubanks has written extensively on how privacy abuses manifest in very different ways for lower-income and higher-income people in *Automating Inequality* and *Digital Dead End*.

One of our critiques of CCPA in its current form is that given the origin of much of the language in a ballot initiative developed by a wealthy real estate developer, the finished language of the bill is not always as attuned as it could be to the specific privacy challenges faced by lower-income communities. It is understandable that such issues may not have been front and center in the ballot initiative's drafting. But at this juncture, it is your task, and one that we hope you embrace, to craft a regulatory structure that makes the law operational and functional for all Californians, including those of limited financial means.

Using this lens, we turn to the existing pay for privacy language in the current text of CCPA, namely section 1798.125, reproduced below for convenient access. We also cite section 1798.185 Sections 4(A) and 4(B) and 7 to indicate that the recommendations contained herein are firmly within the DOJ mandate.

1798.125.⁵

(a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer's rights under this title.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data.

² <https://www.theguardian.com/uk-news/2018/dec/23/cambridge-analytica-facebook-scoop-carole-cadwalladr-shocked-world-truth-still-elusive>

³ <https://www.nbcnews.com/news/us-news/equifax-breaks-down-just-how-bad-last-year-s-data-n872496>

⁴ https://motherboard.vice.com/en_us/article/ypwe9x/why-mass-surveillance-is-worse-for-poor-people

⁵ https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375

- (b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data.*
- (2) A business that offers any financial incentives pursuant to subdivision (a), shall notify consumers of the financial incentives pursuant to Section 1798.135.*
- (3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.135 which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.*
- (4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.*

In turning to this language, we want to address practical imports. The text in the California Consumer Privacy Act is clear in the intention to prevent consumers from being discriminated against for choosing to opt out of sales of their data, including facing pricing differentials that are in any way coercive, unreasonable or unjust. We believe this language reflects the intent of the Legislature,⁶ which recognizes that it is problematic to establish a right, and then allow that right to become overly burdensome or difficult to execute.

Out of a seeming concern for business models which rely on the sale of customer data for a significant amount of their income stream, the language then provides a pay for privacy clause. The clause permits consumers who choose to opt out to be given a different price or rate or to be denied a discount because of their choice to opt out, as long as the discrimination is reasonably related to the value of their data.

As has been discussed, CCPA's current language states the criteria as "reasonably related to the value provided to the consumer by the consumer's data". This is a confusing phrase, at best, since consumers will have different interpretations of the value of their data. Additionally, that value will differ depending on the nature of the data collected (i.e. my email address and the fact that I like suede boots is probably of less value to me than facts about my medical status, my home address or the state of my finances). Even using the interpretation that the phrase refers to the value of the customer's data **to the business** (i.e. how much it can be sold for to other parties), the phrase leads to an inconsistent standard as the market value for data is likely connected to the nature of the specific data collected. This leaves "reasonableness" with a not clearly quantifiable number across different business models and transactions. Privacy conscious consumers would not be entirely cognizant of the potential expenses of utilizing the opt out, even if companies follow the regulations scrupulously. We are not entirely convinced that the average consumer has an intricate enough knowledge of the ins and outs of the data sale marketplace to assess if a business is correctly quoting the value of their data⁷ or going for as much as they think they can get without a complaint being filed for unreasonableness.

⁶ https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375

⁷ <https://medium.com/wibson/how-much-is-your-data-worth-at-least-240-per-year-likely-much-more-984e250c2ffa>

Also relevant is the simple reality that California has the highest cost of living in the United States. Many Californians are financially struggling with preposterously high rents and/or mortgages and crushing student loan debt.⁸ Workers trapped in lower-wage jobs in retail and service industries suffer from housing instability and those on fixed incomes can barely pay their bills. Even working adults with well-paying jobs are often living paycheck to paycheck.

This does not, in any way, mean that financially struggling Californians are not concerned about what companies are doing with their data. Every poll shows that a large majority are very concerned about the uses of their data and feel a lack of control about where it ends up.⁹ But the impact it has in a practical sense, is to apply a cap to the number of times that many California residents are going to be able or willing to reimburse a company for the value of their data in order to avoid having it sold on the open market.

There is no doubt that consumers will vary greatly in the amount and nature of data-driven transactions they participate in and that would be subject to CCPA. Some engage in frequent online transactions, some do not. Some make efforts to use small local businesses as much as possible, others are frequent customers of huge national and international companies.

But one thing is certain. The vast majority of consumers engage in numerous transactions every year that are likely subject to CCPA: their ISP, their wireless provider, various social media platforms, and several service providers and retail outlets every year. The opt-out and pay the company for your privacy choice will be in front of California consumers over and over again.

A modest fee of \$5/year for your data, or \$10/year, or \$20/year, all fees that most people might consider in the reasonable range become increasingly less reasonable when replicated 10 times a year or 20 times a year or 30 times a year.

While it is true consumers do not have to adopt a global opt-out or opt-in position, it is also true that assessing the best use of an annual \$50 or \$100 privacy budget among the multiplicity of companies who collect your data is a task more suited to a privacy expert than a busy single mom. Do you pick your ISP? Or Facebook? What about Amazon? The national pharmacy chain where you fill your prescriptions?¹⁰ And on and on.

While surely a cottage industry will develop in advising people how best to opt out, it is perhaps naive to expect that advice will reach everyone, or even most of the people who might need or want it.

For the most economically vulnerable communities, no advice in the world will make an extra \$50 present when it isn't there. We have been privacy advocates long enough to know that in a contest between privacy protection and food on the table, food on the table will win every single time.

8 <https://www.kqed.org/news/11689103/survey-nearly-half-of-working-californians-struggling-to-make-ends-meet>

9 <https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds>

10 <https://medium.com/bestcompany/5-companies-that-have-been-caught-violating-their-customers-privacy-9cfe660ea3eb>

The financial incentive language in CCPA probably has its origin in beliefs by businesses that rely on the sale of personal data that if customers are notified their data is being sold, large numbers of them will choose to opt out. By its nature, this is a speculation.¹¹

Given that we are dealing with a brand new law and consumers have never before received comprehensive information about how extensively their data is being sold, it is a guessing game to estimate how many will shrug, and how many will fill out the opt-out form. But if those with the most direct knowledge of data sale practices are convinced transparency will lead to a scale of opt-outs that will threaten their business models, then they are probably in the best position to make that guess.

So we will take it at face value that the problem here is two-fold.

- ◆ Firstly, that consumers may be pecked to death with small opt-out fees to such an extent that their ability and willingness to make free decisions about their privacy will be compromised by financial worries;
- ◆ Secondly, that many businesses may face such extensive opt-outs that their business model will be challenged, if not totally rendered unworkable;

As the AG's office navigates these interests, we want to note that there are distinctions to be made about the nature of affected transactional relationships and the affected business models.

In the first example, the nature of the transactions are the customer purchasing an item or service for a set price. While doing so, they provide data including their contact information, their product preferences and interests, and other related data. A business may then engage in collateral monetization of that collected data, usually without much knowledge by the customer who paid little-to-no attention to the lengthy privacy policy disclosing their info may be shared with third party partners.

In a simple example, I buy a hat on-line from a hat company. The hat company may have a collateral activity of selling their customer data to a company which then provides lists to sellers of similarly styled apparel items. In a broader sense, consumers pay their Internet Service Provider (ISP) for the ability to connect to the Internet. In this case, the fundamental transaction is not for the customer's data per se, but for a product or service - with the generated browsing data and any actual or potential monetization of it as a collateral activity. We will call these companies product providers.

The second example is companies that provide a service or product for free and engage in third party monetization of collected customer data as their fundamental source of income. This is a popular model for technology companies, including much of the social media Californians rely on.

¹¹ <https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules>

To go back to our hat example, a tech company might offer online a free hat reference service that directs potential customers to possible sources for different kinds of hats with comparative pricing and availability info. All for free, as long as they enter some data about their location, contact information, and consumer preferences into a form. Consumers often choose to use such services because they are convenient and save time. The company then has a data trove of interest to apparel companies everywhere and can and does monetize that collected data to support the costs of operating the referral site.

In this model, consumers generally suspect that their data is the product, expect they may see a few ads in the mail or on their screens in the future, and are sacrificing privacy about their consumer preferences in exchange for some convenience.

But it is fair to say that in at least some cases, users (as these individuals are not customers in the traditional sense of the word) may not be aware of the range of monetization activities and they may exceed the scope of their expectations.¹² So companies using this business model have some expectation that transparent disclosure of how user data is monetized will lead to a significant number of opt-outs. Like any business, they are justifiably terrified that the law will essentially break their business model and deprive them of their fundamental income stream. We will call these companies data providers.

It is our belief that a pay for privacy regulatory protocol would benefit greatly from separating these two categories of businesses to the extent legally permissible in the existing language. This would allow the law to address their needs independently, as they are not fundamentally the same.

Consumers are paying product provider companies for the service or product they are receiving. They reasonably think the price they pay is for the purpose of covering the company's costs for goods and labor to provide the product or service, and the data they provide to the company is primarily for the purpose of filling their order. In the free market economic model, a company adjusts the price for their product or service if what they are charging does not cover their costs and allow for some level of profit.

For product provider companies, we believe it is largely inappropriate for consumers to be charged twice, once for the product or service they bought, and once to halt the sale of the data they were required to submit in order to obtain the product.

We would recommend that product provider companies, since they have the discretion to adjust product prices to account for any loss of income from customer opt-outs, be prohibited from giving customers less advantageous prices for choosing to opt-out.

In the language of CCPA, the value of a customer's data to a business whose primary business is not data, can be mathematically defined as \$0. In practical terms the value of the data can be recompensed through product pricing. The fundamental business model here is product-based transactions, not the sale of data to third parties.

¹² https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1177&context=qc_pubs

This would protect consumers from a veritable flood of privacy-based fees by imposing enough market discipline that companies would raise prices only in the face of documented losses of revenue from CCPA opt-outs. Rather than what might otherwise happen with companies trying to de-incentivize opt-outs in advance with punitive pricing by default that is targeted only at privacy-protective customers.

For data providers, companies that provide free services in exchange for customer data that are then monetized as the primary function, it is understandable that CCPA provides a potentially existential crisis. If a substantial chunk or even most of the users opt out of data sales, the companies stand to go out of business.

We believe that it is these companies who the pay for privacy clause in CCPA is largely meant to protect. And deservedly so, at least to the extent they are offering services and products people want to use and for which users are willing to surrender their data in order to get them free of charge.

The problem for such companies in a post-CCPA world is that the exact nature of the deal may not have been clear to their users. Users understand that nothing is free (as in the old joke, if you don't know what the product is, rest assured that it is you), but they may not have been aware of the full extent of how their data was monetized. The risk that CCPA carries for such companies is that the transparency requirements will convince their users that the deal is a bad deal and they will lose them in such quantity that they can no longer cover their operating costs.

For such companies, a price different than free for a formerly free service may be the only way they can survive with a user base that partially or even substantially chooses to opt out of data sales. We agree that it may be necessary for such companies to reserve the free pricing of the service for users that permit the monetization of their data.

However, such a change should be as reality-based as possible. We'd like to see such pricing changes linked to verifiable data that users of a formerly free service have chosen to opt out of data sales in sufficient numbers. Pricing changes, especially in widely used services, should be necessary, not gratuitous or speculative.

We'd also like to have the numbers that are assessed as "the value of the customer's data" vetted for reasonableness, justness, non-coerciveness and non-usuriousness by the AG's office in advance of users being charged.

We envision a possible roll out of transparency requirements and opt-out notifications preceding any pay-for-privacy charges being levied. Armed with data about the what initial opt-out levels actually are, the AG would receive proposed non-advantageous pricing for opt-outs in 2021 and approve they are compatible with the law and meet standards for being reasonably related to the value of the data and are just, reasonable, non-coercive and not usurious.

We consider this to have two significant advantages:

- ◆ Firstly that the AG's office will not be overrun with complaints that pricing changes are neither just nor reasonable
- ◆ Secondly that better business decisions will be made with data on hand rather than speculation about how many users may choose to opt out.

We would hate to see users, especially low-income users, crowded off, for example, social networks that are important to many for connecting to friends and family and participating in civic dialogue, by sky-is-falling projections by data provider companies that are fear-based instead of fact-based.

One of the most contentious areas in the pay-for-privacy arena has been so-called “customer loyalty” programs which give users preferential pricing. Some businesses in the product provider category have indicated CCPA's language would prohibit such programs, which are popular with customers.

We are not sure that it is the case, for two reasons.

- ◆ Firstly, there is the intent of such programs. As we understand them, they are reward programs, but the reward is not for the provision of the customer's personal data to the company, but for the customer's loyalty i.e. their repeated purchases of the company's product or services. Accordingly the preferential pricing or discounts and/or gifts to the customer are not, by definition, reasonably related to the value of the customer's data. The incentivization is not to decline to opt out of data sales, but to repeatedly patronize the business.
- ◆ Secondly, there is the mode of selection. CCPA protocol allows an opt out of data sales. If customers do not affirmatively take action to opt out of data sales, then by definition, they have passively opted in. However CCPA's language adds a second bar for loyalty programs. The customer must affirmatively opt in.

The constraints applied by CCPA regarding pricing incentives is specific. The wording is relative to exercising the consumer's rights under the title.

With regard to financial incentive programs like loyalty programs, CCPA refers to section 1798.35.

A business that offers any financial incentives pursuant to subdivision (a), shall notify consumers of the financial incentives pursuant to Section 1798.135.

A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.135 which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.

Section 1798.135 specifies the requirement to provide a clear and conspicuous form to allow customers to opt out. The language in CCPA referring to discrimination with regard to financial incentives is specific to customers who exercise their right to **opt out**. Not those who exercise their right to voluntarily and affirmatively opt in to loyalty or discount programs.

There are three sets of customers:

- ◆ Those who **choose to opt-out**;
- ◆ Those who **affirmatively and voluntarily opt-in** to preferential pricing/discount/loyalty programs;
- ◆ Those who **do neither**.

CCPA's price discrimination language is directed at groups (1) and (3), specifically protecting group (1), who are exercising their rights under this title from being discriminated against relative to group (3), who are not choosing to exercise their rights under this title. Group (2) is affirmatively choosing to sell their data on a voluntary basis in order to get better pricing or goodies. Treating them identically to customers who passively fail to exercise their right to opt out would seem like a misreading of the text.

In other words, we would consider the language in CCPA to be intended to waive customers who intentionally opt in to loyalty programs from the language cited below, as the customer is affirmatively choosing not to exercise their right to opt-out under the title.

Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

*Providing a different level or quality of goods or services to the consumer, **if the consumer exercises the consumer's rights under this title.***

Media Alliance believes the language in this section was intended to exempt product provider company's loyalty discount programs from the preferential pricing prohibition, and was simply poorly written.

This distinction between opting out affirmatively, passively failing to opt out, and opting in affirmatively is significant in both understanding and functionally implementing the law as written. We hope it is one the Attorney General will recognize as such. The distinction will greatly assist efforts to protect consumers from untoward financial burdens should they wish to protect their private data from sales to third parties.

We believe the conflation of a passive failure to opt out and an affirmative choice to opt in to a loyalty program, whether accidental in the drafting or not, will be a strong contributor to industry frustration with the law and it's purported "unworkability". Untangling that conflation in the regulatory process would be a meaningful step in the real world implementation of CCPA.

We will add that the privacy community's general support for a global opt-in protocol, rather than an opt-out option, are at least partially based on the increased clarity provided by the global opt-in. But the regulatory process can only address the language in hand. The language in hand provides, we believe, sufficient grounds to exempt loyalty programs customers affirmatively choose from CCPA's differential pricing prohibition.

This clarification focuses the discrimination provisions where they belong; the two choices made by users and customers pursuant to the law: the decision to opt out of data sales or not to utilize the opt-out option.

Summary of Recommendations:

- 1) Separate CCPA-impacted companies according to whether or not they charge for their products or services.**
- 2) Set the value of a consumer's data to a business that charges for their product or service to their customers or users to \$0.**
- 3) For businesses that provide free products or services, vet proposals for less advantageous pricing for users that opt out on receipt of opt-out statistics and demonstration of reasonableness.**
- 4) Exempt customer loyalty programs from the differential pricing constraints in CCPA since customers affirmatively opt-in to such programs and by doing so are not exercising their rights under this title.**

Thank you for the opportunity to provide these comments.

We look forward to the 2020 implementation of the California Consumer Privacy Act of 2018.

We are proud of California for leading the way in consumer privacy protections.

Respectfully,

Tracy Rosenberg

Tracy Rosenberg
Executive Director
Media Alliance
2830 20th Street, Suite 102
San Francisco CA 94110

Web: <https://media-alliance.org>

Message

From: Roxanne Gould [REDACTED]
Sent: 3/7/2019 2:16:28 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments/suggestions relating to promulgation of regulations re: CCPA
Attachments: SKM_C224e19030714060.pdf

Attached please find comments and suggestions relating to the CCPA and regulations that the CA DOJ will be promulgating in the near future. Please feel free to contact me if you have any questions or would like clarification of any of our suggestions.

Best,

Roxanne Gould

Roxanne Gould

Gould Government Relations

1121 L Street, Suite 612

Sacramento, CA 95814



gouldgr.com

Protected Digital Identification and the CCPA

Protected Digital Identification (PDI) extends the convenience of mobile phone biometrics to any transaction in any sales channel. It is controlled by a mobile application that allows consumers to open new accounts in seconds with no typing, no talking or emailing sensitive identity documents, and access accounts with the touch of a finger. Unlike physical identity documents, PDI features built in identity protections and privacy controls that allow the consumer to control the personal information that they share when presenting the PDI. For example, if an organization needs only to verify age, the consumer can provide guaranteed proof that they are of age without disclosing any other personal information like their name, address or date of birth.

PDI provides both a high degree of personal data security and increased consumer convenience and will also help businesses protect their customers' personal data:

- PDI protects a consumer's data privacy by limiting the amount of PII that needs to be made available to accurately verify an individual's identity. Only the specific information required to conduct a transaction needs to be exchanged, and PDI facilitates that exchange.
- PDI reduces the number of organizations that need to store a consumer's PII. Trusted, third party Digital ID companies will provide the identity authentication without passing sensitive information on to the business/organization requesting the ID verification.
- Digital ID reduces the burden on businesses and puts them in a better position to comply with the CCPA and other privacy regulations. By outsourcing identity verification to a trusted third party, businesses get out of the "personal information business" and reduce their liability for keeping that information private.

While implementing the CCPA, the state of California should clear a path such that responsible third-party digital ID companies can be a part of the solution to protect Californians' personal information.

Founded in 2004, AllClear ID is the world leader in customer identity services that eliminate identity friction, fraud and remediate harm from data breaches. As a trusted partner with more than 14 years of experience, AllClear ID has helped over 5,000 businesses prepare for and recover from data breaches, including successfully managing the three largest, fastest and most complex breach responses in history. The award-winning AllClear ID team is recognized for its expertise, customer service, and guaranteed deployment of large-scale response operations in as little as 72 hours. AllClear ID breach response services are now available globally through a collaboration with Deloitte.

Contacts: Bo Holland

Jeff Erramouspe

The logo consists of the text "AllClear ID" in white, sans-serif font, centered within a blue, horizontally-oriented hexagonal shape. The background of the entire page features a large, abstract geometric pattern of overlapping blue and white triangles and parallelograms, creating a sense of depth and movement.

AllClear ID

AllClear ID™

Protected Digital Identity

Questions? Contact:

Bo Holland, Founder & CEO

A solid black rectangular box used to redact contact information, likely a phone number or email address.

About AllClear ID

Founded in 2004, AllClear ID is the world leader in customer identity services that eliminate identity friction, fraud and remediate harm from data breaches. As a trusted partner with more than 14 years of experience, AllClear ID has helped over 5,000 businesses prepare for and recover from data breaches, including successfully managing the three largest, fastest and most complex breach responses in history. The award-winning AllClear ID team is recognized for its expertise, customer service, and guaranteed deployment of large scale response operations in as little as 72 hours. AllClear ID breach response services are now available globally through a collaboration with Deloitte.

Unmatched Expertise

We provide identity protection and Strong Customer Authentication solutions for employees and customers backed by the industry's highest customer service ratings. Highlights include:

- Benefits programs for Blue Shield of California, University of California System, Intel and Cisco
- Successfully managed massive data breaches including Sony, Anthem Blue Cross, and Home Depot
- A "Leader" — in the highest ranking in the Forrester Wave™ Customer Data Breach Notification and Response Services, [Q3 2015](#)¹ and [Q4 2017](#)²
- 96% customer satisfaction rating⁴
- +75 client Net Promoter Score on a scale of -100 to +100)
- 31 Stevie Awards for outstanding customer service
- 100% success rate in resolving financial identity theft cases in the United States³

Leading Organizations Choose AllClear ID



¹ Forrester Wave™ Customer Data Breach Notification and Response Services, Q3 2015 study.

² Forrester Wave™ Customer Data Breach Notification and Response Services, Q4 2017 study.

³ Rate is valid through 2018 and applies to cases involving adults covered by U.S. consumer protection laws.

⁴ Calculation based on the 2018 results of surveys sent to all customers who interacted with the AllClear ID support team.

AllClear Protected Digital Identity (Available 2nd Half of 2019)



A Delightful Identity Experience that Eliminates the Hassles and Vulnerabilities of Passwords

The AllClear ID is a Protected Digital Identity (PDI) that extends the convenience of mobile phone biometrics to any transaction in any sales channel. It is controlled by a mobile application that allows you to open new accounts in seconds with no typing, no talking or emailing sensitive identity documents, and access accounts with the touch of a finger. And it is backed by the AllClear Guarantee (see benefits detail below).

Unlike physical identity documents, it features built in identity protections and privacy controls that allow you to control the personal information that you share when presenting your AllClear ID. For example, if an organization needs only to verify your age, you can provide guaranteed proof that you are of age without disclosing any other personal information like your name, address or date of birth.

The AllClear ID creates a highly secure two-way authentication channel between the device and the AllClear server. This two-way, cryptographically secure channel breaks the dependence on passwords altogether and is practically invulnerable to man-in-the-middle attacks.

What is a Digital Identity?

A highly secure, electronic identity that enables consumers to electronically present their identity for transactions where a physical identity card is useless. Transactions made easy and secure with a digital identity include opening new accounts online and accessing existing accounts with the touch of a finger.

Consumer Benefits

- Open new accounts in seconds — no more typing, talking or emailing sensitive identity documents
- Access existing accounts with the touch of a finger — no more passwords or security questions
- Protect privacy by sharing only the personal information required like age or eligibility
- Prevent identity theft with fraud alerts, identity repair and a \$1M personal identity theft insurance policy
- Backed by the AllClear Guarantee: If you become a victim of identity theft, AllClear will do the work to recover financial losses and repair your credit records.

Organizational Benefits

- Increase customer engagement by up to 7 times by eliminating the identity friction of passwords and knowledge based security questions
- Eliminate lost sales due to forgotten passwords and locked accounts
- Extend the convenience of mobile biometrics to any transaction in any sales channel including online, call center, mobile and in-person
- Reduce fraud and operational costs by eliminating the attacks and vulnerabilities associated with passwords and knowledge-based security questions
- Improve compliance with electronic audit logs, explicit consent and non-repudiation
- Backed by the AllClear Guarantee: If an AllClear transaction results in fraud, AllClear will reimburse the organization for financial losses and provide support for privacy enforcement actions

California Opportunities for Digital ID

- Online ordering and deliver of controlled substances including cannabis, alcohol and prescription drugs
- Age verification for adult venues and online services
- Preventing abuse of the CCPA by verifying identity before downloading or destroying personal data

Message

From: Kelly Hitt [REDACTED]
Sent: 3/8/2019 4:41:13 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CompTIA Comments to Preliminary CCPA Rulemaking
Attachments: CompTIA CCPA 2018 Comments CA AG March 8 2019.pdf

Good Afternoon,

Attached, please find the Computing Technology Industry Association's (CompTIA) written comments for consideration in the preliminary rulemaking stage for the California Consumer Privacy Act of 2018. Thanks you for the opportunity to comment and we look forward to working with you throughout the regulatory process.

Thank you,

Kelly Hitt

Kelly Hitt | Director, Government Affairs – California and Hawaii

Computing Technology Industry Association (CompTIA)

1215 K Street, 17th Floor | Sacramento, CA 95814

[REDACTED] | [REDACTED] | [CompTIA.org](https://www.comptia.org)

Get the latest [IT business and career advice from CompTIA](#)

March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

Thank you for the opportunity to submit the following written comments for consideration in the preliminary rulemaking stage for the California Consumer Privacy Act of 2018 (CCPA). The Computing Technology Industry Association (CompTIA) is a global non-profit trade association serving as the voice of the information technology industry. With approximately 2,000-member companies, 3,000 academic and training partners and nearly 2 million IT certifications issued, CompTIA is dedicated to advancing industry growth through educational programs, market research, networking events, professional certifications, and public policy advocacy.

Below is a set of recommendations that includes policy rationale and regulatory language that we would like considered as part of the regulations. These recommendations were compiled by many of our member companies and reflect necessary changes to protect consumers and ensure compliance by the regulated community.

CCPA Proposed Attorney General Regulatory Language

- (1) Exclusion of employee data. The Attorney General, through regulatory language proposed below, can clarify that section 1798.140 (o)(1) does not cover personal information collected in the employment context. Making this clarification ensures that the CCPA would not impact and conflict with the already existing framework in California for employee access to their employment information.¹

Proposed Regulatory Language

For purposes of paragraph (1) of subdivision (o) of Section 1798.140 of the Act, information shall not constitute "personal information" where the information is collected by a business from an employee or applicant and the information relates to the person's employment or application for employment with the business.

- (2) Exclusion of other non-consumer data. In addition to excluding personal information collected in the employment context as noted above in (1), the Attorney General should clarify that personal information does not include personal information collected in connection with an individual's role as a director, agent, independent contractor, subcontractor or vendor of a business.

¹ See e.g., [Labor Code 1198.5](#) and corresponding Department of Industrial Relations guidance available at https://www.dir.ca.gov/dlse/FAQ_RightToInspectPersonnelFiles.htm; [Labor Code 226\(b\)](#), and [Labor Code 432](#).

Proposed Regulatory Language

For purposes of paragraph (1) of subdivision (a) of Section 1798.140 of the Act, information shall not constitute “personal information” where the information collected by a business related to an individual is collected in connection with that individual’s role as a director, agent, independent contractor, subcontractor or vendor of a business.

- (3) “Do Not Sell My Personal Information” link location. Due to an ambiguity as to where this link needs to appear, resulting from the language in Section 1798.135(a), coupled with the definition of “homepage” in Section 1798.140(l), the Attorney General, through the regulatory language proposed below, can resolve such ambiguity. In particular, when a business or a brand does not maintain what may be traditionally perceived as a “homepage,” flexibility is needed as to where such a link should be placed in order to best reach consumers. For example, it may make sense for the opt-out choice to be offered alongside or in conjunction with a company’s privacy policy or page, as that is the location that consumers generally visit to learn about their choices and manage any offered preferences.

Proposed Regulatory Language

A business shall be deemed in compliance with paragraph (1) of subdivision (a) of Section 1798.135 of the Act where the business places a clear and conspicuous “Do Not Sell My Personal Information” link or logo on a privacy page posted on the business’ Internet Web site or within an online service, such as a mobile application.

- (4) “Do Not Sell My Personal Information” choices. The Attorney General should clarify that a business may comply with Section 1798.120 by providing a consumer with the ability to make more granular opt-out choices with respect to the sale of information in addition to an option to opt-out of all sales. This interpretation is consistent with the approach in the federal Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM ACT). The CAN-SPAM Act, which requires the ability to opt-out of certain email messages, allows the initiator of such messages to offer recipients the opportunity to choose the specific types of messages the recipient wants to receive or not receive, so long as an option to not receive any commercial electronic mail messages from the sender is also made available.²

Proposed Regulatory Language

A business that is required to comply with Section 1798.120 may comply by providing the consumer a list or menu from which the consumer may choose different types of

² 15 U.S.C. § 7704(a) (3) (B). *“More detailed options possible. The person initiating a commercial electronic mail message may comply with subparagraph (A)(i) by providing the recipient a list or menu from which the recipient may choose the specific types of commercial electronic mail messages the recipient wants to receive or does not want to receive from the sender, if the list or menu includes an option under which the recipient may choose not to receive any commercial electronic mail messages from the sender.”*

sales, categories of third parties, or other options, provided that the list or menu includes an option under which the consumer may choose to opt out of all sales of the consumer's personal information.

- (5) "Do Not Sell My Personal Information" safe harbor for opt-in choices. The Attorney General should clarify that, if a business engages in the sale of personal information pursuant to an individual's opt-in consent only, such sales need not be included as part of the global "Do Not Sell My Personal Information" choice that is required under the law. Any interpretation to the contrary would result in a disincentive for businesses to engage in sales only following opt-in consent. If a customer opting in to sales would then be reversed by the required "global" "Do Not Sell My Personal Information" choice, companies will lack incentive to offer opt-in choices. Moreover, consumers would not expect that, if they had affirmatively opted-in to a particular program, that it would be "undone" by a global "Do Not Sell My Personal Information" choice. A consumer would expect to interface with the company specifically as it relates to that program if they decide to no longer opt in. Accordingly, so long as businesses provide individuals with a mechanism to subsequently opt-out of sales for which they had previously opted in, such opt-out need not be included in the global "Do Not Sell My Personal Information" choice. For example, 1798.125(b)(3) requires certain programs to be on an opt-in basis and specifically requires that they may be revoked by the consumer at any time. Opt-in programs, (including ones contemplated by Section 1798.125(b)(3)), to the extent they involve the sale of Personal Information, should not be included as part of the "Do Not Sell My Personal Information" choice, as consumers should have the opportunity to revoke their specific participation in a program, and not make a choice based on a global choice that they may not understand will result in them becoming unenrolled in a program to which they opted in.

Proposed Regulatory Language.

A business shall be deemed in compliance with Section 1798.135 of the Act and shall not need to provide the "Do Not Sell My Personal Information" link or logo where the business requires the consumer to opt in to the sale of personal information and provides the consumer a mechanism to subsequently opt out.

- (6) Personal Information exclusions: SB 1121 revised the definition of "Personal Information" by adding the text in red underline below.

"Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

The addition of this text clarifies that the scope of "Personal Information" should not extend beyond information that "identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly" with a particular consumer or household. To avoid ambiguity, the Attorney General should clarify that pseudonymized data, as well as

deidentified data (which are already defined terms) are outside the scope of “Personal Information.”

Proposed Regulatory Language.

For purposes of paragraph (1) of subdivision (o) of Section 1798.140 of the Act, information shall not constitute “personal information” where the information is pseudonymized or deidentified, or is aggregate consumer information.

- (7) Definition of Sale: The first paragraph of the definition of “sell,” “selling,” “sale” or “sold” in the Act, reads as follows:

1798.140....(t) (1) “Sell,” “selling,” “sale,” or “sold,” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.

The phrase “valuable consideration,” however, is undefined. The Attorney General should clarify that “valuable consideration” is limited to similar monetary consideration to avoid any ambiguity on what was intended by this provision. “Sales” should be limited to those instances where a third party obtains independent rights to ongoing use of Personal Information in exchange for actual monetary consideration. Additionally, in order to avoid a disruption to the online advertising ecosystem, which this Act does not appear intended to reach, the Attorney General should clarify that disclosures for such specified purposes in connection with the delivery of online advertising are outside the scope of what constitutes a “sale.”

Proposed Regulatory Language

For purposes of paragraph (1) of subdivision (t) of Section 1798.140 of the Act, “valuable consideration” shall mean money, a gift, a loan, or similar monetary consideration. Personal information is not “sold” where the disclosure of the personal information is necessary for or incidental to the delivery, display, measurement, customization, or analysis of an online advertisement.

- (8) Verifiable consumer requests. The Act requires businesses to take certain action upon receipt of a “verifiable consumer request.” Verification is critically important to ensure that information about a consumer is only released when his or her identity can be confirmed. Businesses should have flexibility in how they verify such consumers and their requests, and specific methods should not be required. This will allow for the development of innovative methods to ensure that information is not incorrectly disclosed. Considering the potential harm if information about a consumer is disclosed to the wrong person, businesses should have the discretion to determine whether a consumer has been properly verified, particularly when the consumer does not hold an account with the business. Very often, businesses verify individuals during the course of account formation – when an account is lacking certain information, then verification is more difficult. Businesses should be erring on the side of caution and should not disclose information when a consumer has not been properly verified.

The Attorney General should, in its regulations, note that if a business is unable to verify a request that they communicate that to the consumer. In addition, the Attorney General should clarify the

role of service providers in connection with access and deletion requests, by clarifying that consumers should make requests directly to the business, and how service providers should respond to such requests.

Proposed Regulatory Language

- (i) ***If the business cannot reasonably verify the consumer's request based on the information provided, then the business shall send the consumer, or the person authorized by the consumer to act on the consumer's behalf, an explanation that the consumer's identity could not be verified.***
- (ii) ***Consumers shall not make rights requests directly to service providers. If a service provider receives a request directly from a consumer, the service provider may respond with an explanation that the consumer's identity could not be verified or that the request should be submitted to the business with the direct relationship with the consumer. The service provider shall, taking into account the nature of the processing and the relationship with the business, upon the business's request, assist the business in fulfilling the business's obligation to respond to the consumer's request, insofar as this is reasonably possible.***

- (9) **Data Retention.** In its regulations, the Attorney General should clarify that there is no obligation for a business to retain personal information solely for the purposes of fulfilling a consumer's request under the Act. Although Section 1798.100(e) states that a business is not required to retain certain personal information collected for a single, one-time transaction that is maintained in a manner that would be considered personal information, the Attorney General should clarify more broadly the personal information does not need to be retained to honor all the obligations under the Act. Any interpretation to the contrary would actually create additional privacy and security risk to personal information, by potentially requiring organizations to retain data that they otherwise would not.

Proposed Regulatory Language

Under no circumstances is a business required to retain personal information solely for the purpose of fulfilling a consumer request made under the Act.

- (10) **Specific Pieces of Information.** The Attorney General should clarify that companies are not required to provide specific pieces of information to consumers in response to an access request if doing so would create an unreasonable risk to the security of that information. Indeed, the California Legislature has recognized the importance of data security as it relates to certain data elements as outlined in Section 1798.81.5 in California law, which is also referenced in the Act in Section 1798.150.

Proposed Regulatory Language

Under no circumstances shall a business be required to provide a consumer with specific pieces of personal information if such disclosure might unreasonably risk the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks, including but not limited to personal

information as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5.

- (11) Federal law. Although Section 1798.196 includes certain application limitations for the Act, with respect to access requests made by consumers, the Attorney General should further clarify that a business is not required to make disclosures in violation or in conflict with federal law.

Proposed Regulatory Language

Pursuant to paragraph (1) of subdivision (a) of Section 1798.145, a business shall not be required to take any action in response to a consumer request if such action would violate or conflict with any federal law or regulation, including any order issued by a federal agency.

- (12) Effective date. The effective date of the Act is January 1, 2020; however, it is ambiguous as to when access obligations would start to “run” with regard to a business’ obligations to disclose how information is collected, processed, shared, or sold. Accordingly, the Attorney General should clarify that those obligations apply on a prospective basis, as of January 1, 2020.

Proposed Regulatory Language

A business must comply with a consumer request made under the Act only as it pertains to data collected processed, disclosed, or sold by the business after January 1, 2020.

- (13) Disclosures to consumers. Section 1798.115 sets forth what companies have to disclose to consumers, upon a verifiable request, with regard to personal information that is sold or disclosed for a business purpose. Section 1798.115(a)(2) requires businesses to provide consumers with the categories of personal information sold, as well as the categories of third parties to whom the information was sold. The section then continues and says that this disclosure has to correlate the categories of personal information to each third party. Since the requirement is only for the disclosure of categories of third parties, the correlation of the categories of personal information is intended to be to the categories of third parties. However, as noted, because of the ambiguity of the language, there exists a lack of clarity on what is in fact required.

Proposed Regulatory Language

Pursuant to paragraph (2) of subdivision (a) of Section 1798.115, a business shall not be required to correlate the categories of personal information sold to each third party to whom the information was sold. A business shall be in compliance with the paragraph if it correlates the categories of personal information sold to the categories of third parties to whom information is sold.

- (14) **“Publicly available”**. The definition of “publicly available” in Section 1798.140 (o)(2) is unclear and difficult for a business to interpret, as a business that receives personal information from an entity that reproduced and compiled it from government records will lack the requisite knowledge to determine if the purposes for which the information was reproduced is “compatible with the purpose for which the data is maintained”. Accordingly, the Attorney General should clarify that “publicly available” pertains only to government records.

Proposed Regulatory Language

“Personal information” does not include publicly available information. For these purposes, “publicly available” means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. “Publicly available” does not mean biometric information collected by a business about a consumer without the consumer’s knowledge. ~~Information is not “publicly available” if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.~~ “Publicly available” does not include consumer information that is deidentified or aggregate consumer information.

- (15) The definition of a “third party” in Section 1798.140(w)(2) appears to meet the definition of a “service provider” in Section 1798.140(v), except for the certification requirement in Section 1798.140(w)(2)(ii). If this was the intent, the Attorney General should clarify these definitions as follows:

Proposed Regulatory Language

“Service provider” means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business, and includes a certification made by the person receiving the personal information that the person understands the restrictions in this paragraph and will comply with them.

Proposed Regulatory Language

“Third party” means a person who is not any of the following:

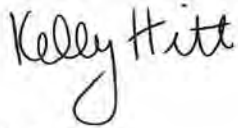
(1) The business that collects personal information from consumers under this title.

(2) A service provider as defined in Section 1798.140(v).

Thank you again for the opportunity to comment in the preliminary rulemaking stage for the California Consumer Privacy Act of 2018 (CCPA). If you have any questions, please feel free to contact me at

[REDACTED]

Sincerely,



Kelly Hitt
Director, State Government Affairs - California & Hawaii
CompTIA (Computing Technology Industry Association)

Message

From: Paul Rudewicz [REDACTED]
Sent: 2/3/2019 11:47:36 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Consumer privacy
Flag: Follow up

Every phone call should be required to provide the source of the telephone number and personal information that was obtained to make the call. The use of phony caller id's should be prohibited. The consumer should be able to call back the offending idiot any time of the day or night at his/her private residence as they already have access to the consumer's information.

Ideally, every robo call should be heavily taxed and be the best benefit to the consumer.

Paul R.

Message

From: Adam Scow [REDACTED]
Sent: 3/8/2019 4:14:11 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Consumer Watchdog Comments on CCPA
Attachments: AGCCPA2019.pdf

Dear Office of the Attorney General,

Please find Consumer Watchdog's comments attached on the CCPA rule making process.

Thanks,

Adam Scow
Consumer Watchdog
[REDACTED]



March 8, 2019

Attorney General Xavier Becerra
P.O. Box 944255
Sacramento, CA 94244-2550

Via email: privacyregulations@doj.ca.gov

RE: California Consumer Privacy Act – Rulemaking Process

Dear Attorney General Becerra:

Consumer Watchdog thanks you for the opportunity to provide input on the implementation of the California Consumer Privacy Act. Americans are increasingly worried about the security of their data and 85% say they want to control what data is collected about them. The CCPA is the first law in the nation to create privacy rights over our digital data, giving us the right to know what is being collected and the right to have that information deleted.

Your job is to make sure that the law is implemented in a way to ensure Californians get the level of protection intended by the act. The latest massive data breach by some of the nation's largest banks, which compromised 24 million financial documents for tens of thousands of loan and mortgage customers, illustrates why this rulemaking process is important. Everything an identity thief needs to impersonate a person and steal sensitive information was exposed in that breach. Similarly, Marriott disclosed a breach of 400 Million of its customers' records including passport numbers and credit cards. Facebook recently revealed another major breach of public trust, admitting that it gave major tech companies greater access to user data than they disclosed.

These breaches demonstrate the need for strong regulations and the right to sue when data is compromised to ensure companies are responsibly managing their customers' data. We would like to make the following recommendations as you begin the rulemaking process:

Financial Incentives

Rules to ensure that companies do not discriminate against those who prefer to have their data private are critical. The CCPA clearly states the intent to ensure: "The right of Californians to equal service and price, even if they exercise their privacy rights." Section 125(b)4 says any financial incentive dreamt up by a company to convince a consumer to allow it to sell their data cannot be "unjust, unreasonable, coercive or usurious."

The law allows businesses to offer financial incentives to convince consumers not to opt out only if those incentives are related to the value of consumers' data. Any incentives provided by companies to convince consumers to allow data sales cannot force mid- and low-income consumers to give up their privacy in order to use a website or service. That means any different price or disparate level of service must be "directly related" to the value of a consumer's data.

When a consumer is offered a financial incentive to allow their data to be sold, the company must be explicit about how it is calculated and prove the charge is correlated to the value of a consumer's data. For example, if a blog site wants to offer the financial incentive of a free subscription in exchange for the right to sell a consumer's data, they should provide evidence that the consumer's data is worth the value of a subscription.

The best way for your office, and the public, to be confident that companies aren't discriminating against consumers who choose privacy, is to require disclosure of revenues and the method by which a company calculates value of the data. To that end, we urge you to require any company seeking to offer consumers incentives to allow their data to be shared to submit quarterly reports to your office on the revenue they bring in from the sale of consumer data, the number of consumers whose data they sell, and a per-user value of that data.

Companies must prove that any financial incentive is directly tied to the value of consumer data to ensure Californians' right to equal service and price under the CCPA.

Opting-Out

Companies must give consumers a clear and obvious way to opt out of having their data sold. We strongly recommend requiring companies to have a link or box that states, "DO NOT SELL OR SHARE MY PERSONAL INFORMATION." The text should be in a larger font than the predominant font size of the website, in a contrasting color, and clearly be a link/invitation for consumers to take action. The opt-out link should be available on every page of a website. This should be a simple process with clear language that avoids confusing legal terms. Companies should be prohibited from burying the opt-out beneath more than two click-throughs: One click to get to the page explaining what it means to opt out, and a second click to actually opt out.

Right to download data

The ability of the consumers to download their data, and move it to another service, is essential for individual control of their data. Despite industry complaints, this right has already been successfully implemented in Europe under the GDPR.

Unique identifiers

The CCPA is clear that an IP address is a unique identifier, and that “personal information” includes anything “capable of being associated with” or “reasonably be linked, directly or indirectly” with a household, consumer or family. There is no good justification for excluding IP address since it can easily be linked to a specific person or household.

Categories of information

Rules should protect all personal information collected by companies. The law defines “personal information” broadly as all data a company collects and relates to a person in any way. This category must not be limited to traditionally “sensitive” categories of data because the inferences companies can make from even seemingly innocuous data are broad.

Categories of information that a website must disclose to consumers should distinctly identify “Data About Your Activity On This Site” (and related sites): purchasing habits, number of hours or time of day a consumer is on a site, articles or products viewed, “likes”, and similar data categories. Companies must also disclose inferences they make about consumers based on that data:

If there is value to a company sharing or selling one’s data, there is a value to consumers opting out of its sale. Consumers who opt-out of data sales must also have their information protected.

Thank you for the opportunity to provide these recommendations towards ensuring a full and fair adoption of California’s landmark privacy act.

Sincerely,

Adam Scow, Consumer Advocate

Message

From: Mary Ross [REDACTED]
Sent: 3/8/2019 7:27:07 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Edits on Enforcement
Attachments: MSR Edits to SB 1121 v.1.docx

Please use this draft. I added the following language. Thanks!

Mary

I agree with the concerns raised by your office that the Attorney General alone is not well positioned to be the sole enforcer of such a broad act. I encourage your office to work with Sacramento to allow, like the original initiative, enforcement “by any district attorney, by any county counsel authorized by agreement with the district attorney in actions involving a violation of a county ordinance, by any city attorney of a city having a population in excess of 750,000, by any city attorney of any city and county, or, with the consent of the district attorney, by a city prosecutor in any city having a full-time city prosecutor, in any court of competent jurisdiction.”

Mary Stone Ross
Principal
MSR Strategies


CONFIDENTIALITY NOTICE: This electronic mail transmission may contain privileged and/or confidential information only for use by the intended recipients. Unless you are the addressee (or authorized to receive messages for the addressee), you may not use, copy, disclose, or distribute this message (or any information contained in or attached to it) to anyone. You may be subject to civil action and/or criminal penalties for violation of this restriction. If you received this transmission in error, please notify the sender by reply e-mail and delete the transmission. Thank you.

On Thu, Mar 7, 2019 at 11:40 PM Mary Ross [REDACTED] wrote:
Hi--

I am attaching my comments to SB 1121 as well as a copy of the remarks I delivered at the open forum at Stanford on Tuesday. I was a co-author and a proponent of the original initiative, however, I am no longer affiliated with Californians for Consumer Privacy.

Please let me know if you have questions. I'm truly happy to help.

All the best,
Mary

Mary Stone Ross
Principal
MSR Strategies


CONFIDENTIALITY NOTICE: This electronic mail transmission may contain privileged and/or confidential information only for use by the intended recipients. Unless you are the addressee (or authorized to receive messages for the addressee), you may not use, copy, disclose, or distribute this message (or any information contained in or attached to it) to anyone. You may be subject to civil action and/or criminal penalties for violation of this restriction. If you received this transmission in error, please notify the sender by reply e-mail and delete the transmission. Thank you.

Senate Bill No. 1121

CHAPTER 735

An act to amend Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.185, 1798.192, 1798.196, and 1798.198 of, and to add Section 1798.199 to, the Civil Code, relating to personal information, and declaring the urgency thereof, to take effect immediately.

[Approved by Governor September 23, 2018. Filed with Secretary of State September 23, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

SB 1121, Dodd. California Consumer Privacy Act of 2018.

(1) Existing law, the California Consumer Privacy Act of 2018, grants, commencing on January 1, 2020, a consumer various rights with regard to personal information relating to that consumer that is held by a business, including the right to request a business to delete any personal information about the consumer collected by the business, and requires the business to comply with a verifiable consumer request to that effect, unless it is necessary for the business or service provider to maintain the customer's personal information in order to carry out specified acts. The act requires a business that collects personal information about a consumer to disclose the consumer's right to delete personal information described above on its Internet Web site or in its online privacy policy or policies.

This bill would modify that requirement by requiring a business that collects personal information about a consumer to disclose the consumer's right to delete personal information in a form that is reasonably accessible to consumers and in accordance with a specified process.

(2) The act establishes several exceptions to the requirements imposed, and rights granted, by the act, including prohibiting the act from being interpreted to restrict the ability of a business to comply with federal, state, or local laws, and by providing that the act does not apply if it is in conflict with the California Constitution.

This bill would provide that the rights afforded to consumers and the obligations imposed on any business under the act does not apply if those rights or obligations would infringe on the noncommercial activities of people and entities described in a specified provision of the California Constitution addressing activities related to newspapers and periodicals. The bill would also prohibit application of the act to personal information collected, processed, sold, or disclosed pursuant to a specified federal law relating to banks, brokerages, insurance companies, and credit reporting agencies, among others, and would also except application of the act to that information pursuant to the California Financial Information Privacy Act. The bill would provide that these

exceptions, and the exception provided to information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994, do not apply to specific provisions of the act related to unauthorized theft and disclosure of information. The bill would revise and expand the exception provided for medical information, would except a provider of health care or a covered entity, and would also except information collected as part of clinical trials, as specified. The bill would also clarify that the act does not apply if it is in conflict with the United States Constitution.

(3) The act generally provides for its enforcement by the Attorney General, but also provides for a private right of action in connection with certain unauthorized access and exfiltration, theft, or disclosure of a consumer's nonencrypted or nonredacted personal information, as defined for this purpose, provided that the consumer bringing an action notify the Attorney General of the action in accordance with a specified process. The act provides that a business, service provider, or other person who violates its provisions, and fails to cure those violations within 30 days, is liable for a civil penalty under laws relating to unfair competition in an action to be brought by the Attorney General. The act prescribes a formula for allocating civil penalties and settlements assessed in these actions with 80% to be allocated to the jurisdictions of the behalf of which the action was brought.

This bill would clarify that the only private right of action permitted under the act is the private right of action described above for violations of unauthorized access and exfiltration, theft, or disclosure of a consumer's nonencrypted or nonredacted personal information and would delete the requirement that a consumer bringing a private right of action notify the Attorney General. The bill would remove references to laws relating to unfair competition in connection with Attorney General actions described above. The bill would limit the civil penalty to be assessed in an Attorney General action in this context to not more than \$2,500 per violation or \$7,500 per each intentional violation and would specify that an injunction is also available as remedy. The bill would eliminate the formula for allocating penalties and settlements and would instead provide that all of these moneys be deposited in the Consumer Privacy Fund with the intent to offset costs incurred by the courts and the Attorney General in connection with the act. The bill would also revise timelines and requirements regarding the promulgation of regulations by the Attorney General in connection with the act.

(4) The act makes its provisions operative on January 1, 2020, provided a specified contingency is satisfied. Provisions of the act supersede and preempt laws adopted by local entities regarding the collection and sale of a consumer's personal information by a business.

This bill would make the provisions of the act that supersede and preempt laws adopted by local entities, as described above, operative on the date the bill becomes effective.

(5) This bill would also make various technical and clarifying changes to the act.

(6) This bill would declare that it is to take effect immediately as an urgency statute.

DIGEST KEY

Vote: 2/3 Appropriation: no Fiscal Committee: yes Local Program: no

BILL TEXT

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS
FOLLOWS:

SECTION 1.

Section 1798.100 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.100.

(a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

(b) A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.

(d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered—per the consumer's preference— by mail or electronically, and if provided electronically or delivered by mail, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

(e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

SEC. 2.

Section 1798.105 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.105.

(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

(c) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.

(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

(6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(8) Comply with a legal obligation.

(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

SEC. 3.

Section 1798.110 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.110.

(a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer any or all of the following:

(1) The categories of personal information it has collected about that consumer.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) The specific pieces of personal information it has collected about that consumer.

(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer.

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The categories of personal information it has collected about ~~that~~ consumers.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) The specific pieces of personal information the business has collected about that consumer.

(d) This section does not require a business to do the following:

(1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.

(2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

SEC. 4.

Section 1798.115 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.115.

(a) A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

(1) The categories of personal information that the business collected about the consumer.

(2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose.

(b) A business that sells personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to paragraph (4) of

subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

(c) A business that sells consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The category or categories of consumers' personal information it has sold, or if the business has not sold consumers' personal information, it shall disclose that fact.

(2) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.

SEC. 5.

Section 1798.120 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.120.

(a) A consumer or a person authorized by the consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out.

(b) A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt-in."

(d) A business that has received direction from a consumer or a person authorized by the consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited, pursuant to paragraph (4) of subdivision (a) of Section 1798.135, from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.

SEC. 6.

Section 1798.125 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.125.

(a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title 1798.100, 1798.110 or 1798.115, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data.

(b)(1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the ~~consumer-business~~ by the consumer's data.

(2) A business that offers any financial incentives pursuant to subdivision (a), shall notify consumers of the financial incentives pursuant to Section 1798.135 and shall clearly define the value provided to the business by the consumer's data.

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.135 which clearly describes the material terms of the financial incentive program, the value provided to the business by the consumer's data, and which may be revoked by the consumer at any time.

(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

SEC. 7.

Section 1798.130 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.130.

(a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.

(2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business's duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business's receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business shall not require the consumer to create an account with the business in order to make a verifiable consumer request.

(3) For purposes of subdivision (b) of Section 1798.110:

(A) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its Internet Web site, and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.

(B) For purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact.

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Sections 1798.110, 1798.115, 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business's verification of the consumer's request solely for the purposes of verification.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.110 and 1798.115 shall follow the definition of personal information in Section 1798.140.

SEC. 8.

Section 1798.135 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.135.

(a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

(2) Include a description of a consumer's rights pursuant to Section 1798.120, along with a separate link to the "Do Not Sell My Personal Information" Internet Web page in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers' privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer.

(5) For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information.

(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(b) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

(c) A consumer may authorize another person solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General.

SEC. 9.

Section 1798.140 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.140.

For purposes of this title:

(a) "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

(b) "Biometric information" means an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a

faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) "Business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) Has annual gross revenues in excess of twenty-five million dollars (\$25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark.

(d) "Business purpose" means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.

(5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.

(6) Undertaking internal research for technological development and demonstration.

(7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

(e) "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving

information from the consumer, either actively or passively, or by observing the consumer's behavior.

(f) "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. "Commercial purposes" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

(g) "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

(h) "Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(2) Has implemented business processes that specifically prohibit reidentification of the information.

(3) Has implemented business processes to prevent inadvertent release of deidentified information.

(4) Makes no attempt to reidentify the information.

(i) "Designated methods for submitting requests" means a mailing address, email address, Internet Web page, Internet Web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

(j) "Device" means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.

(k) "Health insurance information" means a consumer's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer's application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.

(l) "Homepage" means the introductory page of an Internet Web site and any Internet Web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information," or settings page, and any other location that allows consumers to review the notice required by subdivision (a) of Section 1798.145, including, but not limited to, before downloading the application.

(m) "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(n) "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(o) (1) "Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household Device. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

Psychometric information

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(2) "Personal information" does not include publicly available information. For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. "Publicly available" does not include consumer information that is deidentified or aggregate consumer information.

(p) "Probabilistic identifier" means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(q) "Processing" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.

(r) "Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(s) "Research" means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes shall be:

(1) Compatible with the business purpose for which the personal information was collected.

(2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

- (4) Subject to business processes that specifically prohibit reidentification of the information.
- (5) Made subject to business processes to prevent inadvertent release of deidentified information.
- (6) Protected from any reidentification attempts.
- (7) Used solely for research purposes that are compatible with the context in which the personal information was collected.
- (8) Not be used for any commercial purpose.
- (9) Subjected by the business conducting the research to additional security controls limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.
- (t) (1) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.
- (2) For purposes of this title, a business does not sell personal information when:
 - (A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.
 - (B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.
 - (C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:
 - (i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.
 - (ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.
 - (D) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).
- (u) "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.
- (v) "Service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise

permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

(w) "Third party" means a person who is not any of the following:

(1) The business that collects personal information from consumers under this title.

(2) (A) A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:

(i) Prohibits the person receiving the personal information from:

(I) Selling the personal information.

(II) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.

(III) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

(ii) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

(B) A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.

(x) "Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

(y) "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

SEC. 10.

Section 1798.145 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.145.

(a) The obligations imposed on businesses by this title shall not restrict a business's ability to:

(1) Comply with federal, state, or local laws.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(4) Exercise or defend legal claims.

(5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.

(6) Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

(b) The obligations imposed on businesses by Sections 1798.110 to 1798.135, inclusive, shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c) (1) This title shall not apply to any of the following:

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

(2) For purposes of this subdivision, the definitions of "medical information" and "provider of health care" in Section 56.05 shall apply and the definitions of "business associate," "covered entity," and "protected health information" in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) This title shall not apply to the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined by subdivision (d) of Section 1681a of Title 15 of the United States Code, and use of that information is limited by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

(e) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code). This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This subdivision shall not apply to Section 1798.150.

(g) Notwithstanding a business's obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to any verified consumer request may be extended by up to 90 additional days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.

(h) A business that discloses personal information to a service provider shall not be liable under this title if the service provider receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title.

(i) This title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(j) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.

(k) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.

SEC. 11.

Section 1798.150 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.150.

(a) (1) Any consumer whose nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the

misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(b) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

(c) The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

SEC. 12.

Section 1798.155 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.155.

(a) Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title.

(b) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars (\$2,500) for each violation or seven thousand five hundred dollars (\$7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General or by any district attorney, by any county counsel authorized by agreement with the district attorney in actions involving a violation of a county ordinance, by any city attorney of a city having a population in excess of 750,000, by any city attorney of any city and county, or, with the consent of the district attorney, by a city prosecutor in any city having a full-time city prosecutor, in any court of competent jurisdiction. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.

(c) Any civil penalty assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (b), shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with this title.

SEC. 13.

Section 1798.185 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.185.

Formatted: Font: 11 pt, Complex Script Font: 11 pt

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

(1) Updating as needed additional categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (o) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Updating as needed the definition of unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and additional categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to Section 1798.130.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.

(4) Establishing rules and procedures for the following:

(A) To facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information pursuant to paragraph (1) of subdivision (a) of Section 1798.145.

(B) To govern business compliance with a consumer's opt-out request.

(C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

(5) Adjusting the monetary threshold in subparagraph (A) of paragraph (1) of subdivision (c) of Section 1798.140 in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter.

(7) Establishing rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received by a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

(b) The Attorney General may adopt additional regulations as necessary to further the purposes of this title.

(c) The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.

SEC. 14.

Section 1798.192 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.192.

Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of

enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt-out of a business's sale of the consumer's personal information, or authorizing a business to sell the consumer's personal information after previously opting out.

SEC. 15.

Section 1798.196 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.196.

This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.

SEC. 16.

Section 1798.198 of the Civil Code, as added by Section 3 of Chapter 55 of the Statutes of 2018, is amended to read:

1798.198.

(a) Subject to limitation provided in subdivision (b), and in Section 1798.199, this title shall be operative January 1, 2020.

(b) This title shall become operative only if initiative measure No. 17-0039, The Consumer Right to Privacy Act of 2018, is withdrawn from the ballot pursuant to Section 9604 of the Elections Code.

SEC. 17.

Section 1798.199 is added to the Civil Code, to read:

1798.199.

Notwithstanding Section 1798.198, Section 1798.180 shall be operative on the effective date of the act adding this section.

SEC. 18.

This act is an urgency statute necessary for the immediate preservation of the public peace, health, or safety within the meaning of Article IV of the California Constitution and shall go into immediate effect. The facts constituting the necessity are:

In order to prevent the confusion created by the enactment of conflicting local laws regarding the collection and sale of personal information, it is necessary that this act take immediate effect.

Message

From: Bennett Cyphers [REDACTED]
Sent: 3/8/2019 5:04:14 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Lee Tien [REDACTED] Adam Schwartz [REDACTED]
Subject: Electronic Frontier Foundation Privacy Regulations Comments
Attachments: 2019-03-07 - EFF CCPA AG comments-resolved.docx

Please see attachment.

Sincerely,

Bennett Cyphers



EFF Comments to the California Attorney General Regarding CCPA Rulemaking March 8, 2019

The California Consumer Privacy Act (CCPA) grants consumers new rights in their relationships with businesses that collect and share their personal data. *See* Cal. Civil Code sec. 1798.100 *et seq.* The CCPA requires the California Attorney General (AG) to promulgate regulations to implement the CCPA, including rules regarding how businesses must handle consumers' requests to exercise their rights. *See* sec. 185.

These comments from the Electronic Frontier Foundation (EFF) address two aspects of the AG's rulemaking. First, the CCPA creates consumer rights to transparency about their personal information, but limits these rights to *verified* requests from consumers, and requires the AG to make rules on how business should determine which requests are sufficiently verified. *See* sec. 185(a)(7). EFF proposes rules that protect the privacy and security of consumers from fraudulent requests for their data, while ensuring that consumers can readily make bona fide requests.

Second, the CCPA creates a consumer right to opt-out¹ from the sale of their personal data, and requires the AG to make rules about how consumers may do so. *See* sec. 185(a)(4). Opt-out requests do not raise significant privacy and security hazards for consumers, so there is no need for verification of opt-out requests. Instead, we propose an automatic, World Wide Web-based opt-out mechanism: a "do not track" header sent by a user's web browser.

I. Verified consumer requests

Defining what constitutes a "verified consumer request" requires a careful balancing of two important considerations. On one hand, the regulations must ensure that consumers are readily able to exercise their CCPA rights with as many businesses as reasonably possible. On the other hand, these regulations must protect consumers from the risk of fraudulent requests for their data. While no verification process is perfect, the AG can create one that is both accessible and privacy-protective.

A. Background: CCPA provisions on verification of information requests

The CCPA's information access rules only apply when a business receives a "verifiable consumer request from a consumer." Specifically, this verification requirement applies to the CCPA's *right to know*, meaning the right of consumers to learn what personal information a business has about them. *See* Sec. 100(d), 110(b), and 115(b).² It also applies to the CCPA's

¹ Under the Privacy for All Act (A.B. 1760), consumers would have a right to opt-in consent. Businesses would need to receive a consumer's affirmative consent before selling or sharing any personal data.

² The recommendations in this section apply in particular to requests for specific pieces of personal information under 110(a)(5). Metadata about the kinds of information a business collects and shares, specified in 110(a)(1-4), is less sensitive, and therefore may be



right to portability, meaning the right of consumers to obtain a machine-readable set of their personal information. *See* Sec. 100(d).

The CCPA defines a “verifiable consumer request” to have two elements. *See* Sec. 140(y). First, it must be made by (a) a consumer, (b) a consumer on behalf of their minor child, or (c) “a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf.” Second, the request must be one “that the business can reasonably verify,” pursuant to the AG’s regulations.

The CCPA requires the AG to make rules “to govern a business’s determination that a request for information received by³ a consumer is a verifiable consumer request.” *See* Sec. 185(a)(7). The legislature intended these regulations “to further the purposes” of two of the CCPAs’ right-to-know rules (Secs. 110 and 115), and “to facilitate . . . [the] ability to obtain information” under the CCPA’s compliance rules (Sec. 130), “with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business.”

The CCPA requires different approaches to verification, depending on whether the consumer already has a password-protected account with the business responding to a request. *See* Sec. 185(a)(7). First, it should “treat[] a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request.” Second, it should “provid[e] a mechanism for a consumer who does not maintain an account with the business to request information through the business’s authentication of the consumer’s identity.”

The CCPA gives the AG significant discretion in promulgating verification rules. First, the CCPA defines “verifiable consumer requests” as those “that the business can *reasonably* verify” under the AG’s rules. *See* Sec. 140(y) (emphasis added). This rule of “reasonableness” empowers the AG to ensure sound outcomes. Second, the CCPA section requiring the AG to promulgate verification rules also requires the AG to take into account both (1) “administrative burden on consumers,” and (2) “available technology, security concerns, and the burden on the business.” *See* Sec. 185(a)(7). This empowers the AG to balance the various equities, including data security. Third, the CCPA is to be “liberally construed to effectuate its purposes” (Sec. 194), and the CCPA’s core purpose is “to further Californians’ right to privacy by giving consumers an effective way to control their personal information” (Finding i).

B. Verification of password-protected accounts

subject to less strict standards of verification by the business. While there are some situations in which it may be difficult or impossible for a business to reasonably verify a consumer request in order to disclose specific pieces of information, it should be easier for consumers to discover the types of information that are being collected about them and the categories of businesses to which their information is being sold.

³ The word “by” is apparently a typo that should be “from.”

The AG must ensure that businesses treat a consumer request as verified if it is “submitted [i] through a password-protected account maintained by the consumer with the business [ii] while the consumer is logged into the account.” *See* Sec. 185(a)(7). This language applies whether the account bears the consumer’s name or a pseudonym.

Taken in isolation, this language might rigidly be read to mean that every request that meets these two conditions is verified, with no exceptions. But as discussed above, the CCPA grants the AG significant discretion to promulgate well-balanced verification rules, which should include the power to limit as needed this mode of verification.

Exercising this power, the AG must attend to scenarios in which a wrongdoer might pretend to be a consumer logged into their password-protected account. For example, a thief might steal a consumer’s laptop, and that laptop and one of its online accounts might both be unlocked. Also, a consumer might use a shared public computer to access their password-protected account, and might neglect to sign out when they are done, in which case a thief might use the shared computer to access the account.

To prevent such security intrusions, the AG should mandate re-authentication before a user can access their data. Specifically, the AG can require a business to require that the user log out and then present their password again, before making a request. To prevent the great harm of wrongful access to a consumer’s vast trove of personal data, it is not an undue burden to require a consumer to re-input their password.

The AG should also encourage, but not require, two-factor authentication as a form of verification. Two-factor authentication (2FA) is an information security practice in which a service provider requires a user to identify themselves with both (1) something the user knows, like their password, and (2) something else the user controls, like their mobile phone or email address. Where a consumer already has 2FA enabled on an account with a business, or has voluntarily provided the business with enough information to enable 2FA, it will often be reasonable for the business to require verification by means of 2FA. This will provide additional assurance that the requester is who they say they are. Furthermore, verifying by a second factor can notify the user of fraudulent attempts to access their information if their account is compromised.

But 2FA should not be mandated across-the-board. There are recurring situations where a reasonable user might choose not to associate a “second factor” of their identity with their account. For example, whistleblowers and activists using social media could face grave harm if their pseudonymous accounts are associated with real-world identities. Likewise, survivors of spousal abuse or sex trafficking have the right to share their stories pseudonymously online without risk that their identities will be exposed. Such vulnerable people need to be able to effectively exercise their rights to know what data companies are collecting about them so, among other reasons, they can assess the threats they would face if an adversary stole their data.



Finally, because time may pass from when a person requests data to when a business makes that data accessible to the requester, the AG should require authentication not just of the person who requests data, but also of the person who later accesses it. For example, Facebook’s “download your information” feature used to take a good deal of time for processing. A user had to request that Facebook assemble all of their personal data into one place through a dialog on the website. After a delay of potentially several days, the company would send the user an email with a one-time link allowing them to access their data. If the company verified identity at the time of request but not the time of access, an imposter might have gotten access to the data.

C. Verification in other scenarios

The AG must ensure that companies “provid[e] a mechanism for a consumer who does not maintain an account with the business to request information through the business’s authentication of the consumer’s identity.” *See* Sec. 185(a)(7). This CCPA language is broad, and grants the AG an even higher level of discretion to make sound verification rules that prevent fraud while providing reasonable access.

These are examples of scenarios where the requester has no account with the business:

- a) A consumer who uses their credit card to make a purchase from a business without creating an account with that business, either online (*e.g.*, as a “guest” of a website) or offline (*e.g.*, inside a bricks-and-mortar store).
- b) A business that collects data *from* a consumer without the consumer’s knowledge or consent, either online (*e.g.*, via third-party tracking tools) or offline (*e.g.*, via visual observation).
- c) A business that collects data *about* a consumer without having any direct interaction with the consumer, by purchasing or collecting it from other parties (*e.g.*, a data broker).

If the requester has no existing account with the business, the AG should require businesses to be as certain as reasonably possible that the initiator of a request for access is, in fact, the subject of the personal data in question. There also must be oversight to ensure that businesses are not using the verification process to evade their disclosure duties. Different contexts may require somewhat different approaches.

Data associated with a real identity. The company should require proof that the requester is the consumer in question. If a consumer’s data is associated with something that indirectly ties the consumer to a real identity, like a credit card number or license plate number, the company can require that the requester to prove they are the person associated with the identifier. Likewise, if a consumer’s data is associated with a biometric identifier, the company can require the requester to prove they are the person identified.

Data associated with a communication address. Companies may assemble user data associated with an identifier that doubles as a secure means of communication, such as a mobile phone



number, email address, or social media profile. In these cases, the company can require proof that a requester has control of their communication address. This can be done, for example, by sending a confirmation link to the address.

Data associated with a device. Companies may collect data associated with a physical device, like a mobile phone or voice-activated smart device. In these cases, the company should require proof that the requester owns and controls the device before granting access to the data. Furthermore, the company should be reasonably certain that the requester was in control of the device at the time the data in question were collected. If a device is used by two or more consumers, a verified request should include the consent of all of these consumers.

Data associated with a unique device identifier. The AG should require heightened due diligence if a company verifies a requester's identity through their hardware identifier. For example, every Internet-accessible device is associated with a media access control (MAC) address. MAC addresses are persistent and difficult for an average consumer to change, which makes them attractive device identifiers.⁴ However, it also is fairly easy for sophisticated users to "spoof" them.⁵ Where applicable, companies should require proof that a device identifier has not been forged or spoofed in order to impersonate another consumer.

Data associated with online tracking tools. Some companies use cookies and other tools to track a user's online activity, without necessarily knowing the identity of the user. If the company knows the tracked user's identity, a requester can verify their identity by showing they are that known tracked user. Otherwise, if the requester can reasonably prove that they were the sole person identified by the tracking tool for the duration of the period in which data were collected, a company should consider it a verified consumer request.

Finally, the AG should ensure that any information collected by a business for the purpose of verifying a consumer request must only be used for that purpose, and should be deleted as soon as practical once that purpose is achieved. All too often, companies gather data ostensibly to protect consumer privacy, then use it to intrude on consumer privacy. For example, researchers revealed last year that Facebook collected phone numbers ostensibly for two-factor authentication, then used those phone numbers to target ads.⁶

D. Requests by agents

⁴ In fact, some companies place tiny wireless "beacons" in physical spaces to collect MAC addresses from the devices in the vicinity. This data is used by retailers, marketers, and political consultants. See <https://www.ftc.gov/news-events/blogs/techftc/2014/02/my-phone-your-service>, <https://www.latimes.com/politics/la-na-pol-campaign-tech-privacy-20190220-story.html>.

⁵ See, e.g., <https://web.archive.org/web/20120623060142/http://www.rcmp-grc.gc.ca/ncecc-cncee/factsheets-fichesdocu/macspoof-usurp-mac-eng.htm>.

⁶ See, e.g., <https://www.eff.org/deeplinks/2018/09/you-gave-facebook-your-number-security-they-used-it-ads>.

The CCPA allows consumers to make a verified request indirectly through an agent. *See* Sec. 140(y). From a data security perspective, such requests by agents present a new attack vector that data thieves might attempt to exploit. A business might err not just regarding whether a particular consumer actually has the right to access the data, but also whether that consumer actually authorized a particular agent to make the request.

Thus, the AG should mandate that when a purported agent requests data from a business on behalf of a consumer, the business must require proof that the consumer actually instructed the agent to make the request. In this context especially, the AG must attend to “security concerns.” *See* Sec. 185(a)(7).

E. Verification of deletion requests

In addition to the information requests discussed above, the CCPA empowers consumers to make deletion requests, subject to verification. *See* Sec. 105(c). Compared to information requests, deletion requests raise fewer privacy concerns, because fraudulent deletion requests will not result in adversaries wrongfully acquiring personal information about a target. However, information requests nonetheless raise significant information security concerns. Specifically, fraudulent deletion requests can harm a target by depriving them of access to their own personal information, which the target may have wanted to review, use, share, or store. Accordingly, verification of deletion requests should be like verification of information requests.

II. Consumer requests to opt-out of data sales

A. Background: the CCPA right to opt-out of sales of personal information

The CCPA provides: “(a) A consumer shall have the right, at any time, to direct a business that sells⁷ personal information about the consumer to third parties not to sell the consumer’s personal information. This right may be referred to as the right to opt-out.” *See* Sec. 120(a). The CCPA further provides that a business that has received an opt-out request from a consumer is barred from selling that consumer’s information, unless the consumer subsequently provides “express authorization” to do so. *See* Sec. 120(d).

To implement this right to opt-out of data sales, the CCPA provides that a company must:

Provide a clear and conspicuous link on the business’s Internet homepage, titled “Do Not Sell My Personal Information,” to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer’s personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer’s personal information.⁷

⁷ Under the Privacy for All Act, the right to opt-in consent would apply to both the sale and sharing of personal information.



See Sec. 135(a)(1). After an opt-out, the CCPA requires a business to wait a year before again asking the consumer for permission to sell their data. *See* Sec. 135(a)(5). If a business collects personal information from a consumer in connection with an opt-out request, the business cannot use that information for any other purpose. *See* Sec. 135(a)(6).

The CCPA charges the AG with establishing rules and procedures “to govern business compliance with a consumer’s opt-out request.” *See* Sec. 185(a)(4)(B).

B. Opt-out requests present negligible security risks

Unlike the consumer requests to businesses for personal information discussed above, which present serious risks of fraudulent requests that intrude on consumer privacy and data security, consumer requests to businesses to opt-out of sales present little or no privacy or security risk. If an adversary wrongly opted a consumer out of sales of their data, the adversary would gain nothing of value. And when the wrongdoing was uncovered, the consumer could easily opt back in to sales of their data, if they wanted it. Thus, the CCPA does not require companies to verify consumer requests to opt-out from sales of their personal information.

C. Opt-out requests via the World Wide Web

The CCPA clearly requires a business to maintain a web page to handle consumer opt-out requests, and bars a business from requiring a consumer to create an account in order to make an opt-out request.

Due to the vast diversity of businesses covered by the CCPA, the average California consumer is likely to interact with hundreds or even thousands of businesses that collect and maintain personal information about them, directly or indirectly.

Many consumers will reasonably decide that they want to opt-out of the sale of their personal information *by default for all businesses they interact with*. They should be able to use automatic tools to assist them in doing so.

Fortunately, a way to do so already exists: the Do Not Track (DNT) system. It combines a technology (a browsing header that announces the user prefers not to be tracked online) with a policy framework (how companies should respond to that signal).⁸

EFF proposes that the AG require any business that interacts with consumers directly over the Internet using HTTP or HTTPS to treat an HTTP request with a DNT header set to 1 as a binding request to opt-out of data collection.

The DNT header is already widely supported by most major web browsers, including Google Chrome, Mozilla Firefox, and Opera. This will allow for immediate and widespread use of DNT as a tool for making opt-out requests. Users will be able to configure their browsers, either by

⁸ *See, e.g.,* <https://www.eff.org/issues/do-not-track>.



themselves or with privacy-preserving extensions like EFF's Privacy Badger, to exercise their CCPA right to opt-out from data sales with all businesses they interact with online.

There should be different DNT rules depending on whether the user is logged-in or otherwise verified as the controller of an account with the business. If so, the business should be required to consider the DNT header as an affirmative request to opt-out of *all* sales of the consumer's data until the consumer decides to opt back in. If not, the business should consider it a request to opt-out only from the sale of data collected in the current session.

Conclusion

EFF thanks the California Attorney General's Office for its consideration of these comments on CCPA rulemaking concerning (1) how to verify consumer requests for personal information, and (2) how to structure consumer requests to opt-out of sales of personal information.

Respectfully,

Bennett Cyphers, Staff Technologist, [REDACTED]

Adam Schwartz, Senior Staff Attorney, [REDACTED]

Message

From: Kelsie Nagele [REDACTED]
Sent: 1/18/2019 4:51:34 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Sonia Gibson [REDACTED]
Subject: Encore Capital Group Comments on CCPA
Attachments: Encore Capital Group Comments__CCPA 2018.pdf

Good Afternoon,

Please find attached Encore Capital Group's comments on the California Consumer Privacy Act. Feel free to contact us with any questions or for further information.

Thank you,

Kelsie Nagele



Kelsie Nagele, Manager of Public Policy

3111 Camino Del Rio N., Ste. 1300

San Diego, CA 92108



The information contained in this e-mail message, including attachments (collectively referred to as "Information"), is strictly confidential and proprietary, and/or privileged. This information is intended only for the personal and confidential use of the recipient(s) named above. The Information contained in this email should not be replicated or disclosed to any persons other than the intended recipient(s). If the reader of this message is not the intended recipient or an agent responsible for delivering it to the intended recipient, you are hereby notified that you have received this document in error and that any review, dissemination, distribution, or reproduction of this Information is strictly prohibited. If you have received this communication in error, please notify the sender immediately by e-mail, or by telephone at (877) 445-4581, and delete the original message.

The information contained in this e-mail message, including attachments (collectively referred to as "Information"), is strictly confidential and proprietary, and/or privileged. This information is intended only for the personal and confidential use of the recipient(s) named above. The Information contained in this email should not be replicated or disclosed to any persons other than the intended recipient(s). If the reader of this message is not the intended recipient or an agent responsible for delivering it to the intended recipient, you are hereby notified that you have received this document in error and that any review, dissemination, distribution, or reproduction of this Information is strictly prohibited. If you have received this communication in error, please notify the sender immediately by e-mail, or by telephone at (877) 445-4581, and delete the original message.



January 18, 2018

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Submitted via email to: PrivacyRegulations@doj.ca.gov

RE: Comments regarding the California Consumer Privacy Act of 2018

To Whom It May Concern:

On behalf of Encore Capital Group and its wholly-owned subsidiaries (collectively "Encore"), I am writing to comment on the recently passed California Consumer Privacy Act ("the Act"). We appreciate the state's desire to protect consumers and establish clear standards for businesses. To that end, we have several suggestions regarding how the Act could be improved via rulemaking. Our concerns are focused on clarity, which will allow both consumers and businesses to agree on expectations, avoid costly, time consuming litigation, and promote transparency as was intended by the Act.

By way of background, Encore is a publicly traded company that has provided over 60 years of service to consumers in California and throughout the nation. Purchasing primarily charged-off credit card debt, we currently have accounts with over 4 million California residents. We offer flexible repayment plans, do not collect any fees or interest on new accounts, and often discount a significant amount of the total debt owed. In 2018, we forgave over \$34 million in debt owed by California residents.

Our comments and suggestions regarding the Act are outlined below.

Definition of "Personal Information"

Firstly, the Act could benefit greatly from clarification regarding the definition of "personal information." The current language is so broad that it could be read to include almost any type of information. It includes in part, "any information that identifies, relates to, describes, or is capable of being associated with, a particular individual." It even goes so far as to encompass (but is not limited to) "thermal" and "olfactory" information about an individual. In fact, the only explicit limitation on the definition is that publicly available or deidentified information is not included.

This broad definition may at first seem like a positive, because in theory it provides a large scope of protection for consumers. However, without a clear and unambiguous definition, consumers will not be able to effectively exercise the rights the Act is intended to provide to them. The Act clearly states that the intent of the legislation is to ensure the right of Californians to know what



personal information is being collected about them; to know whether their personal information is sold or disclosed and to whom; to say no to the sale of personal information; to access their personal information; and to equal service and price, even if they exercise their privacy rights. When uncertainty exists around what information is covered, businesses will have to make difficult decisions about various types of information and risk unnecessary costs or inadvertent violation of the Act which will inevitably result in litigation. Similarly, consumers will be unclear on what information is covered by the Act and therefore what information they can control, request, delete etc. The potential for differing opinions and expectations on the part of businesses and consumers makes the Act a ripe source for superfluous litigation, much of which could be avoided if the definition of personal information is clarified. To that end, we ask that “personal information” be sufficiently defined so as to avoid widely disparate interpretations of its meaning.

Gramm-Leach-Bliley Act (GLBA) Exemption

The scope and definition of “personal information” is especially impactful when it comes to intended exemptions for certain businesses and types of information. Specifically, §1798.145(e) states, “This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act...” This adds another layer of ambiguity to the “personal information” definition. What is personal information “collected, processed, sold, or disclosed pursuant to” the GLBA? Can certain types of information be either exempt or subject to the act depending on context, or do blanket rules apply? One way to avoid confusion regarding this section would be to specify that institutions governed by the GLBA are exempt from the Act. Another possibility would be to more specifically explain what “information collected, processed, sold, or disclosed pursuant” to the GLBA is meant to encompass. Currently, companies such as Encore that are subject to the GLBA, have the difficult task of determining whether all or only some of the information they collect is considered under the Act to be “collected, processed, sold, or disclosed pursuant to” the GLBA given that “personal information” is defined differently in the GLBA versus the Act.

Disclosures

§1798.185(a)(6) of the Act specifies that guidance, “Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer...” Because the Act requires covered businesses to provide disclosures to consumers before collecting personal information, it would be helpful to have model forms to reference in order to develop disclosure policies and procedures that meet the requirements of the Act.



Sale and Disclosure to Third Parties

One admirable aspect of the Act is that it allows consumers to “opt-out” of the sale of their personal information. We are supportive of the idea that consumers should have control over sensitive information. It is clear that §1798.120(a) applies to the sale of personal information, however defined. We would appreciate language that clarifies the common-sense intent behind this section. It is obvious that this section should apply to companies who want to sell consumer information for profit. However, it is important to ensure that the many businesses and industries that engage in transactions in which the exchange of consumer information is ancillary to a transaction or sale of an asset—such as mergers, mortgage lending etc. —are able to continue business as usual with regard to the underlying transaction or sale. Any ambiguity in the Act that could be interpreted to allow consumers to “opt-out” of transactions or sale of assets because their personal information will be exchanged could have a crippling effect on various industries and the economy. Clearly, the prohibition of all sales and transactions in which the exchange of personal information is ancillary was not the intent of the Act, and we would appreciate language that makes this even more evident.

Definition of “Single, One-time Transaction”

§1798.100(e) states, “This section shall not require a business to retain any personal information collected for a single one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.” Clarification on the meaning of “single, one-time transaction” is needed here. When we receive personal information in connection with a one-time transaction, our policy is to purge that information so as not to create any unnecessary risks of breach of consumer information. This section supports our policy but leaves ambiguity as to what constitutes a single, one-time transaction. It also suggests that companies do have an obligation to retain information that is not part of a single, one-time transaction. This inference in particular is in need of clarification. Does our obligation to retain personal information extend to cookies or other digital information? This is just one more area in which clarification will ensure businesses are meeting requirements and protecting consumers.

Definition of “Manifestly Unfounded or Excessive”

§1798.145(g)(3) states, “If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.”

We support the intent behind this section and appreciate the recognition that it is neither necessary or prudent for businesses to have to respond to excessive or unfounded requests from



consumers. At the same time, it is important that clear standards for legitimate responses are established as is done in §1798.130(b). What is less clear, is what actually constitutes “manifestly unfounded or excessive” requests. The section provides one useful qualification by implying that repetitive requests would be considered excessive and would not need to be answered so long as the consumer is notified of the reason for the refusal of their requests. However, it is not clear how many requests are needed before a consumer’s attempts would be considered so repetitive as to constitute manifestly unfounded or excessive requests. Further guidance is needed so that businesses can adequately comply with this section without violating consumer rights or incurring unnecessary costs.

Exceptions to the Right to Delete Personal Information

§1798.105(d) states, “A business or service provider shall not be required to comply with a consumer’s request to delete the consumer’s personal information if it is necessary for the business or service provider to maintain the consumer’s personal information” if one of several reasons applies.

Firstly, §1798.105(d)(1) provides that deletion is not required for personal information when it was collected in order to complete a transaction, provide a good or service requested by the consumer, or if maintenance of the personal information is reasonably anticipated within the context of a business’ ongoing business relationship with the consumer. It is unclear whether this is intended to apply to digital marketing information like IP addresses, interactions with applications, websites or advertisements etc. This question is also relevant to §1798.105(d)(9) which provides for the maintenance of personal information for internal use in a manner that is compatible with the context in which the consumer provided the information. Again, clarification on what type of personal information these sections are intended to encompass would be helpful.

Repetition and Drafting Errors

There are several places in the Act where language appears to be unintentionally repetitive. Eliminating the duplication in these sections will ensure that there is no confusion as to the intent of the Act. For example, §1798.110(a) includes some repetition of §1798.100(a). It appears to us that the repetition does not point to any additional qualifications other than those that are deducible from the plain language of the text, but removing the repetition would ensure that there is no question in this regard.

Finally, §1798.110(c)(5) requires that specific pieces of information collected about a consumer be disclosed prior to the collection of the information. It appears that this may be a drafting error since it is technically impossible to disclose individual pieces of information our company may collect prior to collection. The other requirements, such as the need to disclose categories of information, sources, and business purposes for which businesses will use the information prior to collection, make sense and could be operationalized. So, we recommend that either the



§1798.110(c)(5) requirement be removed or clarified, since we are unable to disclose which specific pieces of information are collected *prior* to collection.

Conclusion

Thank you for the opportunity to comment on this very important piece of legislation. We applaud the State's intention of protecting consumers and making business standards clear. With additional clarification we believe this Act can serve California well.

If you have any questions or would like more information on Encore's comments, please do not hesitate to contact me.

Sincerely,

Sonia Gibson
Encore Capital Group
Head of National Government Affairs



Message

From: Tom Foulkes [REDACTED]
Sent: 3/8/2019 12:42:11 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Tim Lynch [REDACTED] Michael Warnecke [REDACTED]
Subject: Entertainment Software Association CCPA Comments
Attachments: ESA Written CCPA Comments.pdf

The Entertainment Software Association (ESA) submits the attached comments in connection with the Attorney General's Office's pre-rulemaking on the California Consumer Privacy Act of 2018 (CCPA).

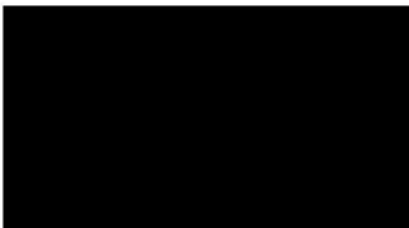
Tom Foulkes

Vice President, State Government Affairs

Entertainment Software Association

601 Massachusetts Avenue NW, Suite 300

Washington, DC 20001





March 8, 2019

Via Email to PrivacyRegulations@doj.ca.gov

California Department of Justice
Attn: Privacy Regulations Coordinator
300 S. Spring St., Los Angeles, CA 90013

Re: Comments of the ESA on the CCPA Pre-rulemaking

Dear Privacy Regulations Coordinator:

The Entertainment Software Association ("ESA") submits these comments in connection with the Attorney General's Office's pre-rulemaking on the California Consumer Privacy Act of 2018 ("CCPA").¹ ESA shares the goal of providing consumers transparency and choice over how personal information is processed, while also avoiding interpretations that would unintentionally harm consumers.

ESA's members agree with the California Legislature's finding that it "is possible for businesses both to respect consumers' privacy and provide a high level [of] transparency to their business practices."² Indeed, ESA's members have long provided consumers important information about how their information is processed and have offered choices over this processing (including, for example, over their children's information).

We request that the Attorney General adopt rules or make clarifications in *six* areas to ensure that the CCPA is not applied in ways that unintentionally could harm consumers. These six areas include:

1. Preventing individuals from abusing rights under the CCPA to further harmful conduct;
2. Encouraging businesses to tailor their verification processes and communications channels based on reasonable industry practices and consumer expectations;
3. Clarifying that the non-discrimination provision does not restrict ad-supported and similar video game offerings;
4. Specifying that businesses may de-identify or aggregate data in response to consumer requests;
5. Clarifying the meaning of the Act's requirement for "explicit notice"; and
6. Clarifying the definition of "sale."

¹ ESA is the U.S. association for companies that publish computer and video games for video game consoles, handheld devices, personal computers, and the internet. There are over 900 video game companies in the State of California.

² CCPA, Section 2(h).

We detail each of these requests in the following sections.

I. The Attorney General Should Establish Exceptions That Prevent Individuals From Using the CCPA To Infringe IP Rights Or Engage In Other Misconduct.

Section 1798.185(a)(3) requires the Attorney General to “establish any exceptions necessary to comply with state or federal law, including ... those relating to trade secrets and intellectual property rights.” As explained below, ESA requests that the Attorney General use this authority to establish exceptions that prevent individuals from using the CCPA to infringe intellectual property rights or engage in other misconduct.

As currently drafted, the CCPA does not clearly permit businesses to protect their trade secrets and proprietary technology. For example, many video game publishers utilize proprietary techniques to detect and prevent cheating, fraud, infringement of intellectual property, and similar misconduct within the video game. These techniques involve processing certain personal information, such as information regarding the individual’s video game equipment (mouse, keyboard, controller, etc.) and his/her interaction with a game including game play patterns and inferences regarding the person’s predispositions or behavior, to assess whether the player is cheating or otherwise engaging in harmful conduct. In our members’ experience, however, a player whose account has been suspended for cheating might use a data access request to try to determine what specific types of patterns, interactions, predispositions, behaviors, and other actions enabled the publisher to detect the misconduct and suspend the account. In this manner, a consumer can try to use the data access right to, in essence, uncover the business’s trade secrets and proprietary technology to try to evade the anti-cheat system and similar monitoring in the future. It should never be permissible for a consumer to hijack the consumer rights in a manner that would help further harmful conduct.

Similarly, the CCPA does not explicitly protect a business’ ability to prevent harassment, bullying, fraud, abuse, or other malicious activity. For example, video game publishers often post terms and codes of conduct prohibiting players from harassing or bullying other players. The CCPA as written, however, would appear to permit one roommate to bully another roommate by requesting access to and potentially deleting game play data for the entire household. As long as the conduct does not rise to the level of being unlawful, the CCPA potentially could be interpreted to require the video game publisher to comply with the request. The CCPA therefore leaves businesses vulnerable to bad actors, while unintentionally stripping businesses of their ability to protect consumers.

To avoid these unintended consequences, ESA encourages the Attorney General to issue the following regulation:

The obligations imposed on businesses by this title do not restrict a business's ability to: collect, use, retain, authenticate, process, or disclose personal information in order to (i) exercise, defend, or protect against legal claims; (ii) protect against or prevent fraud or verify

*identity; or (iii) protect against security incidents, theft of intellectual property, or other malicious, deceptive, harassing, or illegal activity or violations of applicable terms.*³

II. The Attorney General Should Encourage Businesses To Tailor Their Verification Processes And Communications Channels Based On Reasonable Industry Practices And Consumer Expectations.

Under Section 1798.185(a)(7), the Attorney General is responsible for issuing regulations governing the business's process for determining whether a consumer request is a "verifiable consumer request" for CCPA purposes. ESA requests that the Attorney General's Office take measures to ensure that data access requests do not become a new cyberattack vector through which hackers, phishers, and other malicious actors can gain unauthorized access to personal information. This includes clarifying that a toll-free telephone number is not required when it would prevent the business from verifying the consumer's request.

ESA's members rely on a variety of existing means to communicate with consumers and to verify their identities. The chosen method depends on a variety of circumstances, including the consumer's expectations and the sensitivity of the information being transmitted. In the video game industry, for example, businesses and consumers might communicate through real-time text or voice chat, sometimes directly through the game, or through game accounts that require the player to be authenticated. Players are accustomed to submitting requests through accounts, particularly when those requests relate to sensitive information that should not be transmitted freely (*e.g.*, credit card information related to prior in-game transactions). This layer of authentication is an important security measure to ensure that the person making the request is the person who is actually authorized to use the account.

In order to protect personal data from unnecessary security risks, the Attorney General's Office should provide businesses the flexibility to use any reasonable method available to receive and process data rights requests. This will help ensure that consumers are able to submit requests to exercise their rights in the manner in which they are accustomed to communicating with the company and which are appropriately secure for the types of information being requested.

Specifically, ESA requests that the Attorney General clarify that a business must provide consumers with a toll-free telephone number and a website address to exercise their rights *only* if those are the methods of communication that the consumer typically uses to communicate with the business and such mechanism is reasonably secure based on the nature of the request and the type of personal information requested. In addition, the Attorney General should clarify that a business may require a consumer to authenticate an account to verify his or her identity if the

³ Similar language should be added in Section § 1798.140(d) to clarify, for example, that the definition of "business purposes" includes all activities conducted in order to (1) exercise, defend, or protect against legal claims; (2) protect against or prevent fraud or verify identity; and (3) protect against security incidents, theft of intellectual property, or other malicious, deceptive, harassing, or illegal activity or violations of applicable terms.

business usually communicates with users through such accounts. Finally, the Attorney General should adopt the following regulation:

The business must provide the consumer at least two reasonable methods, based on available technology, for the consumer to exercise the rights afforded under the Act.

The business must establish a reasonable method, based on available technology and the sensitivity of the request, for verifying a consumer's identity within a reasonable period of time for purposes of fulfilling consumers' requests to exercise their rights under this statute.

III. The Attorney General Should Clarify That The Non-Discrimination Provision Does Not Restrict Ad-Supported Video Game Offerings.

The California Legislature empowered the Attorney General to adopt all "additional regulations as necessary to further the purposes of this title." § 1798.185(a)(7). ESA urges the Attorney General to use this authority to clarify that the CCPA's non-discrimination provision does not prevent video game publishers from offering video game content through ad-supported and similar business models.

Section § 1798.125, if interpreted and applied strictly, could disrupt the offering of video games through ad-supported and similarly innovative business models that have made it possible for a broad swath of players to access video games for little or no cost. Modern game development and publishing is heavily dependent on data analysis and, to some extent, customized advertising, especially in the context of mobile games. This data analysis typically requires the collection and processing of IP addresses, cookie IDs, and similar device identifiers to determine, for example, what features of the game are most popular, whether there are any errors that need to be corrected, and what features could be further improved. Being able to determine the types of audiences that are most likely to enjoy the game or an advertising partner's products and services, and to deliver customized advertising to the player, is a critical aspect of this process because this analysis helps the business more effectively advertise to the demographic of people who are most likely to actually want to play the game or want to use the particular products or services.

Many game publishers depend upon this data processing and advertising to be able to effectively develop, publish, and improve their games. Therefore, the value to the business of the data processing and advertising is significant. But because this processing doesn't involve the sale of personal information and the benefits to the company are indirect and difficult to measure, it may be challenging for the business to demonstrate precisely and empirically that any difference in price or service levels that could result from (for example) a consumer requesting deletion of her data is directly related to the value of that consumer's data.

To ensure that video game players can continue to benefit from broad access to these ad-supported games and similarly innovative business models, ESA encourages the Attorney General to clarify the meaning and scope of the non-discrimination provision and to state

explicitly that the provision will not be interpreted to prevent ad-supported and similar business models.

IV. The Attorney General Should Specify That Businesses May De-Identify or Aggregate Data in Response to Consumer Requests.

The CCPA gives consumers the right to request that a business delete their personal information. § 1798.105. However, the statute does not explicitly define “deletion” or specify what a business must do to comply with such a request.

Guidance on this issue should be developed by reference to the exemption for de-identified or aggregated data. § 1798.145(a)(5). For example, the statutory text explains that data is “de-identified” if it “cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer” and the business takes certain technical and administrative measures to prevent the re-identification or release of the de-identified data. In other words, deidentified data is not personal information.

By exempting deidentified and aggregated data from the statute, the legislature plainly indicated that de-identification and aggregation of data is as robust of a measure for compliance as deletion. In both scenarios, the consumer will no longer be associated with the data remaining within a business’ systems and therefore the individual’s privacy interests have been sufficiently addressed.

As explained above, the Attorney General can adopt any “regulations as necessary to further the purposes of this title.” Accordingly, in order to provide greater clarity and meaning to the data deletion right, ESA requests that the AG’s regulations clarify that:

A business “deletes” personal information when it (i) erases the personal information from its systems; (ii) deidentifies the information; or (iii) aggregates the information.

V. The Attorney General Should Clarify the “Explicit Notice” Requirement.

Section 1798.185(a)(6) requires the Attorney General to issue rules that are “necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer.” ESA requests that the Attorney General act under this authority to clarify the requirement in § 1798.115(d), which requires “explicit notice” before third parties may re-sell PI.

Section 1798.115(d) does not specify what constitutes “explicit notice.” However, other parts of the statute do. In particular, Section 1798.110(c), which describes the information that a business must disclose to the consumer through an online privacy statement, appears to be most relevant under these circumstances. Because this privacy disclosure is made at or before the point of collection, and regardless of whether the consumer requests it, this is the most explicit privacy notice that the business makes under the statute. Consequently, the Attorney General

should clarify that the “explicit notice” standard is met if the re-sale is disclosed in the online privacy statement at the time the personal information was collected.

Moreover, to ensure that the consumer will receive this explicit notice in a manner that is effective and easily understood by the average consumer, the Attorney General should clarify that the party who has the direct relationship with the consumer (and not any downstream third parties within the ecosystem who might receive a copy of the personal information) should be responsible for providing the consumer the explicit notice that the personal information may be resold. This interpretation not only provides the consumer useful “just-in-time” notice at the time that is most actionable for the consumer (*i.e.*, at the time the information is collected), but it also is a practical necessity since consumers often will have no direct relationship with the downstream third-party and third parties need not be identified by name under the CCPA.

Accordingly, ESA asks that the Attorney General enact the following clarifications:

The party responsible for providing a consumer with explicit notice, and the opportunity to opt out, of a third party's sale of certain data is the party with the direct relationship with the consumer from which that data originated.

A party provides “explicit notice” when it provides notice consistent with § 1798.110(c).

VI. The Attorney General Should Clarify the Definition of “Sale.”

Section 1798.185(a)(4) requires the Attorney General to issue regulations “to facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information.” In order to regulate requests to opt out of the sale of personal information, it must be clear what constitutes a “sale.” Therefore, the Attorney General should clarify the meaning of “sale” under the CCPA consistent with this statutory authority.

Specifically, the Attorney General should clarify the meaning of “monetary consideration or other valuable consideration.” Video game publishers and console manufacturers must disclose personal information to each other and certain other vendors to (for example) facilitate game play, conduct analytics for research and product improvements, personalize content, and deliver advertising to the consumer. Clearly, however, the legislature did not intend to treat these disclosures of personal information as “sales,” notwithstanding the fact that such data sharing is necessary to perform the services and that one or both parties may incidentally benefit from such disclosures. Such an interpretation would, in essence, impose an opt-out right on data disclosures generally, rather than those disclosures that have a specific, and narrow, legal effect.

Notably, the California legislature rejected an approach that would have applied the opt-out right broadly to any data disclosure. The ballot initiative defined “sale” to include “sharing orally, in writing, or by electronic or other means, a consumer’s personal information with a third party, whether for valuable consideration or for no consideration, for the third party’s commercial purposes.” CCPA Ballot Initiative § 1798.106(q)(1)(B). The legislature struck that

language in passing the CCPA, signaling its intent to distinguish between direct sales of data and mere incidental disclosures of data that are needed to facilitate the performance of the bargained-for exchange of services.

Importantly, just because data is exchanged in connection with the performance of a contract does not mean that the data itself constitutes the consideration. For there to be consideration, "a performance or a return promise must be bargained for... A performance or return promise is bargained for if it is sought by the promisor in exchange for his promise and is given by the promisee in exchange for that promise." Restatement (Second) of Contracts § 71 (1981). The California "Supreme Court authoritatively adopted the concept of consideration as a bargained for exchange." *Jara v. Suprema Meats, Inc.*, 121 Cal. App. 4th 1238, 1248, 18 Cal. Rptr. 3d 187, 194 (2004) (considering whether a purported contract between shareholders was a gratuitous promise that lacked consideration).

In many commercial relationships, the data is not the bargained-for exchange. To the contrary, an advertiser might pay money to an advertising partner in exchange for the partner providing more effective ad placement (in which case the bargained-for exchange is money for services) or the parties could alternatively enter into a co-marketing agreement (in which case the bargained-for exchange is services for services). In neither of these circumstances is the data the consideration, because the data is not itself exchanged directly for money or a monetary equivalent (such as a loan or office).

Accordingly, ESA requests that the Attorney General clarify the meaning of "other valuable consideration" as follows:

A business "sells" personal information under this title only when it discloses consumers' personal information directly in exchange for any money, loan, or office, for himself or any other person. The business must receive the valuable consideration from the business or third party that receives the personal information.

* * *

ESA looks forward to working with the Attorney General's Office as it considers draft regulations. Please let us know if you have any questions about our recommendations.

Sincerely,



Stanley Pierre-Louis
Interim President & CEO
Entertainment Software Association

Message

From: Shelly Gensmer [REDACTED]
Sent: 3/7/2019 12:00:55 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: ERC's Formal Response and Comments regarding CCPA
Attachments: CCPA Letter_ERC.docx
Importance: High

Dear Sirs or Madams,

Please find attached is a letter addressing my company's comments and concerns regarding the California Consumer Privacy Act.

It is our hope that the Debt Collection and Asset Recovery industry can gain clarity and guidance on the Act in order to ensure we are compliant.

We look forward to working with California's Privacy Regulations Coordinator, along with our peers, to finding the answers we so badly need.

Thank you in advance for your time and consideration.

I am available by email or phone if you have any questions for me or for ERC.

Kindest Regards,

Shelly Gensmer | Vice President of Legal and Compliance, CCCO

ERC

8014 Bayberry Rd | Jacksonville | FL | 32256

[REDACTED]
ercbpo.com



This message and any attachments are intended only for the use of the addressee and may contain information that is privileged and confidential. If the reader of the message is not the intended recipient, or the authorized agent of the intended recipient, you are hereby notified that any dissemination of this communication is strictly prohibited. If you have received this communication in error, please notify ERC immediately by telephone at (800) 617-0049 and delete the message and any attachments from your system. Thank you for your cooperation.



From: Enhanced Recovery Company

Address: 8014 Bayberry Rd Jacksonville, FL 32217.

ATTN: Privacy Regulations Coordinator, 300 S. Spring St., Los Angeles, CA 90013.

To whom this may concern,

ERC is a debt collection agency that meets the threshold requirements of a company subjected to the California Consumer Privacy Act (CCPA) going into effect January 2020. Because it is clear the CCPA was not designed or written with our industry in mind, ERC has a list of concerns regarding provisions of the CCPA and its effect on the Debt Collection industry.

We first seek clarification on the definition of a 'consumer'. The CCPA's definition of consumer is broader than the traditional definition of consumer, that existing laws in California use as applied to persons who a business serves. The already existing California Rosenthal Fair Debt Collection Practices Act as well as the Fair Debt Collections Practices Act (FDCPA) which governs the debt collection industry defines consumer as any natural person obligated or allegedly obligated to pay any debt. The CCPA, on the other hand, defines consumer as a natural person who is a resident of California.

The definition of consumer provided by the CCPA seemingly refers to a data subject. Clarification on whether the CCPA's definition of consumer is actually any person whose personal data is being collected, held, or processed would assist industries like ours in becoming compliant as it would clarify whether the definition would include employees of a business as well.

Communications are a large portion of lawsuits that affect the debt collection industry. The CCPA provides that a consumer may request access to personal information a business has collected about them and a business must disclose the requested information free of charge within 45 days of the receipt of a consumer's request. Standardizing communications by providing businesses subjected to CCPA compliance with safe harbor language will allow a safe way to notify consumers, per disclosure requirements, without communications being found as "false, deceptive, or misleading" per industry and Federal Debt Collection Practices Act ("FDCPA") standards.

Privacy and confidentiality are a business's top priority in the financial service industry. Specifically, in the debt collection industry, the FDCPA provides that a collector must not disclose the existence of a debt to a third party. The California Rosenthal Fair Debt Collection's Protections Practices Act is even more restrictive providing that an agency must obtain written consent before speaking with a third- party. Fulfilling CCPA requests will put businesses at a high risk of third-party disclosure. There are currently no provisions regarding requests received from agents of the consumer and verification of a principal agency relationship whether it be parent guardian, attorney client, or spouse just as examples.

The debt collection industry would also benefit from clarification regarding verifications. The CCPA allots for letters or email verifications. Requiring businesses to disclose the requested information free of charge, may come at a significant cost to businesses depending on the number of requests received. Although, industry executives seek to ideally reduce postage expenses, and have the option to provide verifications via email, there are third party disclosure concerns specifically regarding emails used in consumer communication. Debt collection agencies have a duty to protect consumers against inadvertently sharing their information with a third party. Providing verifications per consumer request through emails creates the risk that a consumer may provide a work email or shared email address which would give rise to third-party disclosures.

When providing any sort of deletion in compliance with a request, ERC seeks clarification on a business's ability to retain records that show they have responded to a request for deletion, along with a record retention period.

The CCPA private right of action is amended under SB-1121 to clarify a consumer may bring action only for a business's alleged failure to "implement and maintain reasonable security procedures and practices" that result in a data breach (CCPA § 1798.150 (c)). Additionally, § 1798.155(b) allows the AG to impose up to \$2,500 for unintentional violations, and up to \$7,500 for intentional violations. How does a business prove it implemented "reasonable" security practices and procedures? Moreover, what defines intentional versus unintentional? This broad definition opens a very large platform for interpretation and leaves businesses without guidance.

SB-1121 amends CCPA § 1798.150(k) which stated a business must disclose on its website or in its privacy policy a consumer's right to request deletion of his or her personal information, to now require businesses to make this disclosure "in a form that is reasonably accessible to consumers". The debt collection industry communicates with consumers through mail and telephone. ERC, like most debt collectors in our industry, also uses its website to facilitate communications and account maintenance. Our industry seeks clarification on what is to be considered a form that is reasonably accessible to consumers.

Lastly, we suggest California provide a platform for businesses to ensure a structured and efficient means for CCPA compliance, in the form of an official CCPA certification. Certification can serve as marketing tools to encourage CCPA Compliance. CCPA certification will also assist businesses in onboarding third party service providers to ensure businesses are dealing with a trusted third party.

Thank you for allowing a forum where businesses can provide feedback. It is our hope that the concerns of the debt collection industry are given serious consideration when executing any future comments or amendments to the CCPA.

Kind Regards,

Michelle Gensmer
Senior Vice President of Legal and Compliance



Message

From: Ari Paparo [REDACTED]
Sent: 1/3/2019 6:32:15 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Feedback on privacy regulations
Flag: Follow up

Hello, I am a practitioner in the ad tech space and CEO of Beeswax.com. As background I am an expert in the practices of ad tech and was highly involved in the preparation for GDPR.

From my experience with GDPR, the largest problems with that law, and the areas where California could make improvements, is in the overly broad definitions of "Personal Data" under the European laws. By including anonymous cookies, IP addresses, and pseudo-anonymized hashed identities as Personal Data GDPR's scope became highly intrusive to marketing and advertising businesses and radically increased the costs and complexity of compliance. Further, the real consumer privacy risks around an anonymous cookie are an order of magnitude smaller than what any reasonable person would actually consider "personal" such as email, home address, etc.

Further, while the primary concern of the government in this process is to protect the consumer, I would hope consideration would be made of the commercial impact of this law. In the case of GDPR, the law as written threw many legitimate business practices relating to "real time bidding" into chaos, with zero benefit to consumer privacy. In particular, the real time bidding ecosystem relies on the "syncing" of IDs between buyers and sellers of advertising, and this process was not contemplated properly in GDPR rule making.

In sum, I believe strongly in consumer privacy and believe that strong legislation is necessary. However, the definition of "personal data" should reflect data that is actually personal and that has negative consequences of being disclosed. No consumer has ever been harmed by an anonymous cookie and these are fundamental to the way the Internet works.

--

Ari Paparo
Beeswax.com

Message

From: Christopher Mohr [REDACTED]
Sent: 2/15/2019 1:29:37 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Christopher Mohr [REDACTED]
Subject: First Amendment Problems with the CCPA
Attachments: SIIA Letter to General Becerra.pdf; Memo re CCPA (FINAL).pdf
Flag: Follow up

Please see the attached materials.

Sincerely,

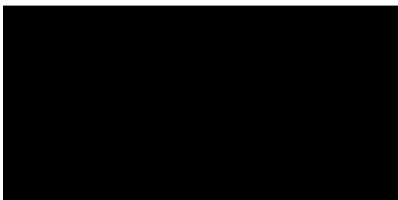
Christopher A. Mohr

VP for Intellectual Property and General Counsel

Software & Information Industry Association

1090 Vermont Ave. NW, Ste. 600

Washington, D.C. 20016



February 15, 2019

VIA EMAIL

Hon. Xavier Becerra
Attorney General
State of California
1300 I Street
Sacramento, CA 95814

**Re: First Amendment Issues with the CCPA and Public Domain
Information**

Dear General Becerra:

I am writing on behalf of the Software and Information Industry Association, a trade association located in Washington, D.C. to convey our First Amendment concerns with the CCPA's treatment of publicly available information and to request a meeting to go through it.

SIIA is the principal trade association of the software and information industries and represents over 800 companies that develop and market software and digital content for business, education, consumers, the Internet, and entertainment. SIIA's members range from start-up firms to some of the largest and most recognizable corporations in the world. They include software publishers, financial trading and investment services, and educational, specialized and business-to-business publishers. They also include a number of firms who use public domain information to track down witnesses, enforce child support payments, and prevent a variety of financial crimes.

SIIA supports privacy as a fundamental value—one essential to individual autonomy and a functioning democracy. California has a legitimate interest in protecting the privacy of its citizens, one we do not gainsay. Nonetheless, we wish to voice our concerns over the CCPA's treatment of "personal information" and its collision with equally important values: those of the First Amendment.

As explained in more detail in the attached memorandum from outside counsel at Mayer Brown, the CCPA's treatment of public domain information creates potentially fatal problems under the First Amendment. First, the law attempts to pull certain information out of the public domain on a content-discriminatory basis: it bars some people who possess lawfully acquired, accurate public-domain information from disseminating it. Second, the statute has vagueness problems: it is difficult if not impossible for a speaker to know *ex ante* whether his communication is "compatible with the purpose" for which a particular piece of information is maintained. And third, the legislation discriminates among speakers: it allows certain entities to transmit personal information, and compels others to be silent.

Many of the CCPA's First Amendment problems could be ameliorated by excluding public domain information from the definition of personal information. While we understand that you are tasked with defending the constitutionality of state laws, we would appreciate the opportunity to discuss these issues with you in the context of supporting an appropriate legislative amendment.

Thank you for your consideration of our views.

Respectfully submitted,



Christopher A. Mohr

Vice President for Intellectual Property
and General Counsel

MEMORANDUM

Date: January 24, 2019

To: Christopher Mohr
General Counsel
Software and Information Industry
Association

From: Andrew J. Pincus
Miriam R. Nemetz
Eugene Volokh

Subject: Invalidity Under The First Amendment Of
The Restrictions On Dissemination Of
Accurate, Publicly Available Information
Contained In The California Consumer
Privacy Act of 2018

The California Consumer Privacy Act of 2018 (CCPA) violates settled First Amendment principles by restricting the dissemination of accurate, publicly available information. If the Act is not amended to eliminate these unconstitutional speech restrictions, it is highly likely to be invalidated in court.¹

Under the CCPA, California residents will be able to block businesses from selling “personal information” relating to them. The Act’s definition of “personal information” is not limited to private, sensitive data—it also encompasses information obtained from publicly available sources, such as information released to the public by government agencies. If the Act takes effect in its current form, individuals will be able to veto the inclusion of public-domain

¹ I write on behalf of the Software Information & Industry Association (SIIA) and the Coalition for Sensible Public Record Access (CSPRA). As you know, SIIA’s members include publishers of business-to-business and business-to-consumer products in both digital and print form, as well as financial news services, software companies, and databases. Through their independent news-gathering and publishing activities, SIIA’s members inform businesses, journalists, and governments on a wide variety of activities. CSPRA is a non-profit organization dedicated to promoting the principle of open public record access to ensure consumers and businesses the continued freedom to collect and use, for personal and commercial benefit, the information made available in the public record.

Some of the publications produced by the members of these groups include names and other information about individuals. Many other businesses—including industry analysts, marketing experts, executive search firms, agents, lobbyists, ratings services, private detectives, and many others—also gather and sell information about people. These publications are an important resource for users investigating potential employees, investors, business partners, clients, service providers, customers, and competitors.

information about them in the databases and publications that many businesses provide to customers who use them for important, entirely legitimate purposes. For example:

- businesses conduct background checks on potential employees and on the officers and directors of potential business partners and merger or acquisition candidates;
- law enforcement officers obtain information relevant to their investigations regarding persons of interest;
- financial institutions and other businesses employ third parties use publicly available data sources to help them meet “know your customer,” anti-money laundering, anti-terrorism and anti-human trafficking obligations, as well as other financial crime and modern slavery laws, regulations, and industry practices; and
- industry analysts and ratings services obtain information critical to their analyses.

The Supreme Court has made clear that “the creation and dissemination of information is speech for First Amendment purposes.” *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011). The State may not infringe these rights to protect a generalized interest in consumer privacy. *See generally* E. Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 Stan. L. Rev. 1049, 1081 (2000).

The CCPA’s extraordinarily broad definition of “personal information” and the resulting restrictions on businesses that sell publicly available information—restrictions unprecedented in American law—violate the First Amendment in at least three independent ways:

- *First*, the CCPA’s restrictions on the dissemination of publicly available information impose a heavy burden on protected speech without advancing a compelling governmental interest, or even a substantial one. These provisions therefore violate the First Amendment rights of the businesses whose speech is burdened by them, as well as of potential users of the information that the businesses provide.
- *Second*, the law suffers from the independent constitutional flaw that it adopts an unjustified and impermissibly vague standard for determining when a business may disseminate information from public government records.
- *Third*, the Act discriminates among speakers and discriminates on the basis of speech content, which separately violates the First Amendment.

To avoid the need for a judicial challenge to the provisions at issue, the Legislature should amend the Act to eliminate these unconstitutional speech restrictions.

I. Background.

The CCPA applies to “personal information,” which it defines broadly to encompass all information that “identifies, relates to, describes, is capable of being associated with, or could

reasonably be linked, directly or indirectly, with a particular consumer or household.” Cal. Civ. Code § 1798.140(o)(1).²

“Personal information” excludes “publicly available information,” but the CCPA adopts an unusually narrow definition of the latter term. Cal. Civ. Code § 1798.140(o)(2). The definition first states that “publicly available” information means “information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information.” *Id.*³ It continues that “[i]nformation is not ‘publicly available’ if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.” *Id.*

The statute provides no guidance for determining when the sale of information obtained from public government records is “not compatible with” the purpose for which the data was maintained or made available by a governmental source. *See* Cal. Civ. Code § 1798.140(o)(2). Data “made available from federal, state, or local government records” therefore qualifies as personal information that is subject to the Act’s obligations and restrictions, depending on the meaning of the undefined “compatibility” test.

Importantly, the Act does not exclude from the definition of “personal information” *any* information that is available to the public but was not derived from governmental records. Thus, under the statute, a business may be precluded from selling information about a person that it gathers from phone directories, media outlets, and other widely available sources.

The CCPA—which takes effect on January 1, 2020—imposes obligations on any business that collects consumers’ personal information, does business in the State of California, operates for profit or for the benefit of its shareholders (thereby excluding non-profit entities), and either (1) has more than \$25 million in annual revenue; (2) annually buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or devices; or (3) derives 50 percent or more of its annual revenues from selling consumers’ personal information. Cal. Civ. Code § 1798.140(c).

First, the Act requires businesses to disclose to consumers the types of personal information that it collects from them, to provide them with copies of the information, and to delete the information upon request. Cal. Civ. Code §§ 1798.100, 1798.105, 1798.110(a)-(b).⁴

² The sweeping definition includes, but is not limited to, a consumer’s “name, . . . physical characteristics or description, address, telephone number, . . . education, . . . [or] “employment history.” Cal. Civ. Code § 1798.140(o)(1)(B) (incorporating Cal. Civ. Code § 1790.80). It also includes “[i]nferences drawn from any of the information identified . . . to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.” *Id.* § 1798.140(o)(1)(K).

³ This definition appears to be missing key words.

⁴ The Act defines “consumer” to mean any California resident who is natural person. Cal. Civ. Code § 1798.140(g).

Second, the Act also imposes obligations with respect to personal information that a business obtains from sources other than the consumer (which it defines broadly in Cal. Civ. Code § 1798.140(e) as a business that obtains such information “by any means”).

- The business must, upon request, disclose to the consumer the categories of personal information about that consumer that the business has collected, the purposes for which the information was collected, the categories of third parties with whom the business shares personal information, and the specific information that it has collected about that consumer. Cal. Civ. Code § 1798.110(a)-(b).
- If the business sells or discloses a consumer’s personal information for a business purpose, it must, upon request, provide the consumer with detailed information about such sales or disclosures. Cal. Civ. Code § 1798.115.
- Any consumer “shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer’s personal information.” Cal. Civ. Code § 1798.120(a). Businesses must notify consumers that they have the right to “opt out” of the sale of their personal information. *Id.* § 1798.120(b).⁵

II. The Act’s Restrictions On The Dissemination Of Accurate, Publicly Available Information Violate The First Amendment.

The CCPA’s provisions restricting the dissemination of publicly available information are unconstitutional for three independent reasons. *First*, these limitations are content-based restrictions on speech that are not justified by a sufficiently weighty governmental interest to satisfy strict scrutiny, or even intermediate scrutiny. *Second*, the regulation limiting dissemination of information publicly disclosed by government agencies is unconstitutionally vague. *Third*, the CCPA’s restrictions unconstitutionally distinguish among speakers and among different types of speech.

A. The Act’s limitations on speech are subject to strict scrutiny.

The First Amendment, which applies to the States through the Fourteenth Amendment, prohibits laws that abridge freedom of speech. Content-based regulations, which do not affect speech incidentally but instead “target speech based on its communicative content,” are “presumptively unconstitutional.” *Reed v. Town of Gilbert*, 135 S. Ct. 2218, 2226 (2015); *see also, e.g., R.A.F. v. City of St. Paul*, 505 U.S. 377, 382 (1992) (“Content-based regulations are presumptively invalid.”). “If a statute regulates speech based on its content, it must be narrowly tailored to promote a compelling Government interest.” *United States v. Playboy Entm’t Grp.*,

⁵ The right to demand that businesses *delete* information about them is limited to information “which the business has collected from the consumer” (Cal. Civ. Code § 1798.105(a))—but the rights to demand that information be disclosed, and not be sold, lack such a limitation, and thus apply to information about people gathered from all sorts of sources.

Inc., 529 U.S. 803, 813 (2000). “If a less restrictive alternative would serve the Government’s purpose, the legislature must use that alternative.” *Id.*

The CCPA’s limits on dissemination of publicly available information plainly qualify as content-based regulations. The Act flatly prohibits certain businesses from selling the “personal information” of people who exercise their statutory right to opt out. Such a law does not affect speech incidentally but instead directly “imposes a burden based on the content of speech and the identity of the speaker.” *Sorrell*, 564 U.S. at 567. Indeed, under the Act, “the government is prohibiting a speaker from conveying information that the speaker already possesses.” *Id.* at 568 (internal quotation marks omitted). As “a content-based speech restriction,” the Act’s bar on the dissemination of personal information “can stand only if it satisfies strict scrutiny.” *Playboy Entm’t Grp., Inc.*, 529 U.S. at 813.

The First Amendment standard applicable to the CCPA is not lessened because the law targets speech for which businesses receive compensation. The Supreme Court has emphasized that “the degree of First Amendment protection is not diminished merely because . . . speech is sold rather than given away.” *City of Lakewood v. Plain Dealer Publ’g Co.*, 486 U.S. 750, 756 n.5 (1988). The Court has also observed that “a great deal of vital expression” “results from an economic motive.” *Sorrell*, 564 U.S. at 567; *see also Smith v. California*, 361 U.S. 147, 150 (1959) (“It is of course no matter that the dissemination [of speech by the claimant] takes place under commercial auspices.”); *Joseph Burstyn, Inc. v. Wilson*, 343 U.S. 495, 501 (1952) (“That books, newspapers, and magazines are published and sold for profit does not prevent them from being a form of expression whose liberty is safeguarded by the First Amendment.”).

For that reason, laws that “establish[] a financial disincentive to create or publish works with a particular content” (*Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd.*, 502 U.S. 105, 115 (1991)) are subject to strict scrutiny under the First Amendment. The Act meets that description: It imposes a powerful “financial disincentive to create or publish” certain works by prohibiting the sale of any publication containing the personal information of a person who has opted out.

The Supreme Court’s decisions do distinguish between “speech proposing a commercial transaction, which occurs in an area traditionally subject to government regulation, and other varieties of speech.” *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n of N.Y.*, 447 U.S. 557, 562 (1980); *see also Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 66 (1983) (the “core notion of commercial speech” is “speech which does no more than propose a commercial transaction”) (internal quotation marks omitted). Laws that limit such speech are unconstitutional unless they “directly advance[]” a “substantial” governmental interest and are not “more extensive than is necessary to serve that interest.” *Cent. Hudson Gas & Elec. Corp.*, 447 U.S. at 566.

But the regulations here reach a range of communications that do not propose any commercial transaction. For example, a business that publishes and sells information for use by other businesses is producing an information-based product, but that speech is not in the nature of advertising and does not qualify as “commercial speech.” As discussed above, moreover, the regulations will impede speech outside the commercial realm by speakers ranging from book

publishers to photographers. The Act's limitations therefore must be assessed under the strict scrutiny test.

B. The Act's limitations on the dissemination of publicly available information fail strict scrutiny, and fail even intermediate scrutiny.

The CCPA's broad-brush restrictions on the dissemination of publicly available information are not narrowly tailored to further compelling governmental interests. Indeed, even if examined under the more permissive standard that governs commercial-speech regulation, the provisions are infirm because they do not “directly advance[]” a “substantial” governmental interest, and because they are more extensive than necessary to serve any such interest. *Cent. Hudson Gas & Elec. Corp.*, 447 U.S. at 566. As in *Sorrell*, “the outcome is the same whether a special commercial speech inquiry or a stricter form of judicial scrutiny is applied.” 564 U.S. at 571.

The government cannot defend a speech restriction “by merely asserting a broad interest in privacy.” *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1235 (10th Cir. 1999). “[P]rivacy may only constitute a substantial state interest if the government specifically articulates and properly justifies it.” *Id.*

Here, the privacy concerns animating the Act's passage had a specific focus: They arose from businesses' collection and dissemination of data gleaned from consumers' online activities, shopping, and use of computerized devices, which left consumers vulnerable to security breaches and other risks. *See* California Senate Judiciary Committee Bill Analysis, A.B. 375, at 1-2 (June 25, 2018). The CCPA's statement of purpose recites that “there is an increase in the amount of personal information shared by consumers with businesses”; that many businesses “collect personal information from California consumers” without their knowledge; and that “[t]he unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals,” including “financial fraud” and “identity theft.” Cal. Civ. Code § 1798.100.

Many of the Act's provisions respond to these identified risks, but the Act also applies to a wide variety of businesses that gather and sell information about people who are not customers. Their communications do not present the risks that the Legislature identified—and the stated interests therefore do not justify the regulations imposed on such businesses.

The government's interest in protecting consumers from businesses that track their activities, moreover, is not furthered by restricting the publication and distribution of publicly available information. The firms that publish such information do not exploit customer relationships to obtain it. Nor do they disseminate otherwise confidential information that will threaten an individual's safety and security if released. Instead, they distribute data that is already in the public domain so that it can be used efficiently by businesses, news organizations, and others that need the information.

Much of this public information has been released by government agencies. In California, these agencies have both a statutory and a constitutional obligation to provide “access to

information concerning the conduct of the people's business" (Cal. Const. art. 1, § 3(b)(1)), unless one of the statutory exceptions to disclosure applies. When a government agency "plac[es] the information in the public domain," it "must be presumed to have concluded that the public interest was thereby being served." *Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 495 (1975). That is particularly true in California, because the Public Records Act exempts from disclosure records "the disclosure of which would constitute an unwarranted invasion of personal privacy" (Cal. Gov't Code § 6254(c)); information available to the public therefore by definition falls outside that category. Businesses that facilitate access to such information serve the public interest underlying the California constitutional and statutory provisions—and the CCPA thus infringes on government interests rather than furthers them.

In adopting the Act, the Legislature also posited more generally that the right of privacy granted by the California Constitution confers "the ability of individuals to control the use, including the sale, of their personal information." Cal. Civ. Code § 1798.100. But the constitutional right of privacy is not so broad. Although "[i]nformational privacy is the core value furthered by" the constitutional privacy right, the California Supreme Court has explained that "information is private" only when "well-established social norms recognize the need to maximize individual control over its dissemination and use to prevent unjustified embarrassment or indignity." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 35 (Cal. 1994); *see also id.* at 37 ("A 'reasonable' expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms.").

In fact, there is no general expectation of privacy with respect to all personal information as defined by the Act. The right of access to information from public records is enshrined in the California Public Records Act and in the Constitution, which both "strike a careful balance between public access and personal privacy." *City of San Jose v. Superior Court*, 389 P.3d 848, 852 (Cal. 2017). Most Californians know that a substantial amount of information about them can be obtained through a Google search and a review of public records, and there is no "indignity" in that state of affairs. Thus, the right of privacy does not trump a business' First Amendment right to sell information in the public domain.

The Act's restrictions also have the potential to reach a wide variety of communications. For example, the law could reach:

- political opposition research businesses that sell information about the people they are hired to investigate;
- freelance press photographers who sell "visual . . . information" about newsworthy people and events; and
- private detectives, who sell information about the people they are investigating.

Moreover, people will be able to demand that private detectives and opposition researchers—and even book publishers—disclose any information that they have gathered about them. Cal. Civ. Code § 1798.110(a)-(b). That would include information gathered in the course of investigations: People who learn that they are the subject of a forthcoming book or investigative

report can demand to promptly learn all the information that was confidentially gathered about them.

Nor do the statute's narrow exceptions for free speech, journalism, and politics prevent such applications. The exception for a business' right to "[e]xercise free speech" (Cal. Civ. Code § 1798.105(d)(4)) applies only to people's right to delete information about them, under Section 1798.105; it does not apply to their right to demand that information about them not be sold, under Section 1798.120. Though journalism and politics are excepted from the definition of "commercial purposes" (*id.* § 1798.140(f)), publishing organizations with revenue of over \$25 million or political research groups that earn more than 50 percent of their revenue from selling information about research subjects are still covered "business[es]" under Section 1798.140(c)(1); the statute's prohibitions and requirements apply to them without regard to whether their purposes are viewed as "commercial." And though Section 1798.145(k) provides an exception for the "noncommercial activities" of certain publishers covered by Cal. Const. art. I, § 2(b), those publishers are limited to broadcasters and publishers of periodicals, and do not include publishers of other works, such as books, databases of information, or nonperiodical research reports. *See also* Legislative Counsel's Digest, S.B. 1121, § 2 (describing this exception as limited to "newspapers and periodicals").

Even if the publication of particular types of governmental information could be appropriately limited on the ground that widespread dissemination would lead to "unjustified embarrassment" (*Hill*, 7 Cal. 4th at 35), that would not save the statute from invalidation. "In the First Amendment context, . . . a law may be invalidated as overbroad if a substantial number of its applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep." *United States v. Stevens*, 559 U.S. 460, 473 (2010) (internal quotation marks omitted).

The CCPA is fatally overbroad, because it gives consumers the right to veto a large number of communications as to which they have no legitimate privacy right. The statute is thus facially invalid even if a small subset of its applications would be appropriate. *See Stevens*, 559 U.S. at 473. If a compelling governmental interest would be served by limiting the further dissemination of certain public information, then that interest can be advanced by a statute that narrowly targets the troubling information.⁶ But the Act's extensive burdens on speech cannot be justified on the ground that a small fraction of the information should be protected.

The Act's restrictions on dissemination of certain information are invalid for the additional reason that they are fatally underinclusive—the CCPA does not prohibit a number of indistinguishable means of disseminating widely the very same information. Information excluded from publications under the Act may still be distributed by businesses not covered by the Act, in newspaper and magazines (which are generally excluded from the Act), and in innumerable other ways, including on Facebook, Instagram, or Twitter.

No substantial governmental interest in consumer privacy is advanced by singling out certain businesses and prohibiting them from transmitting personal information when many other

⁶ The protections of health-related information enacted in the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, provide one such example.

individuals and businesses (including any nonprofit entities and smaller businesses) may continue to share the very same information. As the Supreme Court has held, the “facial under-inclusiveness” of an information privacy law “raises serious doubts” about whether it serves any genuine governmental interest at all. *Fla. Star v. B.J.F.*, 491 U.S. 524, 540 (1989) (striking down law barring publication of rape victims’ names by mass media where the provision did not “prohibit the spread” of the information “by other means,” such as “the backyard gossip who tells 50 people that don’t have to know”).

In sum, the asserted interests in privacy do not justify the broad and unfocused restrictions on dissemination of publicly available information that the Act imposes. These provisions thus violate the First Amendment.

C. The exception for publicly available information from governmental records is both impermissibly narrow and unconstitutionally vague.

The CCPA suffers from the independent, constitutional flaw that it adopts an unjustified and impermissibly vague standard for determining when a business may disseminate information from public government records.

As discussed above, the Act excludes from the definition of “personal information” “information that is lawfully made available from federal, state, or local government records,” unless “that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.” Cal. Civ. Code § 1798.140(o)(2). The compatibility requirement, which in other contexts restricts the sharing of personal information *among* governmental agencies, is not an appropriate standard for limiting the dissemination by private parties of information that an agency has *publicly disclosed*. The Act itself, moreover, articulates no standard for discerning whether use of a particular category of government information is “compatible” with the purpose for which the government maintained or released the information. Thus, even if the State could articulate a substantial interest in limiting the sale of information that a governmental agency has made public, the vagueness of this provision renders the Act’s restrictions invalid under the First Amendment.

The concept of compatible use appears to have been modeled on analogous language in the federal Privacy Act’s “routine use” exception. The Privacy Act governs federal agencies’ use and disclosure of information about individuals, such as information about an individual’s education, financial transactions, medical history, criminal record, and employment history. 5 U.S.C. § 552a(a)(4). Under the Privacy Act, an agency may not disclose such information to other individuals or agencies without the prior consent of the person to whom the record pertains, unless the disclosure is authorized by one of several statutory exceptions. *Id.* § 552a(b). Under one such exception, an agency may disclose information to another agency for a “routine use” (*id.*), which means “the use of such record for a purpose which is compatible with the purpose for which it was collected.” *Id.* § 552a(a)(7). A disclosure cannot be authorized under the routine use exception unless the disclosing agency first publishes a notice describing “each routine use of the records contained in the system, including the categories of users and the purpose of such use.” *Id.* § 552a(e)(4)(D).

The Privacy Act's "compatible use" requirement is "intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material." *Britt v. Naval Investigative Serv.*, 886 F.2d 544, 555 (3d Cir. 1989) (quoting *Analysis of House and Senate Compromise Amendments to the Federal Privacy Act*, reprinted in 120 Cong. Rec. 40,405, 40,406 (1974)). Similar requirements have been incorporated in laws that govern information-sharing by some California agencies. See, e.g., Cal. Code Regs. tit. 15, § 2087(c)(1)(A) (allowing disclosure of personal information maintained by the Parole Board to a state agency if "the transfer is compatible with a purpose for which the information was collected"); *id.*, tit. 5, § 42396.2(d) ("Personal information should not be transferred outside The California State University unless the transfer is compatible with the disclosed purpose for which it was collected.").

Because the "compatible use" requirement was designed to protect privacy by limiting the disclosure of confidential personal information, it is not an appropriate standard to govern the use of information *after the agency has released it to the public*. Cf. *Fla. Star*, 491 U.S. at 534 (making clear that, even when an agency has broad power not to release information about a person, once that information is released, the public is generally free to redistribute it). Under the Privacy Act, the determination whether a particular use is compatible requires "a dual inquiry into the purpose for the collection of the record in the specific case and the purpose of the disclosure." *Britt*, 886 F.2d at 548-49. Some courts have required "a nexus approaching an identity of purpose . . . between the reason the information was collected and the proposed routine use." *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993). Were that standard applied to the dissemination of publicly disclosed information by private parties, it would prohibit virtually every such use because agencies generally do not maintain or release their records for the purpose of having their records republished. It would also excessively burden speech by requiring a case-by-case determination of the agency's purpose in maintaining the records and its compatibility with the proposed use.

Were a court to conclude instead that the Privacy Act precedent is inapplicable, then the provision would be unconstitutionally vague because the statute provides no guidance for determining whether a proposed use of governmental information is "not compatible" with the government's purpose in maintaining or releasing it. A content-based regulation that is vague "raises special First Amendment concerns because of its obvious chilling effect on free speech." *Reno v. ACLU*, 521 U.S. 844, 871-72 (1997). "[V]ague laws chill speech" because "[p]eople 'of common intelligence must necessarily guess at [the law's] meaning and differ as to its application.'" *Citizens United v. FEC*, 558 U.S. 310, 324, (2010) (quoting *Connally v. Gen. Constr. Co.*, 269 U.S. 385, 391 (1926)). "The prohibition against vague regulations of speech" also is motivated by concerns about the "risk of discriminatory enforcement." *Gentile v. State Bar of Nev.*, 501 U.S. 1030, 1051 (1991).

The Act's "compatible use" requirement raises both concerns: It is so ambiguous and unclear that many businesses will forgo disseminating governmental information rather than risk violating the provision, and it is so indeterminate that the risk of discriminatory enforcement is high.

Under the Privacy Act, agencies must disclose the purposes for which they may transfer information to another agency under the “routine use” exception. But agencies do not typically explain the reasons for which they release information to the public. Nor could they, because an agency gives up control of the information when it makes it available to the public without conditions. Because agencies may not even consider how the information that they release may be used, there is no consistent, predictable and non-arbitrary way to determine whether a particular use of publicly available government information comports with the agency’s intent. This makes it likely that such determinations will be made in an *ad hoc* and standardless manner that will single out certain uses for unfavorable treatment.

A familiar example illustrates the problem. Records of home sales often are made public, and the information is used for many purposes. Neighbors may look up the information out of curiosity, appraisers working for lenders or insurers may employ the information in valuing other properties, and local businesses may use the information to direct their marketing efforts. Such information also may be published in the real estate sections of magazines and newspapers and on websites such as Zillow and Redfin. If a California resident objected under the Act to a particular use of the information—such as the inclusion of his or her name, address, and home price in a guide to movie stars’ homes—it is anyone’s guess whether that use would be deemed “not compatible” with the purpose for which the information was made publicly available. The publisher thus would face the choice between removing the requester’s name from the publication or risking an enforcement proceeding.

Each type of publication of each category of government information will present a similar dilemma. Given the uncertainty surrounding the concept of “compatible use,” many publishers will hesitate to include certain types of government information in their publications. The vagueness of the “compatible use” requirement thus will substantially limit protected speech.

D. The regulations disfavor certain speakers and messages.

Laws that “disfavor[] specific speakers” or “speech with a particular content” (*Sorrell*, 564 U.S. at 564) rarely survive First Amendment scrutiny. *See Rosenberger v. Rector & Visitors of Univ. of Va.*, 515 U.S. 819, 828 (1995) (“In the realm of private speech or expression, government regulation may not favor one speaker over another.”).

The CCPA on its face favors some speakers and some uses of information while disfavoring others. It also allows consumers to use the power of the State to suppress particular speakers and facts. And it does so in a frankly content-based way, aiming at restricting the publication of certain information but not other information. *See Reed*, 135 S. Ct. at 2227 (concluding that content-based speaker restrictions are subject to strict scrutiny); *Citizens United*, 558 U.S. at 340 (same); *Sarver v. Chartier*, 813 F.3d 891, 903 (9th Cir. 2016) (holding that statute that restricts the commercial use of people’s personal identifying information “clearly restricts speech based upon its content”). The CCPA therefore violates the fundamental First Amendment principle against distinguishing among speakers in a number of different ways.

First, the Act selectively burdens the speech of a subset of businesses that maintain and sell personal information—those that have substantial revenues, those that receive or disseminate

the personal information of large numbers of users for commercial purposes, and those that derive more than half of their annual revenues from the sale of personal information. Cal. Civ. Code § 1798.140(c). The Act requires these businesses to provide consumers with an “opt-out” right and bars them from selling information about people who exercise the right, but imposes no such requirements on smaller businesses that generally distribute different sorts of information (aggregated in different ways) than the larger businesses do. Furthermore, the opt-out right is limited to information that is *sold*; consumers may not block the distribution of personal information for other business purposes unless the information was collected from the consumer. *Id.* §§ 1798.105(a), 1798.120(a). The Act thus disfavors large businesses and smaller businesses that depend on selling personal information.

Second, the Act discriminates among speakers in another way: It provides that “the rights afforded to consumers and the obligations imposed on any business” under the Act “shall not apply to the extent that they infringe on” the activities of persons engaged in journalism and connected with a “newspaper, magazine, or other periodical publication, or . . . a press association or wire service.” Cal. Civ. Code § 1798.145(k); Cal. Const. art. I, § 2(b).

Thus, the *Los Angeles Times* could not be stopped from sharing information about a California resident’s criminal record with millions of daily readers, but that person could bar other businesses—including, for instance, book publishers—from including the same information in their publications. Because “[t]he law on its face burdens disfavored speech by disfavored speakers” (*Sorrell*, 564 U.S. at 564), and does so based on content and not just speaker identity, it violates the First Amendment.

Third, the law’s practical effect is to enable California residents to suppress the communication of particular facts. By exercising their opt-out rights, consumers can prevent a business from disseminating information about them in any communication that the business sells. The veto right conferred by the statute is virtually absolute: As long as the information satisfies the definition of “personal information,” the consumer may direct the business not to sell it, and the business must comply. Indeed, unless the business decides to give away its products rather than sell them, the restriction imposed once an individual opts out amounts to a “complete speech ban[].” 44 *Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 501 (1996). Such bans, “unlike content-neutral restrictions on the time, place, or manner of expression, are particularly dangerous because they all but foreclose alternative means of disseminating certain information.” *Id.* (internal citation omitted).

Moreover, the Act authorizes consumers to ban speech selectively, allowing some businesses to speak about them while silencing others. “[A] law or policy permitting communication in a certain manner for some but not for others raises the specter of content and viewpoint censorship.” *City of Lakewood*, 486 U.S. at 763.

Indeed, the Act appears designed to encourage such censorship. A California resident may first review the personal information that a company maintains and then decide whether to employ his or her opt-out right. Thus, a consumer may permit continued sales of positive information but block sales by businesses that possess negative information. Individuals can also favor some speakers over others: They can direct one business not to sell personal information while allowing

another business to market the very same information. This creates the potential for groups of consumers to burden disproportionately the speech of unpopular speakers, effectively censoring their communications in a manner that violates First Amendment principles.

III. The Act Should Be Modified To Exclude All Publicly Available Information.

Businesses whose speech is burdened by the CCPA will be able to sue in federal court under 42 U.S.C. § 1983 to assert their First Amendment rights and obtain an order invalidating the statute. Successful plaintiffs will be entitled to an award of attorney's fees and costs under 42 U.S.C. § 1988. To avoid the need for expensive litigation, the Legislature should amend the Act to remedy the First Amendment violations identified here. This can be achieved, in part, by modifying the definition of "publicly available information" to include both information that is "lawfully made available to the general public from federal, state, or local government records," without exception, and other information that is generally available to a wide range of persons, such as information from telephone books, information published in newspapers, and information from other public media.

Message

From: Stacey Gray [REDACTED]
Sent: 3/8/2019 4:06:05 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulator]; Eleanor Blume [REDACTED]
CC: Stacey Schesser [REDACTED]; John Verdi [REDACTED]; Amelia Vance [REDACTED]
Subject: FPF's Comments to the AG on CCPA
Attachments: FPF Comments to California AG (CCPA) - March 8, 2019.pdf; Attachment 1 - GDPR_CCPA_Comparison-Guide.pdf; Attachment 2 - FPF_Visual-Guide-to-Practical-Data-DeID.pdf

Hi Ellie & Stacey,

Please see attached FPF's written comments for the AG's office on the implementation of the CCPA. We hope you will find them constructive in the near-term as you work on many of these issues, and we'd be happy to engage further on any topic.

Best regards,
Stacey & FPF team

--



Stacey Gray
Policy Counsel
Future of Privacy Forum

[REDACTED]
Washington, DC 20005



[Subscribe](#) to our monthly newsletter!

www.fpf.org | 1400 Eye Street NW, Suite 450,

The Honorable Xavier Becerra
Attorney General, State of California
1300 I Street
Sacramento, CA 95814

VIA EMAIL TO: Eleanor Blume [REDACTED] and
privacyregulations@doj.ca.gov

March 8, 2019

Dear Attorney General Becerra,

The Future of Privacy Forum (FPF) respectfully submits the following comments regarding the implementation of the California Consumer Privacy Act of 2018 (CCPA).¹

FPF is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. FPF is supported by the privacy officers of more than 150 companies and by leading foundations, with an advisory board of academic, civil society and industry members. We bring together industry, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.²

We commend the Office of the Attorney General (AG) for its sincere and multi-faceted solicitation of feedback from diverse stakeholders and the public in recent months, including through public forums, testimony before the California Assembly, and requests for comments. Specifically, the AG has requested input on several enumerated areas outlined in Cal. Civ. Code § 1798.185. We respond primarily to these topics, and hope that our associated resources can assist the AG's office in its efforts to craft well-informed and meaningful rules and guidance.

We write to:

1. **Commend the State of California for addressing important data protection rights, including transparency, access, deletion, and reasonable security, for personal information.** California has long been a leader in data privacy, and in the last year has served as a legislative model for other states as well as sparking a serious national conversation regarding a federal privacy law. While FPF supports a strong, comprehensive, baseline federal privacy law, we believe that states that do advance legislation should do so in ways that provide consumers with comprehensive protections that are in line with the Fair Information Practice Principles (FIPPs) and take into account interoperability with the EU General Data Protection Regulation (GDPR).
2. **Recommend that rule-making efforts recognize that data exists on a spectrum of identifiability.** While some data is firmly linked to an individual or provably non-linkable to a person, significant amounts of data exist in a gray area — obfuscated but potentially linkable to an individual under some circumstances. We recommend that the AG take account of this spectrum of identifiability and provide incentives for companies to de-identify data using technical, legal, and administrative measures.

¹ California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.198(a) (2018) (hereafter "CCPA").

² The views herein do not necessarily reflect those of our supporters or our Advisory Board.

3. **Encourage further analysis of the impact of CCPA on socially beneficial research by non-HIPAA entities.** Although CCPA excludes health data regulated by the Health Insurance Portability and Accountability Act (HIPAA) and related laws, its provisions govern private companies that may choose to conduct socially beneficial research using non-HIPAA data, including: consumer wearable manufacturers; health-related mobile apps; and genetic testing companies. While these companies should surely be subject to data privacy rules, we recommend that the AG take a close look at specific areas where beneficial research can be enabled or facilitated, or where restrictive requirements may pose particular challenges for researchers.
4. **Encourage the AG to establish guidelines for data subject access requests (DSARs) that are secure, practical, and meaningful for consumers.** The right to access one's personal information is a fundamental tenet of the FIPPs, as well as a central feature of privacy laws in the United States and around the world. At the same time, there are inherent risks for some businesses in complying with data subject access request (DSARs), and often a direct tension between access rights and other important privacy safeguards. Ultimately, access requests should be secure, practical for businesses, and meaningful for consumers.
5. **Recommend greater clarity on the intersection of CCPA and existing student privacy laws governing education technology vendors.** For the benefit of schools, administrators, and education technology ("edtech") vendors, the AG should clarify key points of CCPA that are applicable to education and student privacy, including: edtech vendors' CCPA obligations (if any) when they act solely on behalf of public schools or districts; the circumstances under which edtech vendors may be considered "service providers" under the law; and alternately, how edtech vendors may navigate compliance obligations of CCPA in line with federal laws governing student records and California's existing student privacy laws.

We have attached a list of other relevant resources following this letter, including FPF publications on a variety of commercial privacy topics that may be of interest to the AG. We hope that our comments and the associated resources will be helpful to the important, ongoing discussion regarding consumer privacy in the State of California.

1. Addressing privacy through comprehensive data protection rights

The Future of Privacy Forum (FPF) has long supported a comprehensive, baseline federal privacy law that would fill the gaps between existing sectoral regimes and provide both regulatory clarity for businesses and a consistent set of protections for individuals across state lines.³ Although we are encouraged by recent legislative activity in Congress, the path to a national law remains uncertain. In the absence of a federal law, states that do advance legislation should seek to do so in ways that provide consumers with comprehensive protections in line with the Fair Information Practice Principles (FIPPs) and taking into account interoperability with the EU's General Data Protection Regulation (GDPR).⁴

³ Long Overdue: Comprehensive Federal Privacy Law, Future of Privacy Forum (Nov. 15, 2018), <https://fpf.org/2018/11/15/fpf-comments-on-a-national-baseline-consumer-privacy-law/> (last visited Mar. 8, 2019); FPF Comments to the U.S. Department of Commerce, Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48600 (2018), https://www.ntia.doc.gov/files/ntia/publications/ntia_request_for_comments_future_of_privacy_forum.pdf.

⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>, (hereafter "GDPR").

For these reasons, we commend the State of California for addressing several key data protection rights—including transparency, access to data, deletion, and reasonable security—that are aligned with global norms as well as with long-standing American traditions. Privacy as a common law right in the United States was established over a hundred years ago,⁵ later codified in the Second Restatement of Torts,⁶ and written into the constitutions of many states, including California, to explicitly protect the right to privacy and private life.⁷ Comprehensive privacy values were articulated more fully in 1973 in the globally influential FIPPs published by the U.S. Department of Health, Education, and Welfare.⁸ The FIPPs have since been embodied in United States and international laws, including the EU's GDPR.

As the AG considers additional rule-making and guidance to further the purposes of the CCPA, the FIPPs can provide a foundation for a holistic view of data protection that goes beyond notice and choice, including principles of: individual control, respect for context, focused collection, and responsible use, security, and accountability.⁹ In some areas, GDPR may also serve as a reference for U.S. lawmakers, with an understanding that the U.S. approach to privacy will likely diverge from the EU in some areas, such as in the breadth of data subject rights, or in balancing privacy with other constitutional values, including the First Amendment. **See Attachment 1** (Comparing Privacy Laws: GDPR vs. CCPA).

2. Data identifiability and personal information

The concept of “personal information” and its related aspects—including de-identification, anonymization, and pseudonymization—are at the crux of all privacy regulation, and the focus of considerable attention in a growing body of technical and legal literature. FPF has many years of significant experience working with experts on a range of modern de-identification practices, and a core part of our mission is to help identify and develop leading practices on this issue.¹⁰ We observe that most personal information exists on a spectrum of identifiability, and recommend that lawmakers find ways to incentivize companies to reduce data identifiability, while addressing the challenges that it may present for compliance with other privacy safeguards (such as access to data, discussed below).

We first note that CCPA's broad definition of personal information is in many respects aligned with existing legal standards¹¹ and evolving norms¹² in the United States, as

⁵ Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

⁶ Restatement (Second) of Torts § 652B-E (1977) (describing the four privacy torts: Public Disclosure of Privacy Facts; Intrusion upon Seclusion; False Light; and Appropriation of Name or Likeness).

⁷ The constitutions of eleven U.S. states have specifically enumerated rights to privacy or private life. *Privacy Protections in State Constitutions*, National Conference of State Legislatures, <http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx> (last visited Mar. 8, 2019), including, of course, California. Cal. Const., art. I, § 1 (“All people are by nature free and independent and have inalienable rights. Among these are . . . pursuing and obtaining . . . privacy.”).

⁸ Records, Computer, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Dept. of Health & Human Services, <https://aspe.hhs.gov/report/records-computers-and-rights-citizens> (last visited Mar. 8, 2019).

⁹ Records, Computer, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Dept. of Health & Human Services, <https://aspe.hhs.gov/report/records-computers-and-rights-citizens> (last visited Mar. 8, 2019).

¹⁰ See generally, e.g., De-Identification 201 Secure Multi-Party Computation Webinar, Future of Privacy Forum (Feb. 12, 2018), https://youtu.be/_B1wdzFWpD0 (last visited Mar. 8, 2019); De-Identification 201 Differential Privacy Webinar, Future of Privacy Forum (Feb 16, 2018), <https://www.youtube.com/watch?v=oKT-RrX82x0&feature=youtu.be> (last visited Mar. 8, 2019); Digital Data Flows Masterclass, Future of Privacy Forum (2018) (Class Three), <https://fpf.org/classes-archives/> (last visited Mar. 8, 2019); Brussels Privacy Symposium, Future of Privacy Forum (2016), <https://fpf.org/brussels-privacy-symposium/> (last visited Mar. 8, 2019).

¹¹ See, e.g., the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506. Personal information under COPPA includes “persistent identifiers,” defined as “identifier[s] that can be used to recognize a user over time and across different Web sites or online services . . . [including] a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier.” 16 C.F.R. § 312.

¹² Jessica Rich, *Keeping Up with the Online Advertising Industry*, Federal Trade Commission (Apr. 21, 2016), <https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry>.

well as with the broad definition of personal data in GDPR.¹³ To the extent that there is uncertainty around this alignment, for example due to the inclusion in CCPA of the term “inference” or the phrase “capable of being associated with,” we recommend that the AG provide clarification using existing U.S. laws and the GDPR as points of reference. Similarly, the inclusion of “household data” in CCPA may be perceived as broader than typical statutory descriptions of personal information. In most cases we are aware of, a household is reasonably linked to an identifiable person. However, this an area where the AG can create guidance that would reduce confusion, including for businesses that process data related to, for example: residential buildings; real estate; smart meters; utilities; or data from “smart homes.”

Within this range of “personal information” defined broadly in CCPA, it is important to note that most data exists on a spectrum of identifiability. **See Attachment 2: A Visual Guide to Practical De-Identification.** While some data is firmly linked to an individual or provably non-linkable, significant amounts of data exist in a gray area – obfuscated, but potentially linkable to an individual under some circumstances. As a result, determining when data is no longer “personal” and may be considered “de-identified” is a complex technical and legal question. According to the Federal Trade Commission (FTC), data are not “reasonably linkable” to an individual to the extent that a company: (1) takes reasonable measures to ensure that the data are de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data (the “Three-Part Test”).¹⁴ Commercial entities operate within this legal framework and take this definition into account, often in addition to standards of de-identification found in other longstanding U.S. federal laws.¹⁵

In contrast, under GDPR, information is considered “anonymous” when it “does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.”¹⁶ GDPR requires taking into account “all the means reasonably likely to be used” to identify an individual, including whether an individual can be “singled out” by a controller or another person.¹⁷ In determining “all means” reasonably likely to be used, GDPR also takes into account “all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.”¹⁸

In addition, GDPR creates legal incentives for “pseudonymisation,” defined as a process which results in personal data not being able to be attributed to a specific person without the use of additional information, provided that this information is kept separately and is subject to technical and organisational measures.¹⁹ While many GDPR safeguards still apply to “pseudonymized personal data,” the regulation nonetheless provides incentives for organizations to rely on pseudonymization by, for example: recognizing that pseudonymization is an appropriate safeguard to legitimize

¹³ The GDPR defines personal data as “any information relating to an identified or identifiable natural person (‘data subject’) . . . directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.” GDPR, Art. 4(1)(1).

¹⁴ Protecting Consumer Privacy in an Era of Rapid Change, Federal Trade Commission (2012), at 21, <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

¹⁵ The Health Insurance Portability and Accountability Act (HIPAA) defines de-identified data as “information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.” 45 CFR § 164.514(a). Under the Family Educational Rights and Privacy Act (FERPA), records are considered de-identified “after the removal of all personally identifiable information provided that the educational agency or institution or other party has made a reasonable determination that a student’s identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information.”

34 CFR § 99.31(b)(1)).

¹⁶ GDPR, Recital 26.

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ GDPR, Art. 4(5).

processing for additional, compatible purposes to the initial ones;²⁰ or to ensure compliance with the obligation of “data protection by design”;²¹ as a measure of security of processing;²² or to allow processing of personal data for scientific research.²³

In many cases, the ability to fully or partially de-identify personal data through technical, legal, and administrative measures will allow a company to retain some utility of data (e.g., for research, as we discuss below), while significantly reducing privacy risks. New advances in de-identification and related privacy-enhancing technologies (PETs) are continuing to emerge, including development of approaches such as differential privacy, synthetic data, and secure multiparty computation.²⁴ As a result, it is wise for lawmakers to find ways to incentivize companies to reduce data identifiability, while recognizing that it may create challenges for compliance with other consumer rights, such as data subject access request (DSARs).

Overall, we recommend that the AG be aware of the complexity and breadth of legal and technical literature on this topic. We hope our resources in this field can be of assistance to the AG and are available to engage further.

3. Enabling socially beneficial private research

We encourage the AG to interpret and implement CCPA, to the greatest extent possible, in ways that support meritorious, socially beneficial academic and private research in fields such as medicine, public health, or environmental impact. Although CCPA excludes data regulated by the California Medical Information Act (CMIA), the Health Insurance Portability and Accountability Act (HIPAA), and Federal Policy for the Protection of Human Subject (“the Common Rule”),²⁵ its provisions govern many companies that conduct similar research, such as: consumer wearable manufacturers; health-related mobile app developers; and genetic testing companies.

For example, it is helpful that CCPA contains an exception to consumer deletion requests for data that is necessary to engage in “*peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws . . . if the consumer has provided informed consent.*”²⁶ An important way that the AG might further enable beneficial research might be to permit companies to meet this requirement through self-regulatory mechanisms that are approved by the AG. Examples of self-regulatory mechanisms that the AG might approve include:

- *Voluntary compliance with the Common Rule.* The Common Rule provides ethical standards for research involving human subjects that is conducted, supported, or otherwise subject to regulation by federal agencies.²⁷ Companies that are not subject to the Common Rule often comply with its requirements voluntarily, receiving approval from an institutional review board (IRB) and obtaining informed consent from research subjects.
- *Corporate ethical review processes.* While informed consent may be feasible in a controlled research setting with a well-defined group of individuals, such

²⁰ GDPR, Art. 6(4)(e).

²¹ GDPR, Art. 25(1).

²² GDPR, Art. 32(1)(a).

²³ GDPR, Art. 89(1).

²⁴ Commission on Evidence-Based Policymaking, *The Promise of Evidence-Based Policymaking* (2017), available at https://www.govexec.com/media/gbc/docs/pdfs_edit/090617cc1.pdf.

²⁵ Cal. Civ. Code § 1798.145(6)(c)(1)(A-C).

²⁶ Cal. Civ. Code § 1798.105(d)(6).

²⁷ 45 CFR 46 (amended 2018). Currently, 20 US agencies and departments intend to follow the revised Common Rule and their CFR numbers. See US Department of Health & Human Services, *Federal Policy for the Protection of Human Subject (“Common Rule”)* <https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html> (last visited Mar. 8, 2019).

as a clinical trial, it is usually untenable for researchers analyzing large datasets of millions, or billions, of data subjects.²⁸ Ethical review processes (also sometimes referred to as consumer subject review boards, or corporate ethics boards) may serve an important goal of helping researchers identify and balance the risks and benefits of this kind of research, including to individuals, the company, and the public interest.²⁹

Legal mandates that require companies to obtain continual permission from individuals for future uses are appropriate in many commercial contexts (for example, obtaining opt-in permission from consumers who have exercised the right to opt out of sales under CCPA). However, such mandates may also create burdens for researchers using purchased or licensed data, who do not know what insights a future study might reveal, and who may rely on datasets containing individuals that they cannot contact or who have been de-identified.

As FPF noted in a report from a 2015 inter-disciplinary workshop, *Beyond IRBs: Designing Ethical Review Processes for Big Data Research*,³⁰ companies that engage in private research on large datasets have the opportunity to reap tremendous social benefits by analyzing data from cities, governments, health care institutions, schools, social networks, and search engines—but they must do so in a way that protects privacy, fairness, equality, and the integrity of the scientific process. In the words of one commentator, this may be “the biggest civil rights issue of our time.”³¹ For these reasons, we encourage the AG to recognize the challenges of consent and deletion requirements for researchers, while engaging in rule-making and guidance that will incentivize companies to voluntarily comply with strong privacy and ethical frameworks.

4. Establishing guidelines for Data Subject Access Requests (DSARs)

The right to access one’s personal information is a fundamental tenet of the FIPPs, as well as a central feature of privacy laws in the United States and globally. In many contexts, the right of access is an “enabling” right, meaning that it opens the door to other data protection rights, such as data portability, the rights to correct, supplement, or rectify data, and the right of deletion.

In spite of this, there are inherent risks for some businesses in complying with DSARs, and often a direct tension between access rights and other important privacy practices, such as collection minimization, and privacy by design (or data protection by design).³² This is a particularly prevalent issue for companies that do not have a direct relationship with consumers (often referred to as “third parties”), particularly

²⁸ In the words of danah boyd and Kate Crawford: “It may be unreasonable to ask researchers to obtain consent from every person who posts a tweet, but it is problematic for researchers to justify their actions as ethical simply because the data are accessible.” danah boyd & Kate Crawford, *Critical Questions for Big Data*, 15(5) INFO. COMM. & SOC. 662 (2012).

²⁹ See Future of Privacy Forum, *Beyond the Common Rule: Ethical Structures for Data Research in Non-Academic Setting* (2015), <https://fpf.org/wp-content/uploads/Polonetsky-Tene-final.pdf>; Dennis D. Hirsch, et al., Roundtable: *Beyond IRBs: Designing Ethical Review Processes for Big Data*, 72 Wash. & Lee L. Rev. Online 406–98 (2016); Ryan Calo, *Consumer Subject Review Boards: A Thought Experiment*, 66 Stan. L. Rev. Online 97 (2013).

³⁰ In 2015, FPF convened an interdisciplinary workshop, *Beyond IRBs: Designing Ethical Review Processes for Big Data*. The workshop brought together researchers, including lawyers, computer scientists, ethicists, and philosophers, as well as policymakers from government, industry, and civil society to discuss a blueprint for infusing ethical considerations into organizational processes in a data rich environment. See Roundtable: *Beyond IRBs: Designing Ethical Review Processes for Big Data*, 72 Wash. & Lee L. Rev. Online 406–98 (2016), <https://scholarlycommons.law.wlu.edu/wluir-online/vol72/iss3/>; Future of Privacy Forum & Washington and Lee School of Law, *Beyond IRBs: Designing Ethical Review Processes for Big Data*, <https://bigdata.fpf.org/> (last visited Mar. 8, 2019).

³¹ Alistair Croll, *Big data is our generation’s civil rights issue, and we don’t know it*, O’Reilly Radar, Aug. 2, 2012, <http://radar.oreilly.com/2012/08/big-data-is-our-generations-civil-rights-issue-and-we-dont-know-it.html> (last visited Mar. 8, 2019).

³² See, e.g., M. Veale et al., *When data protection by design and data subject rights clash*, Intl. Data Privacy L., Vol. 8, No. 2 (2018), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3081069.

when they collect or receive personal information that falls somewhere on a spectrum of less readily identifiable data. This includes, for example: IP addresses; cookie identifiers; mobile advertising identifiers (Ad IDs); or other persistent identifiers that are commonly used for online and mobile advertising.³³

For third parties that process less readily identifiable personal information (such as cookie IDs), it can often be challenging if not impossible to validate that the person making an access request is in fact requesting his or her own data. As a result, companies must carefully tailor the scope of their access tools in light of: the sensitivity of the data; their relative ability to identify the data without taking extra steps to re-identify it;³⁴ and their ability to adequately verify that the data belongs to the requester while avoiding onerous requests that she or he provide validating documents. For example, a company that processes geo-location data tied to an advertising identifier may find that it is too sensitive to disclose in an access request, due to the revealing nature of the information and the potential for abuse, including identity theft or domestic violence. Yet reasonable compliance might include confirmation that the data exists, a description of its geographic scope and time period, and/or the option to have the data deleted.

Ultimately, access requests should be:

- **Secure.** Access request mechanisms, such as “download my data” tools, should be required to be provided in ways that ensure the data is transmitted safely and securely, using reasonable technical, legal, and administrative safeguards that are proportional to the sensitivity of the underlying data.
- **Practical for Businesses.** Access requests should not require businesses to take steps to re-identify individual data that has been de-identified, nor incentivize them to make overly burdensome requests to consumers for additional information for purposes of validation.
- **Meaningful for Consumers.** In some cases, individuals may be primarily interested in learning about the existence of data held by a company, or may be concerned primarily with categories of information, such as how they have been characterized or placed into a particular marketing segment. In other cases, they may be satisfied instead with having the data deleted. As the AG considers options for regulatory flexibility that might prove practical for businesses, they should still ensure that access requests meet the underlying needs of individuals.

Finally, we note that this is not an issue unique to CCPA, and we recommend that the AG look to existing guidance from U.S. and international sources, including: U.S. federal agencies;³⁵ the Office of the Privacy Commissioner of Canada;³⁶ the UK

³³ As we discussed in a 2015 report on cross-device tracking, some companies may also engage in probabilistic identification of devices, particularly for purposes of associating devices for advertising attribution (measurement and reporting), or as an alternative to cookies where browsers block or limit the placement of third-party cookies. See Jules Polonetsky & Stacey Gray, Future of Privacy Forum, *Cross-Device: Understanding the State of State Management* (2015) (at 9), available at https://fpf.org/wp-content/uploads/2015/11/FPF_FTC_CrossDevice_F_20pg-3.pdf. In reaction to the perceived risks of this kind of statistical identification or “data fingerprinting,” Apple’s Safari recently eliminated support for the Do Not Track (DNT) standard. *Safari 12.1 Beta 3 Release Notes, Developer Documentation*, Apple, https://developer.apple.com/documentation/safari_release_notes/safari_12_1_beta_3_release_notes (last visited Mar. 8, 2019).

³⁴ In several places, CCPA states that companies are not obligated to take steps to re-identify individuals, which is good policy and aligns with GDPR’s Article 11, which states that data controllers “shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of [compliance].” GDPR, Art. 11.

³⁵ See, e.g., Federal Communications Commission (FCC) Privacy Act Manual (FCCINST 1113.1) (2017). <https://www.fcc.gov/sites/default/files/fcc-privacy-act-manual.pdf>.

³⁶ Office of the Privacy Commissioner of Canada, Responding to access to information requests under PIPEDA, What businesses need to know (February 2014), https://www.priv.gc.ca/en/privacy-topics/access-to-personal-information/giving-individuals-access-to-their-personal-information/02_05_d_54_ati_02/ (last visited Mar. 8, 2019).

Information Commissioner's Office (ICO);³⁷ the European Commission;³⁸ and the Ireland Data Protection Commission.³⁹ Because the GDPR has not been in effect for very long, there remains a broad diversity in approaches that global companies are currently taking to comply with access requests. As far as possible, we recommend taking into account interoperability with GDPR to facilitate regulatory clarity for businesses as well as consistent expectations for individuals.

5. The intersection of CCPA with California's education privacy laws

FPF has significant expertise working with stakeholders at the intersection of privacy and education. FPF's Education Privacy team has testified before Congress⁴⁰ and the Federal Commission on School Safety,⁴¹ was invited to speak at the 2017 FTC and U.S. Department of Education workshop on Student Privacy and EdTech, and publishes extensive resources for parents, students, educators, edtech vendors, practitioners, and policymakers.⁴² FPF also co-founded the Student Privacy Pledge, a self-regulatory framework that safeguards student privacy regarding the collection, maintenance, and use of student personal information.⁴³

We recommend that for the benefit of schools, administrators, and education technology ("edtech") vendors, the AG should clarify key points of CCPA that are applicable to edtech, and its interaction with existing state and federal education privacy laws. Specifically, we recommend greater clarity for understanding when edtech vendors may be considered "service providers" under the law; and alternately, how edtech vendors may navigate compliance obligations when they are subject to overlapping requirements under CCPA, the Federal Educational Rights and Privacy Act (FERPA),⁴⁴ and the Student Online Personal Information Protection Act (SOPIA).⁴⁵

As a threshold issue, we recommend that the AG clarify that a "service provider" under CCPA may include edtech vendors. Edtech companies support schools — including their teachers, students and parents — to manage student data, carry out school operations, support instruction and learning opportunities, and develop and improve products and services intended for educational use.⁴⁶ Edtech vendors range

³⁷ *Guide to the General Data Protection Regulation (GDPR), Right of Access*, Information Commissioner's Office, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/> (last visited Mar. 8, 2019); *Responding to access to information requests under PIPEDA*, Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/en/privacy-topics/access-to-personal-information/giving-individuals-access-to-their-personal-information/02_05_d_54_ati_02/ (last visited Mar. 2019); *Complying with COPPA: Frequently Asked Questions*, Federal Trade Commission, <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions> (last visited Mar. 8, 2019).

³⁸ *How can I access my personal data held by a company/organisation?*, Policies, Information and Services, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/how-can-i-access-my-personal-data-held-company-organisation_en (last visited Mar. 8, 2019).

³⁹ *Limiting Data Subject Rights and the Application of Article 23 of the General Data Protection Regulation*, Data Protection Commission, <https://www.dataprotection.ie/en/individuals/know-your-rights/restriction-individual-rights-certain-circumstances-article-23-gdpr> (last visited March 8, 2018).

⁴⁰ FPF Testifies Before Congress on Promoting and Protecting Student Privacy, FERPA SHERPA (May 18, 2018), <https://ferpasherpa.org/fpf/> (last visited Mar. 8, 2019).

⁴¹ FPF Testifies Before Federal Commission on School Safety, FERPA SHERPA (July 11, 2018), <https://ferpasherpa.org/fpf-testifies-before-federal-commission-on-school-safety/> (last visited Mar. 8, 2019).

⁴² The Education Privacy Resource Center, FERPA SHERPA, <https://ferpasherpa.org/> (last visited Nov. 9, 2018).

⁴³ 350 leading education technology companies have signed the pledge. See The Student Privacy Pledge, Future of Privacy Forum & The Software & Information Industry Association (2019), <https://studentprivacypledge.org/> (last visited Mar. 8, 2019).

⁴⁴ Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g.

⁴⁵ Student Online Personal Information Protection Act, Cal. Bus. & Prof. Code § 22584 (2014). SOPIA was the first law in the United States to comprehensively address student privacy.

⁴⁶ The US Department of Education refers to edtech vendors as "vendors and other third party providers who are developing, or selling educational technology apps or services that utilizes or collect or uses Students' Personally Identifiable Information." *BY AUDIENCE: Education Technology Vendors*, US Department of Education, <https://studentprivacy.ed.gov/audience/education-technology-vendors> (last visited Mar 8, 2019).

from some of the largest technology companies in the world to a rapidly growing world of start-ups and small businesses.⁴⁷

Currently, CCPA defines a service provider as a business that:

*“... processes information on behalf of a **business** and to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any [other] purpose . . .”⁴⁸*

It is good policy, and in line with existing legal norms, to exclude service providers from compliance obligations related to access, deletion, and control, on the basis that they are under contractual limitations and do not retain further rights to retain, use, or disclose data.⁴⁹ However, CCPA’s definition appears to exclude service providers who process data on behalf of non-businesses, such as non-profits and government entities. Yet it is certainly within the spirit and purpose of CCPA to apply this exclusion equally to service providers who process data on behalf of government entities, who frequently use contracted vendors for services such as direct mailing, customer management, or IT support.

In the context of K-12 education, many edtech vendors process data on behalf of schools or school districts. Under the federal law FERPA, schools and school districts must maintain direct control over data they share with third parties without parental consent. This means that an edtech provider receiving student data under this exception is only allowed to use, disclose, or retain data as allowed by the school or school district. Furthermore, California’s leading student privacy law, SOPIPA, and its companion AB1584 also require privacy protections and contractual restrictions that protect student privacy. While in some respects SOPIPA is clearly more privacy protective than CCPA,⁵⁰ in other ways the interaction between the laws might not be as clear.

As a result, it could create intractable conflicts for an edtech vendor to be obligated to respond to CCPA access or deletion requests while under a contract or other legal obligation that simultaneously reserves access and deletion rights to the school or district. This does not mean students or parents would be limited in accessing their data; it simply means that they would be required to go through existing FERPA-mandated processes to access their data through the school or district.

Overall, we recommend further engagement on the intersection of CCPA with existing state and federal laws, including SOPIPA, COPPA, and FERPA. In addition to the fact that many edtech companies are small businesses without robust legal compliance programs, further guidance will also help bring regulatory for schools, school districts, and school administrators who negotiate privacy and data use conditions related to educational products and services.

⁴⁷ In 2017, of the nearly \$9.52 billion in edtech investment, “[c]onsumer companies raised \$3.85 billion in 2017, and corporations came in slightly below at \$3.79 billion.” Robyn Shulman, *EdTech Investments Rise to a Historical \$9.5 Billion: What Your Startup Needs to Know*, *Forbes* (Jan. 26, 2018), <https://www.forbes.com/sites/robynshulman/2018/01/26/edtech-investments-rise-to-a-historical-9-5-billion-what-your-startup-needs-to-know/#5064e8a93a38> (last visited Mar. 8, 2019). Edtech vendors provide thousands of products to students. See The EdSurge Product Index, EdSurge (2019), <https://www.edsurge.com/product-reviews> (last visited Mar. 8, 2019).

⁴⁸ Cal. Civ. Code § 1798.140(v).

⁴⁹ GDPR defines processing as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.” GDPR, Art. 4(1)(2).

⁵⁰ For example—assuming that SOPIPA covers a similar range of personal information (which is not clear)—while CCPA requires that consumers must be permitted to opt out of the sale of data, SOPIPA completely prohibits the commercial sale of data for its covered entities (edtech providers).

Additional Resources

Finally, FPF has published a broad range of technical, legal, and policy analysis on other commercial privacy issues that may be of interest to the AG. Below are a few highlights from recent months (for more visit www.fpf.org):

- **The Internet of Things (IoT) and People with Disabilities.** In January 2019, FPF published *The Internet of Things (IoT) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions*, a report that examines the nuances of privacy considerations for people with disabilities using IoT services and provides recommendations to address privacy considerations, which can include transparency, individual control, respect for context, the need for focused collection and security.⁵¹
- **Artificial Intelligence (AI) and Machine Learning (ML).** In October 2018, FPF released the *Privacy Expert's Guide to AI and Machine Learning*, a guide for non-programmers to understand the technological basics of AI and ML systems, and to address privacy challenges associated with the implementation of new and existing ML-based products and services.⁵²
- **Digital Data Flows “Masterclass” Series.** In October 2018, FPF launched a “Masterclass” series for U.S. and European regulators and staff who are seeking to better understand the data-driven technologies at the forefront of data protection law & policy. The program features experts on machine learning, biometrics, connected cars, facial recognition, online advertising, encryption, and other emerging technologies.⁵³
- **Facial Recognition.** In September, 2018, FPF published the infographic *Understanding Facial Detection, Characterization, and Recognition Technologies*,⁵⁴ along with *Privacy Principles for Facial Recognition Technology in Consumer Applications*.⁵⁵ These resources are intended to help policymakers better understand and evaluate the growing use of consumer-facing technologies used for facial detection, characterization, and recognition.
- **Non-HIPAA Health Data.** In July 2018, FPF published *Privacy Best Practices for Consumer Genetic Testing Services*, which provides a privacy policy framework for the collection, protection, sharing, and use of genetic data by consumer genetic and personal genomic testing companies.⁵⁶ FPF also released *Best Practices for Consumer Wearables and Wellness Apps and Devices*, a detailed set of guidelines that provide practical privacy protections for consumer-generated health and wellness data.⁵⁷

⁵¹ Future of Privacy Forum, *The Internet of Things (IoT) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions* (Jan. 31, 2019), https://fpf.org/wp-content/uploads/2019/01/2019_01_29-The_Internet_of_Things_and_Persons_with_Disabilities_For_Print_FINAL.pdf.

⁵² Future of Privacy Forum, *The Privacy Expert's Guide to Artificial Intelligence and Machine Learning* (2018), https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf.

⁵³ Digital Data Flows Masterclass, Future of Privacy Forum (2018), <https://fpf.org/classes-archives/> (last visited Mar. 8, 2019).

⁵⁴ Future of Privacy Forum, *Understanding Facial Detection, Characterization and Recognition Technologies* (2018), https://fpf.org/wp-content/uploads/2018/09/FPF_FaceRecognitionPoster_R5.pdf.

⁵⁵ Future of Privacy Forum, *Privacy Principles for Facial Recognition Technology in Commercial Applications* (2018), https://fpf.org/wp-content/uploads/2018/09/FR-Final-doc1_publish.pdf.

⁵⁶ Future of Privacy Forum, *Privacy Best Practices for Consumer Genetic Testing Services* (2018), <https://fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf>.

⁵⁷ Future of Privacy Forum, *Best Practices for Consumer Wearables and Wellness Apps and Devices* (2016), <https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf>.

We hope these comments and attached resources will be useful to the rule-making process in the State of California, and look forward to engaging further on these important issues.

Sincerely,

Stacey Gray
Policy Counsel

Carson Martinez
Policy Fellow

Amelia Vance
Director of Education Privacy

Future of Privacy Forum
1400 Eye St. NW Ste 510,
Washington, DC 20005

Attachment 1: "Comparing Privacy Laws: GDPR vs. CCPA"

Attachment 2: "A Visual Guide to Practical De-Identification"

Resources also available at www.fpf.org



Comparing privacy laws: **GDPR v. CCPA**



About the authors

DataGuidance provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

The DataGuidance platform includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Future of Privacy Forum is a nonprofit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. FPF brings together industry, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.

Contributors

DataGuidance: Alice Marini, Alexis Kateifides, Joel Bates

Future of Privacy Forum: Gabriela Zanfiri-Fortuna, Michelle Bae, Stacey Gray, Gargi Sen

Image credits:

Cover: Bulgac / Signature collection / iStockphoto.com, cnrythz / Signature collection / iStockphoto.com

Keys: enisaksoy / Signature collection / iStockphoto.com



Table of contents

Introduction	5
1. Scope	
1.1. Personal scope	7
1.2. Territorial scope	8
1.3. Material scope	9
2. Key definitions	
2.1. Personal data (personal information)	13
2.2. Pseudonymisation	16
2.3. Controllers and processors (businesses and service providers)	17
2.4. Children	19
2.5. Research	21
3. Legal basis	23
4. Rights	
4.1. Right to erasure (right to deletion)	26
4.2. Right to be informed	28
4.3. Right to object (right to opt-out)	30
4.4. Right of access	31
4.5. Right not be subject to discrimination for the exercise of rights	33
4.6. Right to data portability	34
5. Enforcement	
5.1. Monetary penalties	37
5.2. Supervisory authority	38
5.3. Civil remedies for individuals	39
Index: CCPA provisions	41

Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and the California Consumer Privacy Act of 2018 ('CCPA') (SB-1121 as amended at the time of this publication) both aim to guarantee strong protection for individuals regarding their personal data and apply to businesses that collect, use, or share consumer data, whether the information was obtained online or offline.

The GDPR, which went into effect on 25 May 2018, is one of the most comprehensive data protection laws in the world to date. Absent a comprehensive federal privacy law in the U.S., the CCPA is considered to be one of the most significant legislative privacy developments in the country. Like the GDPR, the CCPA's impact is expected to be global, given California's status as the fifth largest global economy. The CCPA will take effect on 1 January 2020, but certain provisions under the CCPA require organizations to provide consumers with information regarding the preceding 12-month period, and therefore activities to comply with the CCPA may well be necessary sooner than the effective date.

As highlighted by this Guide, the two laws bear similarity in relation to their definition of certain terminology; the establishment of additional protections for individuals under 16 years of age; and the inclusion of rights to access personal information.

However, the CCPA differs from the GDPR in some significant ways, particularly with regard to the scope of application; the nature and extent of collection limitations; and rules concerning accountability. Regarding the latter for example, the GDPR provides for obligations in relation to the appointment of Data Protection Officers, the maintenance of a register of processing activities, and the need for Data Protection Impact Assessments in specified circumstances. Conversely, the CCPA does not specifically focus on accountability-related obligations, even though such provisions exist, such as the obligation for companies to train their staff that deal with requests from consumers.

It is also noteworthy that the core legal framework of the CCPA is quite different from the GDPR. A fundamental principle of the GDPR is the requirement to have a "legal basis" for all processing of personal data. That is not the case for the CCPA.

Moreover, the CCPA excludes from its scope the processing of some categories of personal information altogether, such as medical data covered by other U.S. legal frameworks, including processing of personal information for clinical trials, and personal information processed by credit reporting agencies.

Moreover, the CCPA focuses on transparency obligations and on provisions that limit selling of personal information, requiring a "Do Not Sell My Personal Information" link to be included by businesses on their homepage. In addition, the CCPA includes specific provisions in relation to data transferred as a consequence of mergers and acquisitions, providing consumers with the right to opt-out if the "third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection."

This Guide aims to assist organizations in understanding and comparing the relevant provisions of the GDPR and the CCPA, to ensure compliance with both pieces of legislation.

Structure and overview of the Guide

This Guide provides a comparison of the two pieces of legislation on the following key provisions:

1. Scope
2. Key definitions
3. Legal basis
4. Rights
5. Enforcement

Each topic includes relevant articles and sections from the two laws, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the CCPA. The degree of similarity for each section can be identified using the key below.



Consistent: The GDPR and CCPA bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.



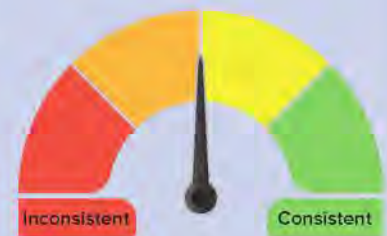
Fairly consistent: The GDPR and CCPA bear a high degree of similarity in the rationale, core, and the scope of the provision considered; however, the details governing its application differ.



Fairly inconsistent: The GDPR and CCPA bear several differences with regard to the scope and application of the provision considered, however the rationale and core present some similarities.



Inconsistent: The GDPR and CCPA bear a high degree of difference with regard to the rationale, core, scope and application of the provisions considered.



Usage of the Guide

This Guide is general and educational in nature and is not intended to provide, and should not be relied on as a source of legal advice. The information and materials provided in the Guide may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on particular circumstances.

The analysis is based on the version of the CCPA amended by the California legislature in October 2018. Please note that the CCPA provides a mechanism for additions or changes to some provisions through rulemaking by the California Attorney General. In addition, many stakeholders – lawmakers, advocates, companies, and others – anticipate additional revisions through the legislative process.

1. Scope



1.1. Personal scope

With regard to personal scope, businesses, public bodies and institutions, as well as not-for-profit organisations are subject to the GDPR, whilst only for-profit entities (“businesses”) are covered under the CCPA. In addition, the CCPA sets thresholds that determine businesses covered by the law, while the GDPR does not. Both laws apply to those businesses that determine the “purposes and means of the processing” of data.

The CCPA protects “consumers” who are natural persons and who must be California residents in order to be protected, whilst the GDPR protects “data subjects,” who are natural persons and does not specify residency or citizenship requirements.

GDPR	CCPA
Articles 3, 4(1)	Sections 1798.140 (c), (g), 1798.145(a)(6)
Recitals 2, 14, 22-25	

Similarities

The GDPR only protects natural persons (individuals) and does not cover legal persons.

A controller is defined by the fact that it establishes the means and purposes of the processing.

The CCPA only protects natural persons (individuals) and does not cover legal persons.

A covered business is defined by the fact that it establishes the means and purposes of the processing, though there are also other criteria to be met (see below).

Differences

Article 4(1) of the GDPR clarifies that a **data subject** is “an identified or identifiable natural person.” Article 3 and Recitals 2, 14, and 24 provide that a data subject may be any individual whose personal data is processed, and do not specifically require that the data subject holds EU residency or citizenship, or is located either within or outside the EU. However, there is a location-related requirement as a condition to trigger applicability when the controller does not have an establishment in the EU (see below). A data subject must be a living individual as the GDPR does not cover the processing of personal data of deceased persons.

The GDPR obligations apply to “**controllers**,” which can be natural or legal persons, irrespective of whether their activity is for profit or not, irrespective of their size and whether they are private law or public law entities, as long as they determine the means and purposes of processing activities.

A “**consumer**” who has rights under the CCPA is “a **natural person who is a California resident**.” The California Code of Regulations defines a resident as “(1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. All other individuals are nonresidents.”

The CCPA obligations apply to an organization (“**business**”) that:

1. is **for-profit**;
2. collects **consumers’ personal information**, or on the behalf of which such information is collected;
3. **determines the purposes and means** of the processing

Differences (cont'd)

of consumers' personal information;

4. **does business in California**; and

5. meets any of the following thresholds:

- has annual gross revenue in excess of \$25 million;
- alone or in combination, annually buys, receives for the business's commercial purposes, sells or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or
- derives 50% or more of its annual revenues from selling consumers' personal information.

Several obligations also apply to **"processors,"** which are entities that process personal data on behalf of controllers.

The CCPA also applies to any entity that controls or is controlled by the business. There are no obligations directed specifically at **"service providers,"** other than using the personal information solely at the direction of the business they serve. Businesses may also direct service providers to delete consumers' personal information from their records.

1.2. Territorial scope



The GDPR applies to organizations outside the EU if they offer goods or services to, or monitor the behavior of persons within the EU. The CCPA applies to businesses that do business in California and, although not explicitly mentioned, the CCPA appears to be applicable to a business established outside of California if it collects or sells California consumers personal information while conducting business in California.

GDPR

Articles 3, 4(1)

Recitals 2, 14, 22-25

CCPA

Sections 1798.140 (c), (g), 1798.145(a)(6)

Similarities

The GDPR applies to organizations that **do not have any presence in the EU**, but that **offer goods, services or monitor the behavior of persons in the EU**.

It is unclear whether the CCPA applies to a business established outside of California if it collects or sells **California consumers personal information while conducting business in California** and meet one of the other quantitative thresholds. This would depend on how "doing business in

Similarities (cont'd)

California" is interpreted and applied (see below).

Differences

Under Article 3, the GDPR applies to:

1. **entities or organizations established in the EU:** the GDPR applies to processing by controllers and processors in the EU (entities that have an "establishment" in the EU) if processing of personal data takes place in the context of the activities of that establishment, irrespective of whether the data processing takes place in the EU or not. "**Establishment**" in the EU is interpreted broadly, which could include having a minimal presence of using a local agent or having a single representative.
2. **entities or organizations not established in the EU:** the GDPR also applies to organisations located outside the EU (those that do not have an establishment in the EU) if they offer goods or services to, or monitor the behavior of, data subjects located in the EU, irrespective of their nationality and the company's location.

The CCPA applies to organizations "**doing business in California.**" This criterion is not precisely defined in the CCPA. However, according to the California Franchise Tax Board, doing business in California consists of "actively engaging in any transaction for the purpose of financial or pecuniary gain or profit" and an out-of-state entity can be considered as doing business in California if it meets certain thresholds (see Section 23101 of the Revenue and Taxation Code). Therefore, it is conceivable that out-of-state entities collecting, selling or disclosing personal information of California residents can fall under the the scope of the CCPA.

The obligations imposed on businesses by the CCPA do not restrict a business's ability to "collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California [...] Commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California and no personal information collected while the consumer was in California was sold."

1.3. Material scope

The GDPR applies to the processing of personal data by automated means or non-automated means if the data is part of a filing system. The CCPA does not specifically delineate a material scope, but its obligations cover "collecting," "selling" or "sharing" personal information.

The CCPA definition of personal information presents some overlaps with the GDPR definition of personal data. The GDPR excludes from its application the processing of "anonymous data," while the CCPA excludes from its application collection, sharing or processing of "aggregate consumer information" and "deidentified data."



Material scope (cont'd)

Unlike the GDPR, the CCPA provides several specific carve-outs from its scope of application, such as medical information and protected health information. The CCPA also excludes personal information the transfer of data to a third party in the context of a merger (from the definition of “selling”). However, the law still allows the right to opt-out if the resulting entity uses that personal information in a manner that is materially inconsistent with “the promises made at the time of collection.”

Both the CCPA and the GDPR are not applicable in the law enforcement and national security areas, although they may apply to businesses providing services to law enforcement or national security agencies.

The GDPR does not apply in the context of a purely personal or household activity, whilst the CCPA does not apply to non-commercial activities. However, the GDPR exemption only refers to individuals, while the CCPA covers businesses.

GDPR

Articles 2, 4(1), 4(2), 4(6)
Recitals 15-21, 26

CCPA

Sections 1798.140(e),(o),(t),(q), 1798.145

Similarities

The GDPR applies to the “**processing**” of personal data. The definition of “processing” covers “any operation” performed on personal data “such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”

“**Personal data**” comprises “any information” that directly or indirectly relates to an identified or identifiable individual. **Anonymous** data is specifically outside the scope of the GDPR. Anonymous data is information that does not

Some of the CCPA obligations apply to “collecting” personal information and some apply to “selling” or sharing it.

- “**Collecting**” under the CCPA is “buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means.” Therefore, it covers any type of operation by which a business acquires personal information, be it directly from the consumer, or indirectly (e.g. through observation).
- “**Selling**” includes “renting, disclosing, releasing, disseminating, making available transferring, or otherwise communicating personal information for monetary or other valuable consideration.” Note that selling does not necessarily involve a payment to be made in exchange for personal information.
- The CCPA’s definition of “**processing**” is “any operation or set of operations that are performed on personal data” by either automated or not automated means. However, the term “processing” is only used in the definitions section.

“**Personal information**” comprises “information” that directly or indirectly relates to or could reasonably be linked to a particular consumer or household. Businesses do not have to apply the CCPA obligations to “aggregate consumer

Similarities (cont'd)

relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

The GDPR **excludes** from its application **processing of personal data by individuals for purely personal or household purposes**. This is data processing that has “no connection to a professional or commercial activity.”

information,” which is defined as information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. Businesses are also **exempted** from applying CCPA obligations to “**deidentified**” information, which is information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information puts in place some technical and organizational measures to prevent reidentification.

The CCPA stipulates that the rights afforded and the obligations imposed on **businesses do not apply** if they are related to the **non-commercial activities** of a person.

Differences

The GDPR applies to the “processing of personal data” regardless of the type of processing operation, with the exception of the two types of processing listed below.

The GDPR **does not exclude specific categories of personal data** from its scope of application.

The CCPA primarily creates requirements for businesses that share or sell information, with some requirements that are also triggered by collection of information. For example, the **right to opt-out** is only available in the case of selling or sharing personal information.

The CCPA **specifically excludes** from its scope of application collecting and sharing of some categories of personal information:

- **medical information** and protected health information that are covered by the Confidentiality of Medical Information Act and the Health Insurance Portability and Accountability Act;
- **information collected as part of a clinical trial**;
- **sale of information to or from consumer reporting agencies**;
- personal information under the **Gramm-Leach-Bliley Act**;
- personal information under the **Driver’s Privacy Protection Act**;
- **publicly available personal information**, which is defined as information that is lawfully made available

Differences (cont'd)

There are two types of processing activities that are excluded from the scope of the GDPR: **processing conducted through non-automated means that are not part of a filing system** and **processing conducted by a natural person for a purely personal or household purpose**.

from federal, state, or local government records.

The CCPA also excludes several specific processing activities from the definition of “selling”, including:

- where a consumer uses or directs a business to intentionally disclose **personal information to a third party, via one or more deliberate interactions**. “Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer’s intent to interact with a third party”;
- sharing with third parties an identifier that signals a **consumer opted-out** from selling data;
- + where a business shares **personal information with a service provider that is necessary for a “business purpose”** as defined in the CCPA; and
- + where the business transfers the personal information to a third party as **an asset that is part of a merger, acquisition, bankruptcy, or other similar transaction**.

However, if the third party materially alters how it uses the personal information in a manner that is materially inconsistent with the promises made at the time of collection, the right to opt-out still applies.

2. Key definitions



2.1. Personal data (personal information)

“Personal data” under the GDPR and “personal information” under the CCPA are both broadly defined.

The CCPA definition provides practical examples of what “any information” that relates to an identified or identifiable person means. For example, the CCPA definition refers to information relating to households in addition to information related to individuals. Whilst the definition of personal data in the GDPR only explicitly refers to individuals, there have been numerous discussions and enforcement action across Europe showing that personal data, as defined in the law, may also cover households.

Although the GDPR does not address inferences explicitly, while the CCPA does, they may be subject to its requirements as long as they relate to identified or identifiable individuals, according to the definition of “personal data.”

Unlike the CCPA, the GDPR separately provides a definition of sensitive data (“special categories of data”) and prohibits processing of such data, unless one of the specific exemptions applies.

The CCPA provides for a definition to “biometric data,” which includes elements of the GDPR’s definition of special categories of data, such as DNA, fingerprints, and iris scans. However, the CCPA does not create a more protective regime for this category of data.

While the GDPR protects data related to health to a higher degree, since it is considered one of the special categories of data, the CCPA excludes from its protection categories of medical information, as well as data related to health collect for clinical trials.

GDPR
Articles 4(1), 9
Recitals 26 - 30

CCPA
Section 1798.140(b),(o)

Similarities

“**Personal data**” is defined as “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an **identifier** such as a name, an identification number, **location data**, an **online identifier** or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.” The GDPR also explains in its recitals that in order to determine whether a person is identifiable, “account should be taken of all the means **reasonably likely to be used**, such as singling out, either by the controller or by another person” to identify the individual directly or indirectly.

In its recitals, the GDPR specifies that **online identifiers**

“**Personal information**” is defined as “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” The CCPA further clarifies that the categories of information it enumerates are not always personal information, but they become personal information if that information identifies, relates to, describes, is capable of being associated with, or could be **reasonably** linked, directly or indirectly, with a particular consumer or household.

CCPA provides specific categories of information that may be

Similarities (cont'd)

may be considered as personal data, such as **IP addresses**, **cookie identifiers**, and **radio frequency identification tags**.

In Article 9, the GDPR also specifies the personal data that falls under special categories of personal data.

"personal information," which include, but are not limited to:

- **identifiers** such as a real name, alias, postal address, unique personal identifier, online identifier IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- **commercial information**, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- **biometric information**;
- **internet or other electronic network activity information**, that includes browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement;
- **geolocation data**;
- **audio, electronic, visual, thermal, olfactory**, or similar information;
- **professional or employment related information**;
- **education information**, provided that it is not publicly available; and
- **inferences** drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

The GDPR does **not** apply to "**anonymised**" data, where the data can no longer identify the data subject.

The CCPA does **not** apply to "**deidentified**" information or "**aggregate**" consumer information. "**Deidentified**" means information that cannot reasonably identify or be linked, directly or indirectly, to a particular consumer. "**Aggregate**" consumer information is information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device.

Differences

"Personal data" under the GDPR covers **publicly available**

"Personal information" under the CCPA does **not** cover **publicly**

Differences (cont'd)

data. Therefore, if a controller collects personal data from a publicly available source, the controller will be subject to the requirements laid down in the GDPR.

The GDPR prohibits processing of **special categories of personal data**, which is “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.” However, the GDPR provides for exceptions to the prohibition of processing “sensitive data” in certain circumstances. The GDPR defines **biometric data** as “personal data resulting from specific technical processes related to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.” **“Genetic data”** is defined separately as “personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.”

The GDPR **protects personal data related to health** to a higher standard, since it is one of the special categories of data.

available information, which is information that is lawfully made available from federal, state, or local government records, if that data is used for a purpose that is compatible with the purpose for which the data is maintained and made available in the government records for which it is publicly maintained. “Publicly available” does not include biometric information collected by a business about a consumer without the consumer’s knowledge. Therefore, such information is covered by the obligations under the CCPA.

The CCPA does not separately define nor categorise “**sensitive data**” or “special categories of personal data.” The CCPA defines **biometric data** as “an individual’s physiological, biological or behavioral characteristics, **including an individual’s deoxyribonucleic acid (DNA)**, that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.” However, the CCPA does not provide special rules for collecting and sharing biometric data. They seem to only be relevant to indicate that such data can also be personal information, as well as to indicate that the exception of “publicly available information” does not include biometric data collected by businesses without the permission of consumers.

The CCPA **excludes medical information** from its protection, to the extent it is governed by the Confidentiality of Medical Information Act. It also excludes protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, established pursuant to the Health Insurance

Differences (cont'd)

Portability and Accountability Act.

- In addition, it excludes information collected for clinical trials purposes subject to the Federal Policy for the Protection of Human Subjects, which would also include data related to health.



2.2. Pseudonymisation

The definition of “pseudonymisation” under the GDPR and CCPA is very similar in that it is the processing of personal data in such a manner that the personal data can no longer be attributed to an identified or identifiable person without the use of additional information, by putting in place technical and organizational measures which keep the additional information needed for identification separately.

Both the GDPR and the CCPA provide that controllers and businesses cannot be obliged to reidentify datasets in order to be able to comply with their obligations. However, the GDPR provides an exception to this rule concerning the rights of data subjects, to the extent that the additional information to reidentify the data is provided by the data subject himself or herself, while the CCPA specifically states that the rule also applies in the case of the right of access.

GDPR

Articles 4(5), 11
Recitals 26, 28

CCPA

Sections 1798.100(e), 1798.140(r), 1798.145(i)

Similarities

“Pseudonymisation” is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Under the GDPR, “personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered as information on an identifiable natural person.”

“Pseudonymization” is the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

The CCPA does not clearly state whether its obligations apply to personal information that has been pseudonymized.

Similarities (cont'd)

The GDPR provides that the controller cannot be obliged to maintain, acquire or process **additional information in order to identify the data subject** for the sole purposes of complying with the GDPR, if the purposes of that processing do not or do no longer require the identification of a data subject by the controller.

The CCPA provides that its rules cannot be construed “to require a business to **reidentify** or otherwise link information that is not maintained in a manner that would be considered personal information.”

Differences

The GDPR provides that the **only instance** where the controller has to **reidentify** a dataset is where the data subject provides the additional information enabling his or her identification in order for the controller to be able to comply with **requests for the rights of the data subject**.

The CCPA provides that, in the case of the right of consumers to request that a business disclose the categories and specific pieces of information it has collected, that business is **not required to reidentify or otherwise link information** that is not maintained in a manner that would be considered personal information.

2.3. Controllers and processors (businesses and service providers)



“Controllers” under the GDPR bear similarity with “businesses” under the CCPA, as both are responsible for complying with the obligations under the respective laws. Some of the obligations of the GDPR, nonetheless, also apply to “processors,” which are entities that process personal data on behalf of controllers and under the direction of controllers.

Although “processors” under the GDPR also bear similarity to “service providers” under the CCPA, when compared to the CCPA, the GDPR places more direct and detailed obligations on processors.

The GDPR requires a detailed contract or other legal act to be put in place between controllers and processors, laying out the mandate given to processors and other terms of the controller-processor relationship. Similarly, the CCPA requires that personal information is disclosed to service providers pursuant to a written contract.

GDPR

Articles 4, 17, 28, 30, 32, 33, 35, 37, 38
Recitals 90, 93

CCPA

Sections 1798.105, 1798.140, 1798.145, 1798.155

Similarities

A **data controller** is a natural or legal person, public authority,

A **business** is a **for-profit entity** that determines the purposes

Similarities (cont'd)

agency or other body that determines the **purposes and means** of the processing of personal data, alone or jointly with others.

A **data processor** is a natural or legal person, public authority, agency or other body which processes personal data **on behalf** of the controller.

Data processor activities must be governed by a **binding contract or other legal act** with regard to the controller. The contract should set out the subject matter, duration, nature and purpose of the processing, the types of personal data processed, the security measures, and the obligations and rights of the controller. Processors can only process personal data on instructions from the controller. Upon termination of the agreement with the controller, processors must return or destroy personal data at the choice of the controller. In addition, if the processor wants to engage another processor (sub-processor) it has to have the **written authorisation** of the data controller.

Requirement under the “**right to erasure**” or “**right to be forgotten**”:

- Data subjects have a right to request erasure to the controller as provided under Article 17 (see *Right to erasure* section of this Guide.)
- Upon a valid request for erasure, **controllers are obligated to take reasonable steps to have processors erase data**.
- Processors must comply with data subject's rights if required by the controller.

Liability and consequences of **non-compliance**:

- Data subjects have the right to bring an action against processors and **claim damages for "material or immaterial damage"** suffered as a result of an infringement of the processor obligations under the GDPR.
- Processors are only **liable for damage caused by processing in failure of their contractual obligations**

and **means** of the processing of consumers' personal information, **doing business in California** (see *Personal and Territorial scope* section of this Guide).

A **service provider** is a for-profit entity that processes information **on behalf** of a CCPA-covered business.

A business must disclose consumer's personal information for a business purpose pursuant to a **written contract**. The contract should prohibit the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract.

Requirement under “**right to deletion**”:

- Upon a valid consumer's request to delete personal information, a business must direct **any service provider to delete consumers' personal information**.

Liability for **misuse of personal information**:

- A service provider is liable for **civil penalties** if it uses the personal information received from businesses in violation of the CCPA.
- If a service provider fails to cure CCPA violations within 30 days, it is liable for a civil penalty under laws relating to **unfair competition** in an action brought by the Attorney General.

Differences

Other obligations imposed on processors:

- **Keep record of data processing activities:** processors are required to maintain a record of data processing activities in certain situations, including if the processor has 250 or more employees or if it processes data that is likely to result in a risk to the rights and freedoms of data subjects. The record should contain the categories of processing and any data transfers outside of the European Economic Area.
- **Implement appropriate technical and organisational measures:** processors must ensure security for processing data, which could include encryption or pseudonymization practices.
- **Data Protection Impact Assessment:** processors should assist the controller to undertake data protection impact assessments prior to the processing.
- **Appointing a DPO (Data Protection Officer):** processors must designate a data protection officer when required by the law, including where the processor processes personal data on a large scale.
- **Notify the controller of any data breach:** processors are required to notify the controller of any breach without undue delay after becoming aware of a breach.

For a business to not be considered as “selling” personal information when it shares it with a service provider for a business purpose, the service provider **must not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.**

2.4. Children

The GDPR emphasizes special protection for children and provides specific provisions for protecting children’s personal data when processed for providing information society services. The CCPA creates a special rule for children with regard to “selling” personal information, however this rule is not limited to information society services.

Under the GDPR, children under 16 must have their parents’ or guardians’ consent on their behalf, with Member States being allowed to lower that age to 13. By contrast, the CCPA introduces an opt-in requirement for selling personal information of minors between 13 and 16 years old, while parents or legal guardians are required to opt-in for minors under 13.

Another important nuance is that the CCPA allows children personal information to be “sold” only on the basis of consent, unlike the GDPR, which allows other lawful grounds than consent to be applicable for processing of children data.



Fairly consistent

GDPR
Articles 6, 8, 12, 40, 57
Recitals 38, 58, 75

CCPA
Section 1798.120(c)

Similarities

The GDPR does not define “child,” although it recognizes children as “vulnerable natural persons” that merit specific protection with regard to their personal data. Specific protection should apply when children’s personal data is used for marketing or collected for services offered directly to a child.

Where the processing is based on consent, consent of a parent or guardian is required for providing information society services to a child below the **age of 16**. EU Member States can decide to lower the age, which may be no lower than **13**. Controllers are required to make **reasonable efforts** to verify that consent is given or authorised by a parent or guardian. However, the consent of the holder of parental responsibility should not be necessary in the context of preventative or counseling services offered directly to a child.

The CCPA does not define “child.” The CCPA, however, ensures opt-in rights for minors under the age of 16.

Businesses must have opt-in consent to sell personal information of consumers under the **age of 16** if businesses have “actual knowledge” that a consumer is under 16. For consumers under the age of 13, the child’s parent or guardian must affirmatively authorize the sale of the child’s personal information. A business is deemed to have had **actual knowledge** of a child’s age if it “**willfully disregards**” a child’s age.

Differences

The GDPR does not provide for any exception for a controller that is **not aware** that it provides services to a child. It is not clear whether the consent requirement will apply if the child’s personal data is unintentionally collected online.

When any information is addressed specifically to a child, controllers must take **appropriate measures** to provide **information** relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, that the child can easily understand.

The CCPA provides for an **exception** for businesses that did not have actual knowledge of a child’s age.



2.5. Research

The GDPR has specific provisions for processing of personal data for “historical or scientific research,” as well as for “statistical purposes,” and it indicates in its recitals that scientific research should be interpreted in a “broad manner.” The GDPR provides for exceptions in this field, which include specific requirements regarding the lawful basis for processing, considering that processing for scientific research purposes is compatible with processing for any initial purpose and can thus rely on the lawful ground for that initial purpose, and a specific exception to the right of erasure. Member States are allowed to provide for derogations from the rights of the data subject where personal data are processed for scientific or historical research purposes.

The CCPA also defines research in a broad manner and it specifically mentions that processing of consumer data obtained in the course of providing a service can be further processed for research, since it will be considered compatible with the initial business purpose. However, the CCPA does not have an overarching purpose limitation principle that significantly limits the purposes for which personal information can be used by a business.

The GDPR requires that technical and organizational measures are put in place for processing of personal data for research purposes, with a focus on data minimization. Pseudonymization is offered as an example. Likewise, the CCPA requires safeguards to be put in place, but it provides a detailed list of such measures.

While the GDPR applies to clinical trials, the CCPA excludes clinical trials from its scope of application.

GDPR	CCPA
Articles 5(1)(b), 9(2)(j), 14(5), 17(3), 89 Recitals 33, 159, 160, 161	Sections 1798.105(d)(6), 1798.140(d)(6), (s), (t)(C)(ii)

Similarities

“**Scientific research** should be interpreted in a **broad manner**” and it should include technological development and demonstration, fundamental research, applied research, privately funded research and studies conducted in the public interest in the area of public health. The GDPR also refers to “historical research,” which should also include research for genealogical purposes.

Article 5(1)(b) of the GDPR requires that personal data shall be collected for specified, explicit and legitimate purposes and **not further processed for incompatible purposes**. However, it also specifies that further processing for scientific or historical research purposes “shall not be considered incompatible” with the original purpose.

The GDPR provides that processing for research purposes must

“**Research**” is defined as scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health.

Research with personal information that may have been collected from a consumer in the course of the consumer’s interactions with a business’s service or device **for other purposes is considered compatible** with the business purpose for which the personal information was collected.

The CCPA imposes specific safeguards for research conducted

Similarities (cont'd)

be subject to “**appropriate safeguards**” for the rights of the data subject, which shall ensure that technical and organizational measures are put in place in particular to ensure **data minimization**. Pseudonymization is given as an example of such measures.

on consumer information collected initially for other purposes, such as that the personal information:

- should be subsequently **pseudonymized and deidentified**, to a particular consumer;
- should be made subject to **technical safeguards** that prohibit reidentification of the consumer to whom the information may pertain; there is a specific requirement that it should be subject to **additional security controls** that allow access to this information only on a need-to-know basis;
- should be made subject to business processes that specifically **prohibit reidentification of the information and protected from any reidentification attempts**;
- should be made subject to business processes to **prevent inadvertent release of deidentified information**;
- should be used **solely for research purposes that are compatible** with the context in which the personal information was collected; and
- **not be used for any commercial purpose**.

The **right to erasure** does **not** apply to the extent that the processing is necessary for scientific or historical research purposes if erasure “is likely to render impossible or seriously impair the achievement of the objectives of that processing.”

The CCPA provides for a **research exception for erasure**, “when the businesses’ deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.”

Differences

One of the permissible uses of **special categories of personal data**, other than on the basis of consent of the data subject, is where processing is necessary for scientific or historical research purposes on the basis of Union or Member State law, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Undertaking internal research for technological development and demonstration is considered a “business purpose.” Where a service provider uses personal information of a consumer because it is necessary to perform a business purpose, such use is not considered “selling,” and therefore consumers presumably cannot opt out of it.

The CCPA excludes clinical trials from its scope of application.



3. Legal basis



The GDPR provides that the processing of personal data will only be lawful where one of the six grounds under Article 6 is fulfilled. The CCPA does not set a list of grounds that businesses must adhere to *a priori* to collecting, selling and disclosing personal information, and only provides for a *a posteriori* mechanism, namely allowing customers to opt-out to the sale and disclosure of their personal information or to ask for erasure of the information.

GDPR
Articles 5-10
Recitals 39-48

CCPA
Section 1798.120

Similarities

The GDPR provides data subjects with a right to **withdraw consent** at any time as well as a **right to object** if their personal data is processed on the basis of legitimate interest or performing of a task in the public interest.

The GDPR entails special conditions for processing of personal data of **children** for information society services (see section on *Children* of this Guide), when such processing is based on consent.

The CCPA does not have a list of “positive” legal grounds required for collecting, selling or disclosing personal information. However, consumers may ask businesses **not to sell their personal data**. In case a consumer opts-out, the business will only be able to sell and/or disclose personal information if the consumer gives their explicit permission.

The CCPA allows businesses to sell **minors’** data on the basis of consent (see section on *Children* of this Guide). However, this opt-in is only mandated for the sale of information, and is not required for the collection of information.

Differences

The GDPR states that data controllers **can only process personal data when there is a legal ground for it**. The legal grounds are: consent, or when processing is necessary for (i) the performance of a contract which the data subject is part of in order to take steps at the request of the data subject prior to the entering into a contract; (ii) compliance with legal obligations to which the data controller is subject; (iii) to protect the vital interest of the data subject or of another natural person; (iv) performance carried out in the public interest or in the official authority vested in the data controller; or (v) for the legitimate interest of the data controller when this does not override the fundamental rights of the data subject. Further permissible uses are provided for the processing of special categories of personal data under Article 9(2). As a general rule, the processing of special categories of personal data is restricted unless an exemption applies.

The CCPA **does not list the legal grounds** on the basis of which businesses can collect and sell personal information. It only provides that businesses must obtain the consent of consumers when they enter into a scheme that gives **financial incentives** on the basis of the personal information provided.

GDPR Portal

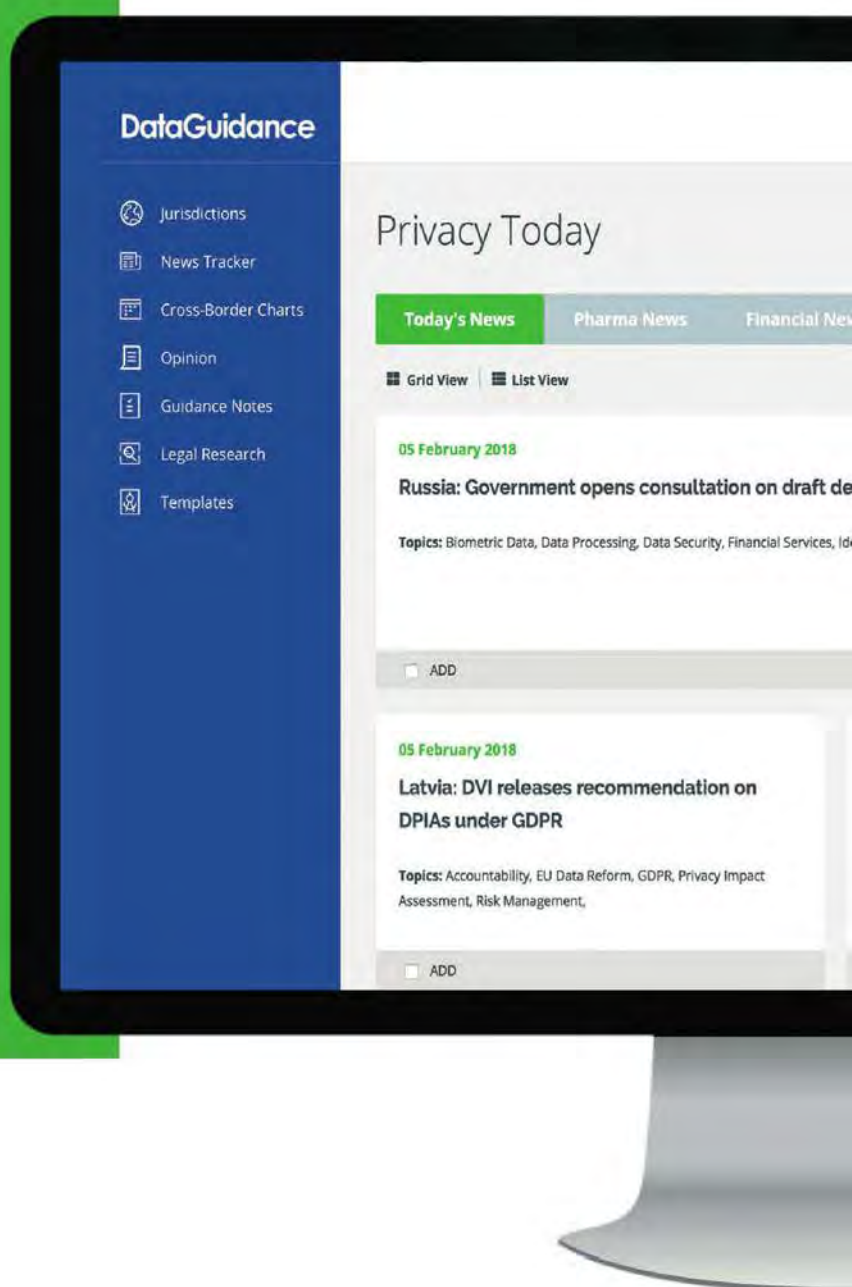
The most comprehensive resource for the development and maintenance of your GDPR programme.

- Understand obligations and requirements across key topics and sectors
- Track developments regarding Member State implementation and regulatory guidance
- Apply expert intelligence to make business decisions
- Utilise GDPR specific checklists and templates

DataGu

Global Privacy

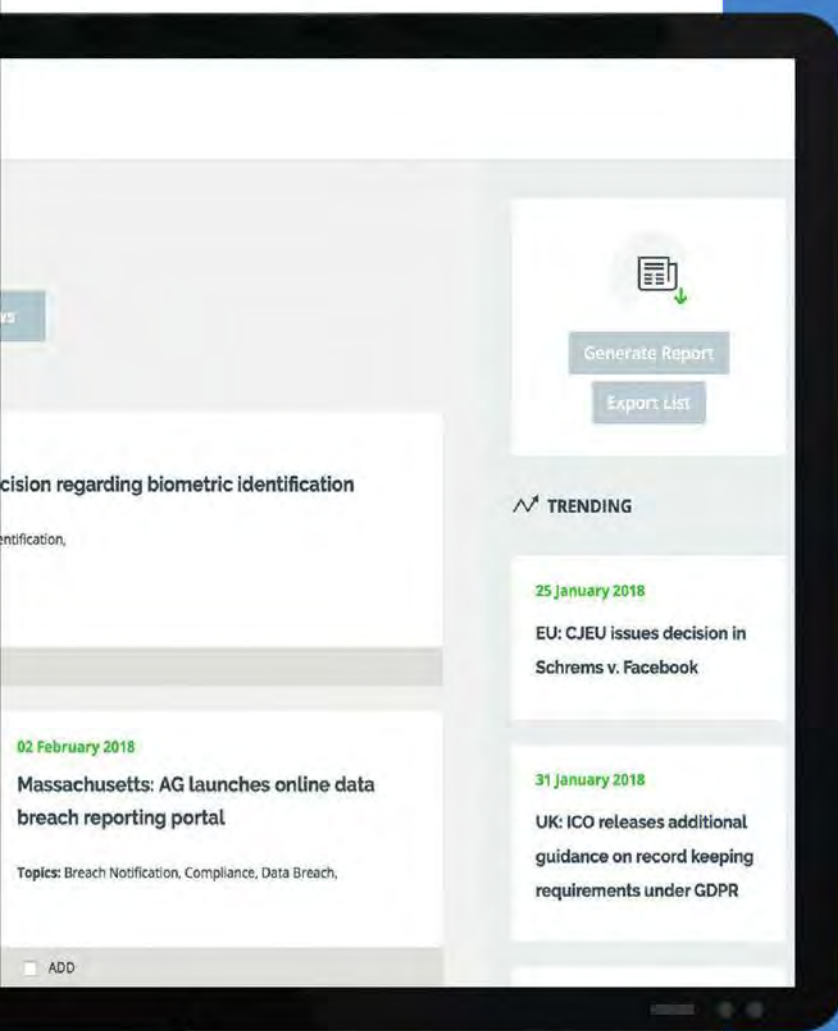
DataGuidance is a platform to monitor regulatory risk and achieve



idance

Compliance

used by privacy professionals
developments, mitigate
global compliance.



CCPA Portal

A new tool to help you understand
and prepare for the CCPA.

- Compare requirements under the GDPR to the CCPA with a dedicated comparative tool
- Employ topic specific guidance to develop your CCPA compliance plan
- Monitor CCPA news and access expert written opinion pieces on the most recent developments

DataGuidance
www.dataguidance.com

4. Rights



4.1. Right to erasure (right to deletion)

Both the GDPR and the CCPA allow individuals to request the deletion of their personal information, unless exceptions apply. Under the CCPA, the right applies to personal information that has been “collected” from the consumer. The core of this right is quite similar in both pieces of legislation, however, its scope, applicability and exemptions vary. It is worth noting that some exceptions are the same under both laws, for example: freedom of speech, processing of personal data for research purposes if erasure of that data would impair the objectives of the research and establishing or exercising legal claims.

GDPR
Articles 12, 17
Recitals 59, 65-66

CCPA
1798.105, 1798.130(a), 1798.145 (g)(3)

Similarities

The scope of this right is not limited to the data controller, but also impacts **third parties**, such as recipients, data processors and sub-processors that may have to comply with erasure requests.

This right can be exercised **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character.

The GDPR specifies that data controllers must have in place **mechanisms** to ensure that the request is made by the data subject whose personal data is to be deleted.

Data subjects must be informed that they are entitled to ask for their data to be erased.

Exceptions: among the exceptions to the right of erasure provided by the GDPR are:

- **freedom of expression** (free speech), freedom of information;
- processing for **research purposes** of personal data that, if erased, would impair the objectives of the research;
- **establishment, exercise or defence of legal claims**; and
- for **complying with a legal obligation**.

The scope of this right is not limited to the business that collects personal data but also impacts **third parties** to whom data has been sold/passed on.

This right can be exercised **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character.

The CCPA specifies that businesses must have in place **mechanisms** to ensure that the request is made by the consumer whose personal information is to be deleted.

The privacy notice must inform consumers that they are entitled to ask for the deletion of their personal information.

Exceptions: among exceptions to the right of deletion provided by the CCPA are:

- **free speech or another right provided by law**;
- processing for **research purposes**, if the deletion of personal information would render impossible or seriously impair the achievement of such research;
- processing of that personal information is necessary to protect against **illegal activity or prosecute those responsible for the activity**; and
- for **complying with a legal obligation**.

Differences

The right to erasure only applies if any of the following grounds apply, such as where consent is withdrawn and there is no other legal ground for processing, or when personal data is no longer necessary for the purpose for which it was collected.

Data subjects' requests under this right must be replied to without "undue delay and in any event within **1 month** from the receipt of the request." The deadline can be extended to **2 additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request.

Methods to submit a request include **writing, orally and by other means which include electronic means** when appropriate.

If the controller has made the personal data public, controller must take "reasonable steps, including technical measures," to inform other controllers that are processing the personal data that the data subject has requested the erasure of any links to, or copy or replication of, those personal data.

Exemptions: in addition to the exceptions enumerated under "Similarities", a data controller is also exempted to comply with erasure requests for reasons of **public interest in the area of public health**.

The CCPA does not limit the scope of this right to specific situations, categories of personal information or purposes.

The right generally applies to personal information that a business has collected from the consumer and it seems that the consumer does not have to justify his or her request.

The deadline to respond a right request is **45 days** from the receipt of the consumer's request. The deadline can be extended an **additional 45 days** when reasonably necessary, if the consumer is informed within the first 45 days, according to Section 1798.130(a). **However**, there seems to be an inconsistency in the current text of the law. In another provision, which generally refers to exceptions to the law (Section 1798.145), the CCPA states that "the time period to respond to any verified consumer request may be extended by up to **90 additional days** where necessary, taking into account the complexity and number of the requests."

The CCPA states that at least two or more designated methods for submitting requests must be provided by the business including, at a minimum, a toll-free telephone number, and if the business maintains an internet website, a website address.

Exemptions: in addition to the exceptions enumerated under "Similarities", a business is not required to comply in the following circumstances:

- to perform a **contract between the business and the consumer**;
- **detect security incidents**, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity;
- **debug to identify and repair errors that impair existing**

Differences (cont'd)

intended functionality;

- to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business; or
- otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.



4.2. Right to be informed

Both the GDPR and the CCPA include prescriptive provisions with regards to the information organizations must provide to individuals when collecting and processing their personal information. In particular, both pieces of legislation prescribe when information must be given to the individuals and what they must be informed of.

Unlike the GDPR, the CCPA does not distinguish between the notice for collecting information directly from individuals and the notice when information is obtained from other sources.

GDPR
Articles 5, 12, 13, 14
Recitals 58 - 63

CCPA
Sections 1798.100(b), 1798.130(a), 1798.135

Similarities

The GDPR states that information on the following must be provided to individuals:

- the **categories** of personal data processed;
- the **purposes** of processing; and
- the **existence of data subjects' rights** and the contact details of the data protection officer.

The GDPR states that information must be provided to data subjects by controllers at the time when **personal data are obtained**, when the personal data is collected directly from

The CCPA states that information on the following must be provided to individuals:

- the **categories** of personal information to be collected;
- the **purposes** for which collected personal information is used; and
- If a business sells personal information about the consumer to third parties, the rights of the consumers and the methods to exercise such rights must be given to consumers. This includes a link to the '**Do Not Sell My Personal Information Page**' where consumers can exercise their right to opt-out.

The CCPA states that businesses must inform customers **before or at the point of collection**.

Similarities (cont'd)

data subjects.

Data controllers **cannot** collect and process personal data for purposes other than the ones about which the consumers were informed, unless they provide them with further information.

Businesses **cannot** collect additional personal information without telling the consumers what information is collected and for which purpose, unless they provide them with further information.

Differences

The GDPR also states that information on the following must be provided to individuals:

- identity of the controller;
- contact details of the data protection officer;
- the legitimate interest of the data controller or the third party;
- the recipients or categories of personal data;
- transfer of data to third parties;
- data retention period;
- the right to withdraw consent at any time;
- the right to lodge a complaint with a supervisory authority.
- when data is necessary for the performance of a contract, the possible consequences of not doing so; and
- the existence of automated decision-making including profiling, including the logic involved and consequences of such processing.

The GDPR provides specific information that must be given to the data subject **when their data is collected by a third party**, which include the sources from which data was collected. Notice must be given within a reasonable period after obtaining the data, but at the latest within one month; or at the time of the first communication with the data subject; or at the latest when personal data are first disclosed to a recipient.

The CCPA also states that information on the following must be provided to individuals:

- the categories of personal information collected/sold/disclosed for business purposes in the previous 12 months; and
- alternatively, if no personal information was sold, that should be written in the privacy policy.

There is a specific requirement that consumers receive “**explicit notice**” when a third party intends to sell personal information about that consumer that has been sold to the third party by a business.

The CCPA specifies that the **privacy policy must be updated every 12 months**.



4.3. Right to object (right to opt-out)

Both the GDPR and the CCPA guarantee a right for individuals to ask organizations to cease the processing, and selling respectively, of their data.

The CCPA requires that a link with the title “Do Not Sell My Personal Information” is provided on the homepage of the business. Additionally, the CCPA provides that any third party that received personal information pursuant to their “selling” can only further sell that personal information if consumers are provided “explicit notice” and the opportunity to opt-out of this subsequent “selling.”

Under the CCPA, consumers can only opt-out of the sale of personal data, and not the collection or other uses that do not fall under the definition of “selling.” By contrast, individuals can object to any type of processing of personal data under the GDPR – either by simply withdrawing consent, or by objecting to processing that is based on legitimate interest, or on necessity for a task in the public interest.

The CCPA right to opt-out of personal information is absolute, while the GDPR general right to object has a specific exception where the controller demonstrates compelling legitimate grounds for the processing that override the rights and interests of the data subject.

GDPR
Articles 12, 21
Recital 70

CCPA
Sections 1798.120, 1798.135

Similarities

Data subjects have several ways to opt-out of processing of their personal data:

- they can **withdraw consent**;
- they can **exercise the general right to object** to processing that is based on legitimate interests or on a task carried out in the public interest; or
- they can **object to processing of their data** for direct marketing purposes.

Information about this right and on how to exercise it must be included in the **privacy notice**. In particular, in the context of direct marketing, opting-out must be as easy as opting-in.

Consumers have the right to **opt-out from selling of their personal information**. They also have the right to opt-out from the subsequent selling of their personal information by a third party that received personal information after an initial “selling.” The third party shall not sell the personal information unless the consumer has received “explicit notice” and is provided an opportunity to opt-out.

If a business sells consumers’ personal information, information about this right must be given to consumers in the **privacy notice**. Moreover, a **link to the page ‘Do Not Sell My Personal Information’** must be included in the homepage of the business. The CCPA allows businesses to create a dedicate homepage for California consumers.

Differences

The GDPR provides data subjects with the **right to object** to the processing of their personal data when the processing is based on the legitimate interest of the controller or a third party. The data controller would have to cease processing personal data unless it demonstrates that there are compelling legitimate grounds to continue the processing. Moreover, the data subject has the right to object to processing for direct marketing as well as to withdraw consent at any time.

The GDPR does **not** prescribe the specific language to be used.

The CCPA provides consumers with a right to opt-out from the selling and/or disclosing for business purposes of their personal information. The opt-out can therefore only stop the selling of personal information, and it does not impact other uses of their information. However, the right to opt-out of the sale is **absolute**, in the sense that businesses cannot reject an opt-out request on the basis of their compelling legitimate grounds.

Businesses must adhere to the language provided in the CCPA, namely the homepage of their website must have a link titled 'Do Not Sell My Personal Information.'

4.4. Right of access

Both the GDPR and the CCPA establish a right of access, which allows individuals to have full visibility of the data an organization holds about them: they can obtain details about the data being processed, but also copies of the data items themselves.

The two laws present some differences, for example, in relation to the procedure organizations should follow to comply with an individual's request. In addition, the CCPA provides that whenever access is granted to consumers electronically, the information must be in a portable and, to the extent possible, readily useable format that allows the consumer to transmit the information to another entity.



GDPR

Articles 12, 15, 20
Recitals 59, 63, 64

CCPA

Sections 1798.100, 1798.110,
1798.130, 1798.145 (g)(3)

Similarities

The GDPR states that, when responding to an access request, a data controller must indicate the **purposes** of the processing; the **categories of personal data** concerned; the **recipients or categories of recipients** to whom personal data have been disclosed to; and **any sources** from which data was collected. The GDPR specifies that individuals also have the right to receive a **copy** of the personal data processed about them.

The CCPA states that, when responding to an access request, a business must indicate the **categories of personal information** collected/sold; the **categories of sources** from which the personal information is collected; the business or commercial **purpose** for collecting or selling personal information; and the **categories of third parties** with whom the business shares personal information. The CCPA specifies that individuals also have the right to be given access to the pieces of personal information collected about them.

Similarities

Data subjects must have a variety of means through which they can make their request, including through **electronic means and orally**. When the request is made through electronic means, the data controller should submit the response through the same means.

The GDPR specifies that data controllers must have in place **mechanisms** to ensure that the request is made by the data subject whose personal data is requested access to.

The GDPR states that data subjects can exercise this right **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character.

Consumers must be given at least two methods to make their request to access their personal information, notably via a **tool-free phone or a webpage**. The business may send the response via mail or electronic means.

The CCPA specifies that businesses must have in place **mechanisms** to ensure that the request is made by the consumer whose personal information is requested access to.

Disclosure and delivery of personal information as required by the right of access must be **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character.

Differences

The right applies to all the personal data collected and processed about the data subject making the request. Under the GDPR, the data controller must include further information in the response to a request of access, notably, the retention period, the right to lodge a complaint with the supervisory authority, the existence of automated decision making, and existence of data transfers.

Data controllers can refuse to act on a request when it is manifestly unfounded, excessive or has a repetitive character.

Data subjects' requests must be complied without "**undue delay** and in any event within **1 month** from the receipt of the request." The deadline can be extended an **2 additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request.

The GDPR has a **distinct right to data portability**, which applies under its own specific conditions (see below).

The right applies **only** to personal information collected in the **12 months prior to the request**.

Businesses are not required to provide access to personal information more than twice in 12 months.

The deadline to respond to such a right is **45 days** of receipt of the consumer's request. It could be extended an **additional 45 days**, but notice should be given to the consumer within the first 45 days. However, there seems to be an inconsistency in the current text of the law that allows an extension to **90 days**, under a different provision (see *Right to erasure* section of this Guide).

The CCPA states that when businesses provide data

Differences (cont'd)

electronically to the consumer this data should be sent in a **portable and readily usable format** that allows for the transmission of this data to **third parties**. The CCPA provides that this must be done only when technically feasible.

4.5. Right not to be subject to discrimination for the exercise of rights



The CCPA introduces the right not to be subject to discrimination for the exercise of rights under the CCPA. This right is not explicitly included in the GDPR, however, some provisions can be found in the GDPR that are based on the same principle.

GDPR
Articles 5, 22
Recitals 39, 71-73

CCPA
Section 1798.125

Similarities

The GDPR does **not include an explicit provision** stating that a data subject must not be discriminated on the basis of their choices on how to exercise their data protection rights. However, it is implicit from the principles of the GDPR that individuals must be protected from discriminatory consequences derived from the processing of their personal data. For example, Article 5 states that personal data must be processed 'fairly'; Article 13 states that data subjects must be informed of the consequences derived from automated decision-making; and Article 22 specifies that individuals have the right not to be subject to automated decision-making that has a legal or significant effect upon them. Additionally, the GDPR emphasizes that when processing is based on consent, in order for consent to be valid, it must be freely given. Consent is not considered freely given if the data subject has no genuine or free choice or is unable to refuse or "withdraw consent without detriment."

The CCPA states that consumers **must not be discriminated because of the exercise of their rights** under the CCPA.

Differences (cont'd)

The GDPR does not explicitly include this right and therefore **no scope is defined**.

The CCPA defines the scope of this right by stating that consumers must not be discriminated against because of the exercise of their rights under the CCPA, which means they must not be:

- **denied goods or services;**
- **charged different prices or rates for goods or services**, including through the use of discounts or other benefits or imposing penalties;
- **provided a different level or quality of goods or services;** and
- suggested they will receive a **different price or rate for goods or services.**

It has to be noted that businesses can set up schemes for providing **financial incentives**, but consumers must **opt-in** to become part of them.



4.6. Right to data portability

Both the GDPR and the CCPA recognize a right to data portability. The CCPA considers data portability as part of the right to access, while the GDPR provides for a separate and distinctive right.

GDPR
Articles 12, 20
Recital 68

CCPA
Sections 1798.100, 1798.110,
1798.130, 1798.145 (g)(3)

Similarities

Data subjects have the **right to receive their data processed on the basis of contract or consent in a "structured, commonly used, and machine-readable format"** and to transmit that data to another controller without hindrance.

The GDPR states that consumers can exercise this right **free of charge**. There may be some instances where a fee may be requested, notably when the requests are

The CCPA states that when businesses provide data electronically to the consumer following an access request this data should be sent in a **portable and readily usable format that allows for the transmission of this data to third parties** without hindrance.

The CCPA states that consumers can exercise this right **free of charge**. There may be some instances where a fee may be requested, notably when the requests are

Similarities (cont'd)

unfounded, excessive or have a repetitive character.

Data subjects must have a variety of means through which they can make their request, including through **electronic means and orally**. When the request is made through electronic means, the data controller should submit the response through the same means.

The GDPR specifies that data controllers must have in place **mechanisms** to ensure that the request is made by the data subject whose personal data is requested access to.

The GDPR provides that this must be done only when **technically feasible**.

unfounded, excessive or have a repetitive character.

Consumers must be given at least two methods to make their request to access their personal information, notably via a **tool-free phone or a webpage**. The business may send the response via mail or electronic means.

The CCPA specifies that businesses must have in place **mechanisms** to ensure that the request is made by the consumer whose personal information is requested access to.

The CCPA provides that this must be done only when **technically feasible**.

Differences

The right to data portability **only** applies to the **personal data** that has been **provided by the data subject** themselves and that is processed on the basis of **consent or contract** and the processing is carried out by **automated means**.

Data controllers must respond without **undue delay** and in any event **within 1 month** of receipt of the request. It could be extended an **additional 2 months**, but notice should be given to the data subject within the first month.

In addition to having data subjects receive personal data under the right to data portability, the GDPR **extends this right to having the personal data transmitted directly from one controller to another**.

The right to data portability is an **extension of the right to access**, and therefore it is subject to the same limitation (e.g. it only applies to data collected in the previous 12 months).

Businesses must respond within **45 days** from receipt of the request. It could be extended an **additional 45 days**, but notice should be given to the consumer within the first 45 days. However, there seems to be an inconsistency in the current text of the law that allows an extension to **90 days**, under a different provision (see *Right to erasure* section of this Guide).

The CCPA's right is limited to allowing consumers receive personal information, and it does **not** extend to having a business transfer the information to another business.



MISSION

The mission of the Future of Privacy Forum is to serve as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies.

WHO WE ARE

FPF brings together industry, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.

VISION

We believe that...

- Technological innovation and new uses of data can help solve big societal problems and improve lives.
- Technological innovation must be accompanied by responsible data practices.
- It is possible to build a world where technological innovation and privacy can coexist.
- It is possible to reach consensus on ethical norms, policies and business practices to address new privacy challenges.

OUR SUPPORTERS

FPF works with the privacy leaders at 175 companies and in partnership with leading academics and civil society organizations. We are supported by industry, charitable foundations and governments.

ENGAGE WITH US

Stay up-to-date on our work by following us at @futureofprivacy on social media. Visit our website and subscribe to our mailing list: <https://fpf.org/subscribe>.

5. Enforcement



5.1. Monetary penalties

Both the GDPR and the CCPA provide for the possibility for monetary penalties to be issued in cases of non-compliance. However, the nature of the penalties, the amount and the procedure to be followed differ quite significantly.

GDPR Articles 83, 84 Recitals 148 - 152	CCPA Section 1798.155
---	--------------------------

Similarities

The GDPR provides for **monetary penalties** in case of non-compliance.

The CCPA provides for **monetary penalties** in case of non-compliance.

Differences

Administrative fines can be directly issued by a data protection authority.

Depending on the violation occurred the penalty may be up to either:

- **2% of global annual turnover or €10 million**, whichever is higher; or
- **4% of global annual turnover or €20 million**, whichever is higher.

The amount of the penalty may also vary depending on “the nature, gravity and duration of the infringement,” the nature of the processing, the number of data subject affected, and the damages suffered, the negligent or intentional character of the infringement, etc., with a complete list in Article 83(2) of the GDPR.

The administrative fine can be imposed directly by the competent data protection authority taking into account that several data protection authorities may be involved if the violation involves more than one Member State.

Civil penalties can be issued meaning that the penalty is issued by a court.

Depending on the violation occurred the penalty may be up to:

- **\$2,500 for each violation;**
- **\$7,500 for each intentional violation.**

CCPA does not provide for a maximum amount that can result for the imposition of several penalties for each violation.

Any violation of the CCPA is assessed and recovered in a civil action brought by the **Attorney General**.



5.2. Supervisory authority

Both the GDPR and the CCPA provide for an authority to supervise the application of the law and to assist organizations in understanding and complying with it. However, the two designated supervisory authorities, the Attorney General and the national data protection authorities under the CCPA and the GDPR respectively, have different investigatory and enforcement powers.

Additionally, it has to be noted that, in the European Union, national data protection authorities form part of the European Data Protection Board, a body that ensures the consistent application of the GDPR across Europe.

GDPR
Articles 51-84
Recitals 117 - 140

CCPA
Sections 1798.155, 1798.185

Similarities

Data protection authorities have the task to **promote awareness and produce guidance** on the GDPR.

The Attorney General is expected to create **regulations** "on, but not limited to," specific areas of the CCPA.

Differences

Data protection authorities have **investigatory powers** which include to: "conduct data protection audits, access all personal data necessary for the performance of its tasks, obtain access to any premises of the data controller and processor, including equipment and means."

The Attorney General has the power to **assess a violation** of the CCPA. The CCPA does not specify which activities are included in this assessment.

Data protection authorities have **corrective powers** which include: "issuing warnings, reprimands, to order the controller and processor to comply, order the controller to communicate a data breach to the data subject, impose a ban on processing, order the rectification or erasure of data, suspend the transfer of data and impose administrative fines."

The Attorney General has the power to assess alleged violations of the CCPA and to bring action before the court for civil penalties, which include **monetary penalties and injunctions**.

The GDPR does not regulate how data protection authorities are funded, this being left to the Member States to decide.

The monetary penalties collected through civil actions under the CCPA form the **Consumer Privacy Fund**, which funds the activities of the Attorney General in this sector.

The GDPR states that data protection authorities must act in "**complete independence when performing their tasks**," which also means that they must be free from financial control by having a separate and dedicated budget.

The Attorney General has the power to **independently start investigations** and actions against alleged non-compliance from businesses.



5.3. Civil remedies for individuals

Both the GDPR and the CCPA provide individuals with a cause of action to seek damages for privacy violations. In addition, both laws allow for class or collective actions to be brought against organizations.

However, it has to be noted that under the GDPR, an action can be brought for any violation of the law, while the CCPA provides a cause for action only with regard to the failure of security measures and in the context of data breaches.

GDPR
Articles 79 - 82
Recitals 141 -147

CCPA
Section 1798.150

Similarities

Both the GDPR and the CCPA provide individuals with a cause of action to seek damages for violation of privacy laws with regard to security measures violations and data breaches.

Both the GDPR and the CCPA provide individuals with a cause of action to seek damages for violation of privacy laws with regards to security measures violations and data breaches.

Differences

Any violation of the GDPR can trigger the claim for judicial remedies. Data subjects can claim both **material and non-material damages**.

This remedy is **only allowed** when non-encrypted or non-redacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of security obligations.

The GDPR allows Member States to provide for the possibility for data subjects to give a mandate for representation to a non-for-profit association, association or organisation that has as its statutory objective the protection of data subject rights.

Prior to initiating any action against a business for statutory damages on an individual or class-wide basis, businesses are provided 30 days' written notice including a reference to the alleged violations. If the violation is "cured" within 30 days and no further violation is claimed, no action is initiated. The CCPA further states that "no notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement."

Differences (cont'd)

The GDPR does not provide any figure for potential damages.

The amount of damages is established by Statute.

Damages could be in an amount not less than \$100 and not greater than \$750 per consumer per incident or actual damages, whichever is greater.

Index: CCPA articles

Section 1 (1798.100)	Rights of access, information and portability with businesses that collect PI*
Section 2 (1798.105)	Right of erasure for PI against businesses that collect PI
Section 3 (1798.110)	Right of access for PI against businesses that collect PI
Section 4 (1798.115)	Right of access for PI against businesses that sell or disclose PI Opt-out from third party selling PI
Section 5 (1798.120)	The right to opt-out from selling PI Parent consent for selling childrens' PI (the right to opt-in)
Section 6 (1798.125)	Non-discrimination of consumers for exercising their rights
Section 7 (1798.130)	Modalities to comply with consumer requests Right to information (online privacy policy) Staff training
Section 8 (1798.135)	"Do Not Sell My Data" link
Section 9 (1798.140)	Definitions of key concepts
Section 10 (1798.145)	Exceptions and restrictions
Section 11 (1798.150)	Private right of action for data breaches
Section 12 (1798.155)	Civil penalties Consultation of the Attorney General
Section 13 (1798.185)	Attorney General implementing regulations
Section 14 (1798.192)	Prohibition to contractually waive consumer rights
Section 15 (1798.196)	Relationship with other state laws and with federal law
Section 16 (1798.198)	Entry into force
Section 17 (1798.199)	Entry into force
Section 18	Urgency statute

(*PI = Personal Information)

A VISUAL GUIDE TO PRACTICAL DATA DE-IDENTIFICATION

What do scientists, regulators and lawyers mean when they talk about de-identification? How does anonymous data differ from pseudonymous or de-identified information? Data identifiability is not binary. Data lies on a spectrum with multiple shades of identifiability.



This is a primer on how to distinguish different categories of data.

DEGREES OF IDENTIFIABILITY

Information containing direct and indirect identifiers.

PSEUDONYMOUS DATA


































Information from which direct identifiers have been eliminated or transformed, but indirect identifiers remain intact.

DE-IDENTIFIED DATA

Direct and known indirect identifiers have been removed or manipulated to break the linkage to real world identities.

ANONYMOUS DATA

Direct and indirect identifiers have been removed or manipulated together with mathematical and technical guarantees to prevent re-identification.

	EXPLICITLY PERSONAL	POTENTIALLY IDENTIFIABLE	NOT READILY IDENTIFIABLE	KEY CODED	PSEUDONYMOUS	PROTECTED PSEUDONYMOUS	DE-IDENTIFIED	PROTECTED DE-IDENTIFIED	ANONYMOUS	AGGREGATED ANONYMOUS
 DIRECT IDENTIFIERS Data that identifies a person without additional information or by linking to information in the public domain (e.g., name, SSN)	 INTACT	 PARTIALLY MASKED	 PARTIALLY MASKED	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED
 INDIRECT IDENTIFIERS Data that identifies an individual indirectly. Helps connect pieces of information until an individual can be singled out (e.g., DOB, gender)	 INTACT	 INTACT	 INTACT	 INTACT	 INTACT	 INTACT	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED
 SAFEGUARDS and CONTROLS Technical, organizational and legal controls preventing employees, researchers or other third parties from re-identifying individuals	 NOT RELEVANT due to nature of data	 LIMITED or NONE IN PLACE	 CONTROLS IN PLACE	 CONTROLS IN PLACE	 LIMITED or NONE IN PLACE	 CONTROLS IN PLACE	 LIMITED or NONE IN PLACE	 CONTROLS IN PLACE	 NOT RELEVANT due to nature of data	 NOT RELEVANT due to high degree of data aggregation
SELECTED EXAMPLES	Name, address, phone number, SSN, government-issued ID (e.g., Jane Smith, 123 Main Street, 555-555-5555)	Unique device ID, license plate, medical record number, cookie, IP address (e.g., MAC address 68:A8:6D:35:65:03)	Same as Potentially Identifiable except data are also protected by safeguards and controls (e.g., hashed MAC addresses & legal representations)	Clinical or research datasets where only curator retains key (e.g., Jane Smith, diabetes, HgB 15.1 g/dl = Csrk123)	Unique, artificial pseudonyms replace direct identifiers (e.g., HIPAA Limited Datasets, John Doe = 5L7T LX619Z) (unique sequence not used anywhere else)	Same as Pseudonymous, except data are also protected by safeguards and controls	Data are suppressed, generalized, perturbed, swapped, etc. (e.g., GPA: 3.2 = 3.0-3.5, gender: female = gender: male)	Same as De-Identified, except data are also protected by safeguards and controls	For example, noise is calibrated to a data set to hide whether an individual is present or not (differential privacy)	Very highly aggregated data (e.g., statistical data, census data, or population data that 52.6% of Washington, DC residents are women)

Message

[REDACTED]

From: Ariel Fox Johnson [REDACTED]
Sent: Friday, December 21, 2018 1:45 PM
To: Lisa Kim [REDACTED]; Stacey Schesser [REDACTED]; Nicklas Akers
[REDACTED]
Cc: Elizabeth Galicia [REDACTED] Samantha Corbin [REDACTED]
Subject: Children Under 16 / Right to Opt In

Stacey, Lisa, and Nicklas,

We wanted to send the following suggestions re: children and opting in. Please let us know if you have any questions, happy to discuss!

Enjoy the holiday season,

Ariel

Ariel Fox Johnson

Senior Counsel, Policy and Privacy | [Common Sense Media/Kids Action](#)

[REDACTED]

www.common sense media.org

CCPA00000825

INITIAL SUBMISSION RE CCPA REGULATIONS - RIGHT TO OPT-IN

To: Office of the Attorney General, California

From: Common Sense Media

Date: December 21, 2018

This submission offers proposed guidance regarding the right to opt-in. Rulemaking is required under Section 1798.185(a)(4) for the right to opt-out; as the right to opt-in is a similar right, Common Sense believes guidance would be helpful to give businesses and families more clarity and certainty.

CCPA Section 1798.120(c): Under CCPA, a business may not sell a child under 13's personal information unless a parent or guardian has affirmatively authorized such sale (the "right to opt-in"). For minors ages 13, 14, and 15, the minor him or herself must affirmatively authorize the sale. Businesses must refrain from selling the personal information of consumers they know are under 16. Businesses cannot willfully disregard a consumer's age.

Proposed regulatory language:

Children under 13: A parent or guardian may affirmatively authorize the sale of a child under 13's personal information (the "right to opt-in"). Such authorization must be both (i) affirmative and (ii) reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent or guardian. Affirmative authorization includes a verifiable consumer request, made specifically by the parent or guardian, in response to a clear and conspicuous disclosure detailing the business's sale of personal information. Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include:

- (i) Providing a consent form to be signed by the parent and returned to the business by postal mail, facsimile, or electronic scan;
- (ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;
- (iii) Having a parent call a toll-free telephone number staffed by trained personnel;
- (iv) Having a parent connect to trained personnel via video-conference;
- (v) Having a parent communicate in person with trained personnel;
- (vi) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the business from its records promptly after such verification is complete.

To the extent a business is also seeking verifiable parental consent under federal law to comply with the Children's Online Privacy Protection Act and Rule, 16 CFR 312 , it must obtain separate affirmative authorization to sell a child's information under CCPA.¹

Children ages 13, 14, and 15: A child aged 13, 14, or 15 may affirmatively authorize the sale of his or her personal information (the "right to opt-in"). Affirmative authorization includes a verifiable consumer request, made by the teen, in response to a clear and conspicuous disclosure detailing the business's sale of personal information. The disclosure must be appropriate to the teen's age and level of understanding.

Additional considerations:

Children visiting sites, services, and businesses should not have the misimpression that companies are selling their information, when the default is companies are not allowed to sell their information. One way to achieve this would be to require that businesses do not have any "Do Not Sell" link, button, or logo in such situations; or that they have a link, button, or logo indicating the business is not at present selling the child's information. See the first paragraph below for suggested language.

In addition, when children have opted-in to the sale of their information, they should be able to opt-out at any time in just as simple a manner as an adult can. Businesses should assume as much from the statutory language. However, to the extent additional guidance is helpful, the second paragraph below offers suggested language.

Additional potential regulatory language:

Websites, services, and businesses who have identified, or probabilistically identified, consumers under 16, or whose sites, services, and businesses are directed to consumers under 16, shall, to the extent technically feasible, display a button, link, or logo that indicates businesses are not presently selling the consumer's personal information, in a manner that is clear and obvious to the consumer and appropriate to the consumer's age and level of understanding.

If a consumer under 16's opt-in rights are exercised, a business shall provide the Do Not Sell opt-out button, link, or logo. A consumer, or the consumer's parent or guardian, shall be able to subsequently opt-out by following the standard opt-out procedures. A consumer, or the consumer's parent or guardian, as applicable, shall be able to opt-out at anytime.

¹ NOTE: This is consistent with federal requirements which state that "An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties." 16 CFR 312.5(a)(2).

Message

From: Cynthia Pantazis [REDACTED]
Sent: Friday, February 08, 2019 2:00 PM
To: Eleanor Blume [REDACTED] Nicklas Akers [REDACTED]
Cc: Mufaddal Ezzy [REDACTED]
Subject: Google/CCPA

Ellie: Attached please find our initial comments on CCPA. We would be happy to discuss at any point and appreciate the opportunity to engage on this important issue.

If you have any questions, please let us know.

Best,

Cynthia

--

Cynthia Pantazis

Director, Policy and State Affairs

Google LLC

25 Massachusetts Avenue, NW

Washington, DC 20001

[REDACTED]

[REDACTED]



February 8, 2019

Ms. Eleanor Blume
Special Assistant Attorney General
Office of the Attorney General
455 Golden Gate, Suite 11000
San Francisco, California 94102-7004

Dear Ms. Blume:

Below please find Google's initial comments on the California Consumer Privacy Act of 2018 (CCPA). We look forward to engaging in productive conversations on these issues, both with your office and as part of the broader legislative process.

Introduction

Google supports strong and balanced privacy laws to protect individuals' personal information and to foster and maintain the trust that enables innovation. Our users entrust us with their data and we take that responsibility seriously, continuously striving to ensure that our privacy and security controls, policies, and practices earn and maintain that trust. Over the last two years, for example, we have engaged in a company-wide effort to prepare for the European Union's General Data Protection Regulation (GDPR), further improving on the robust information and tools we provide to users and on Google's industry-leading privacy program.

In line with our historical focus on these issues, Google supports the underlying goals of the CCPA -- to establish legal protections for the privacy and security of California consumers. Our purpose is not to weaken the CCPA or eliminate these protections, but to address issues raised by the law, encourage alignment of the CCPA with other leading privacy regimes, and obtain additional clarity on the law's obligations.

We believe the CCPA should be implemented in a manner that provides users with a meaningful ability to control and to obtain information about and access to their data, while protecting the privacy of others and providing a practicable framework for compliance. While we also support legislative amendments to clarify and refine certain aspects of the law, regulatory guidance could substantially help to clarify a number of these issues and avoid problematic

interpretations of ambiguous provisions. In addition to the initial comments we provide below, we look forward to participating in your office's rulemaking process.

Clarifying the CCPA's definitions and obligations to more closely align with other privacy regimes like the GDPR, protect the privacy of third parties, and provide certainty to covered businesses

As discussed above, Google supports strong privacy rights for consumers and has the practical experience of providing users with the ability to exercise a range of these rights under the GDPR and other privacy laws. Although some commentators have suggested that the CCPA simply extends GDPR's protections to California users, there are a number of potentially important differences and ambiguities that could make the CCPA's obligations both less practicable and less protective of user privacy.

To align the CCPA with other leading privacy regimes and ensure that it provides users with the ability to exercise these rights under a robust and predictable framework, we believe that a number of provisions in the law would benefit from clarification and further guidance, as detailed below. While this letter does not address every issue we believe is raised by the CCPA, we include the areas of clarification that we believe are the most urgent to address.

Personal information

The CCPA's definition of "personal information" is ambiguous and potentially overbroad, and should be clarified to align with existing understandings of that term, such as the Federal Trade Commission's guidance or the GDPR.

The definition of "personal information" is the foundation of the law's substantive obligations and will be central to nearly every aspect of compliance with it. Although improved by Senate Bill 1121 (Dodd, 2018), the definition retains significant ambiguities that could engender confusion throughout the law and lead to a number of unintended consequences. For example, the definition's operative standard continues to refer to information that is "capable of being associated with" a consumer or "household," which some commentators have suggested could encompass nearly any information a business maintains.

To ensure a consistent, meaningful, and appropriate application of the CCPA's substantive requirements, we believe that regulatory guidance should clarify that the law's definition of "personal information" is aligned with commonly accepted understandings of that term. These include, for example, the definition of personal information proposed by the FTC, namely, information that is linked to, or could reasonably be linked to, a particular individual or device,

and does not encompass information only theoretically “capable” of being connected to any person or “household.”¹

An overly broad definition of “personal information” not only risks confusion about the core scope of the law, but also eliminates incentives for businesses to maintain information in a less identifiable and more privacy-protective manner. Appropriate distinctions between “personal information” and less identifiable forms of data that cannot reasonably be linked to a particular individual are a critical feature of other privacy regimes like the GDPR, and encourage businesses like Google to identify where they can store and process data that has been de-identified or anonymized rather than keep all data in an identifiable state. A clear and consistent definition of “personal information” thus both serves privacy interests and enables businesses to continue developing and improving products and services under a practicable compliance framework.

Below we address some of the practical and potentially countervailing privacy problems that such a broader interpretation may cause with respect to particular CCPA obligations.

Access

Regulatory guidance should clarify the CCPA’s data access provisions to provide a framework under which businesses can engage with users requesting data to both confirm their identities and provide them with the information they are seeking while protecting others’ privacy.

Google provides users with a wide range of data access tools and dashboards, as well as responds to specific subject access requests under the GDPR. Based on our experience fulfilling these requests, we believe there are a number of important protections that enable businesses to both engage productively with users to identify the information being requested and ensure that competing rights and interests are taken into account when producing responsive information.

For example, the GDPR enables businesses to both request more specific information about the nature and scope of a request, and to consider the rights and interests of other persons when responding to these requests. In reviewing potentially responsive information, we consider and mitigate potential impacts on the privacy of other persons identified in the relevant information, as well as impacts on other public interests like law enforcement or intellectual property. Recognizing the potential need for additional elaboration and flexibility on these rights, the GDPR also enables Member States to further refine the scope of these obligations to account for other important public interests.

¹ See, e.g., “Protecting Consumer Privacy in an Era of Rapid Change,” FTC Report (Mar. 2012), *available at* <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

While the CCPA contains stray references to some of these concepts, section 1798.100 does not establish a clear framework under which these sometimes competing rights and interests can flexibly be evaluated once a user has made an access request. We support statutory amendments to expand and clarify this framework, but also believe the AG could help in some areas to make clear that a business has the flexibility to engage with users to appropriately tailor access requests, and then to carefully assess other rights and interests potentially implicated by producing responsive information.

Equally important, we believe regulations should clarify that “verifiable consumer request” is a meaningful and robust standard that enables businesses to ensure that a user requesting information has the right to receive that information, as well as that complying with the request does not adversely impact the privacy of others. While the CCPA currently appears to preclude a business from requiring a user to create an account to submit an access request, non-account-based requests for information associated with frequently-shared identifiers like IP addresses raise a number of substantial privacy concerns. Access to a secured account from which information is being requested has proven the most reliable indicator of a requesting user’s identity and their entitlement to receive information associated with the relevant identifier. Absent such a showing, these kinds of requests can be exploited by fraudsters, other malicious actors, and even domestic abusers.

From both a privacy and compliance perspective, ensuring appropriate standards for identity verification is a critical issue that requires careful attention to countervailing privacy risks as well as flexibility for businesses to develop mechanisms that ensure appropriate and secure user access.

Deletion

The CCPA’s deletion framework should similarly be clarified to more closely align with the standards established by the GDPR, which enable businesses to carefully weigh user deletion requests against other legitimate grounds for retaining data.

As with data access and portability, Google maintains a suite of tools enabling users to delete specific information from Google’s servers, or to delete their accounts entirely. This includes providing dashboards to remove particular products or services or even particular activity data from a user’s account, as well as responding to specific “erasure” requests under GDPR. Like many of the CCPA’s requirements, section 1798.105 is frequently unclear and fails to articulate a meaningful framework under which to consider these requests. For example, rather than provide for a balancing test to carefully weigh a user’s deletion request against a business’s legitimate grounds for retaining data, the CCPA delineates a number of ambiguous exclusions that businesses can rely upon when denying such a request. We believe these exclusions -- as well as the contours of the deletion framework more generally -- would benefit from greater clarity and guidance, such as on the scope of information subject to the deletion right.

Service providers

The CCPA's treatment of "businesses" and "service providers" should be clarified and aligned with similar distinctions in other privacy frameworks like the GDPR. Clearly distinguishing between companies that provide services directly to consumers and those acting as service providers or "vendors" for other businesses is critical to ensuring appropriate and clear responsibility for complying with the law's obligations. Service providers (or "processors" under GDPR) should be able to rely on the business (or "controller" under GDPR) to meet the primary obligations under the law, such as transparency, control, and access, while focusing on more programmatic and security responsibilities. Google, along with others in the industry, offers a wide range of enterprise services under this legal framework, which tens of thousands of businesses -- particularly small businesses without their own network infrastructures -- rely on for their daily operations, and to minimize additional compliance costs. These distinctions also ensure that service providers without a direct relationship to a business's customers are not exercising that business's substantive responsibilities.

The CCPA echoes and even borrows some language from the GDPR's distinction between "controllers" and "processors," but suffers from remaining ambiguities concerning the precise requirements for entities to qualify as "service providers," as well as the scope of those entities' responsibilities. To ensure a consistent and appropriate application of the CCPA's various obligations, we believe that regulations should clarify that the law's service provider framework is aligned with GDPR and existing commercial relationships.

Clarifying the CCPA's "sale" requirements to align with common understandings of that term and to provide users with meaningful control over the sharing of their personal information while preserving legitimate and routine data practices

Google supports providing users with strong controls over their personal information, and makes available and continuously improves a range of tools for users to choose the types of data collected and used in our services. In preparation for the GDPR, for example, we improved many of our data access tools and provided users with more granular controls over their information. Compared to the GDPR and other leading privacy regimes, the CCPA's "sale" opt-out requirements are narrower and less empowering for users, but nevertheless contain inflexible obligations that could make them difficult to implement in a clear and privacy-protective manner. In particular, rather than require controls across a business' data processing, based on the risk posed to the user or the type or sensitivity of the relevant data, the CCPA is focused almost exclusively on a category of disclosures the law refers to as "sales," which are confusingly defined and subject to prescriptive requirements that could lead to user confusion about the treatment of their information.

As described below, these requirements are susceptible to overbroad readings that could have important and unintended consequences on a range of services, including those basic to many

online services and the Internet more generally. While Google continues to work with the legislature to consider reforms to better align the CCPA's user controls with the approach taken in other leading privacy regimes in the U.S. and around the world, we believe that regulatory guidance can and should clarify the meaning of "sale," as detailed below.

Sale opt-out

Google does not sell our users' personal information, and supports the regulation of data brokering activities to impose robust transparency and control requirements on these practices and to help build greater trust across the marketing and advertising industry. As our Privacy Policy commits, we do not share our users' personal information outside of Google or Google's authorized service providers unless a user separately and specifically consents to that sharing, or under narrow, specified circumstances, such as responding to a law enforcement request or during an emergency. These foundational principles and commitments extend to Google's advertising services, which help keep many of our services free for users without sharing their personal information with third parties.

Google's approach to protecting user data is consistent with our [support for risk-based privacy regulation](#), focused on the risk of harms posed to individuals and communities by specific types of data processing, with remedies and enforcement proportional to these harms. As part of that approach, organizations should be required to account for and mitigate these privacy risks, with particular care to sensitive information or types of processing that can pose a significant risk to individuals. Indeed, nearly every privacy regime in the world incorporates these concepts, providing businesses the ability to evaluate these risks and engage in a productive dialogue with regulators and users about the appropriate balance in a particular context, and to provide users with appropriate and tailored controls over their information.

The definition of "sale" under the CCPA, however, is vague and subject to a number of critical ambiguities that could render it untethered from both the common meaning of that term and the risks that can flow from the actual sale of personal information. Construed too broadly, these requirements could impose a confusing and arbitrary standard on numerous forms of routine and legitimate transfers of data on the Internet, potentially interfering with a wide range of activities that have never been understood as the "sale" of personal information or as posing a risk to consumers. In particular, under such a reading, the applicability of these obligations would be unrelated to the type of data transferred or the purposes for which the data is transferred, and instead based on whether the relevant activities are determined to have occurred in a context in which a business is receiving any form of benefit or "consideration" -- an extraordinarily vague standard unrelated to the risks posed to a user by the relevant data processing.

In light of the significant uncertainty posed by these broader interpretations, we believe regulatory guidance should clarify that the CCPA's definition of "sale" is aligned with common understandings of that term, namely where a business directly exchanges personal information

for monetary compensation, and excludes circumstances where data is transferred not for monetary or other direct value, but in order to facilitate the basic operation of a website or other commonly used product or service. That construction would align with the stated intention of the legislation's sponsors to regulate data brokering activities and offer users direct control over the sale of their information, while preserving routine, legitimate, and transparent data practices that support a wide array of services relied upon by users. As noted above, Google supports laws requiring appropriate user controls for such processing activities, but not under the confusing label of "sale" or with prescriptive requirements on how these controls need to be presented to users.

Minors

Additional guidance on the CCPA's provision on minors should clarify that the law's "knowledge" standard for triggering these obligations is consistent with longstanding federal guidelines and existing age screening mechanisms.

Google maintains an industry-leading account structure to enable parents to manage and protect their children's privacy online, and, as discussed above, does not sell the personal information of our users, regardless of age. While the CCPA's age-related requirements adopt language from the Children's Online Privacy Protection Act (COPPA), including COPPA's "actual knowledge" standard for determining when a business is considered aware of a user's status as a minor, section 1798.120 has also caused confusion by introducing additional language about the "willful disregard" of age-related information. Read broadly, this provision creates uncertainty about whether businesses are obligated to collect and/or associate additional information about potential minor users, rather than relying on the longstanding FTC guidance that businesses are not required to investigate the age of their users and can rely on users' self-declared age collected via neutral age screening mechanisms.

COPPA and the FTC's careful guidance implementing the law has struck an appropriate balance on the issue of age verification, reflecting the important principle of data minimization. We believe that regulations should therefore clarify that the "knowledge" standard contained in section 1798.120(c) remains consistent with the FTC's guidance under COPPA.

Non-discrimination

Finally, the CCPA's non-discrimination obligation would benefit from additional guidance clarifying that its exemptions permit reasonable distinctions based on a user's choices about data processing, and do not prohibit a wide range of advertising-supported products and services.

These provisions appear to appropriately prohibit businesses from retaliating or otherwise penalizing users for exercising their rights under the law, but also contain a number of ambiguities that could interfere with a wide range of popular and free advertising-supported

products and services. In particular, we believe that additional guidance should be provided on the “value”-based exemptions from the prohibition, to clarify that section 1798.125 enables a business to make reasonable and sometimes necessary distinctions between differently situated users, such as where a user’s exercise of the rights in the CCPA -- requesting deletion of information, for example -- directly impacts the business’s ability to offer a feature or service, or more generally support the revenue model of that feature of service. This would help clarify that businesses can enable users to exercise rights under the CCPA without compromising the ability to offer their services, and would more generally ensure that businesses can continue to fund and to offer -- and that consumers can continue to choose from -- a vibrant ecosystem of free, diverse, advertising-supported products and services.²

Conclusion

We appreciate the opportunity to provide our initial comments and suggestions on needed clarifications to the CCPA. We would be happy to answer and discuss any questions that you have.

Sincerely,

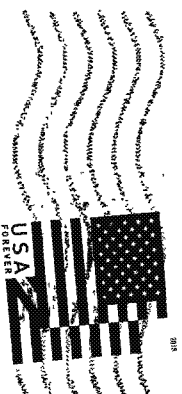
A handwritten signature in black ink that reads "Cynthia Pantazis". The signature is fluid and cursive, with the first name "Cynthia" written in a larger, more prominent script than the last name "Pantazis".

Cynthia Pantazis
Director, Policy and State Affairs

² As one example of these requirements’ potential impact, and the need for flexibility to preserve advertising-supported services, the Austrian Data Protection Authority recently concluded that GDPR’s prohibition on making the provision of a service conditional on a user’s “consent” was not violated by a newspaper offering users a choice between an advertising-supported experience or a paid subscription. The decision took into account the relatively minimal “detriment” of the subscription fee paid by the user for not having consented to personalized advertising, as well as the newspaper’s fundamental need to maintain a viable method of generating revenue. A stricter reading of these kinds of requirements, including of section 1798.125 of the CCPA, could pose substantial problems for these services’ ability to maintain their business, by requiring them both to provide content but without the advertising necessary to fund it. See, e.g., “Validity of consent coupled with free online services - Chair of EDPB opens a path,” Baker McKenzie (Jan. 25, 2019), *available at* <https://www.lexology.com/library/detail.aspx?g=5125ca7c-84fa-483f-aa8d-ded39dc98442>.



SAN FRANCISCO CA 940
11 FEB 2019 PM 5:1



XAVIER BECERRA
ATTORNEY GENERAL, STATE OF CALIFORNIA
1300 "I" STREET
SACRAMENTO, CA 95814-2919

RE: CALIF. CONSUMER PRIV. ACT

95814-298332



Feb. 10, 2019

OFFICE OF THE ATTORNEY GENERAL - STATE OF CALIFORNIA
1300 I STREET
SACRAMENTO, CA. 95814-2919

MR. BECERRA

I'm writing to you (Unfortunately it was not obvious on the AG website how to simply e-mail a comment) to express my support of enactment of the CALIFORNIA CONSUMER PRIVACY Act.

As reported in the Santa Rose Press Democrat on Sunday Feb. 10, 2019, this law has been passed but is yet to be put into effect. At issue, according to reports, are changes the industry to be regulated wishes to make. What a surprise. There are now LOBBYING GROUPS sponsored by Google, Facebook "and other businesses beyond Silicon Valley" working to defend these companies from being regulated on behalf of citizens. Unbounded ability of companies to siphon "consumer data" and exploit a citizen's habits, needs, income and such is something that must not be permitted and relying on "self-policing" on the part of corporations is unwise and ineffective.

Consider this — who lobbies for me? For my rights? For my financial and other data to be protected? For transparency of all business transactions I may enter into?

Please enact the CALIFORNIA CONSUMER PRIVACY Act without the de-fanging being requested by some of the largest, wealthiest, most powerful companies on earth, who rely on citizens' not knowing exactly how information obtained — usually unknowingly —

is being used, often against their own best interest.

And please excuse the hand-written letter, as my printer is out of ink and your website lacks a simple option for communicating one's ideas or thoughts to the Attorney General.

Thank you.

B. Hogue
Bonnie Hogue

PS - who does lobby on behalf of the citizens?



Federal Housing Finance Agency

MEMORANDUM

March 8, 2019

TO: Laura Stuber
California Department of Justice
Office of the Attorney General

FROM: Alfred Pollard *Alfred Pollard*
General Counsel
Federal Housing Finance Agency

RE: Privacy Regulation (for Regulation Coordinator)

Following our conversation regarding the rulemaking process to implement the California Consumer Privacy Act of 2018 (the Act), I am providing information for consideration by the Office of the Attorney General.

The Federal Housing Finance Agency oversees Fannie Mae, Freddie Mac and the eleven Federal Home Loan Banks. Together, they support mortgage financing support for millions of mortgages across the country and in California. As federally chartered institutions, they are subject to coverage by applicable federal laws and supervision by this Agency.

Legislation. The California Legislature recognized, through the inclusion of an exemption for information subject to the federal Gramm-Leach-Bliley Act (GLBA), that personal information required to create and service a mortgage loan is already subject to a comprehensive legal framework, including consumer privacy regulation. It also recognized that a GLBA exemption is critical to avoid adverse impact on currently regulated business practices in the mortgage industry. Further, mortgage transactions are created with full consumer knowledge and at their request.

Investor Clarification. This communication highlights a clarification that would assist California consumers to continue to enjoy full access to mortgage financing in their role as investors in addition to access in their personal financial roles.

California residents as mortgage investors should be treated the same way as residents in their role as mortgage borrowers. Private individuals can access mortgage financing to acquire multiple properties, in many instances to rehabilitate them and place the properties back into the market. The same information gathering and sharing requirements pertain to commercial loans as apply to loans made for personal purposes. And, as is true for data shared by individuals for personal financial purposes, a panoply of existing federal and state laws protects the data individuals share in their role as investors, including the Fair Credit Reporting Act, the Federal Trade Commission Act, and the California Security Breach Notification Law, to name a few.

20

Nevertheless, the term “consumer” in the Act is not clear. In this regard, the definition of consumer in the Act does not align with California SB 1 or GLBA and other federal consumer protection statutes, which clearly do *not* extend to activities engaged in for investment purposes. As a result, the Act could create unintentionally obstacles to the types of data sharing that needs to occur to originate, service and securitize loans made to individuals for investment purposes.

This issue could be remedied by clarifying that the term “consumer” in the Act means “a natural person *interacting with a business for personal, family or household purposes.*” [Emphasis added.]

I would be happy to answer any questions on this subject as the rulemaking process continues. I may be reached at [REDACTED]

Message

From: Amal Amal [REDACTED]
Sent: 2/26/2019 6:19:10 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulator]
Subject: Fwd: Comments for Pending Privacy Regulations- AB 375- CCPA
Flag: Follow up

Not having received confirmation that the DOJ received these comments pertaining to the pending privacy regulations, this information is forwarded to your attention once more. If possible, please confirm receipt of this email. Thank you.

Begin forwarded message:

From: [REDACTED]
Date: February 8, 2019 at 1:29:49 PM PST
To: "PrivacyRegulations@doj.ca.gov" <PrivacyRegulations@doj.ca.gov>
Subject: Comments for Pending Privacy Regulations- AB 375- CCPA
Dear Department of Justice (DOJ):

Thank you for the opportunity to comment on the pending privacy regulations per Assembly Bill 375 (the California Consumer Privacy Act of 2018- CCPA).

Issue:

It is now common practice for insurance companies to use the CarFAX database to rate new and existing consumers who purchase automobile policies with their companies. (CarFAX is an entity that acquires and stores vehicle-related information like DMV information, sales records, maintenance records, mileage, accident reports, etc.) Some of the information on CarFAX is public (i.e., DMV vehicle registration and sales records), but most of CarFAX's information is not publicly attainable. **It is the acquisition of this data that is objectionable.** It is respectfully requested that the DOJ consider this issue when promulgating its CCPA regulations to protect California consumers from this common and unlawful data acquisition.

Facts:

Insurance companies are accessing the information tied to a Vehicle Identification Number (VIN) which is obtained by CarFAX. CarFAX is acquiring this information from service dealerships and repair shops (cumulatively referred to as "shops") who contract with CarFAX. These shops sell or give this information to CarFAX, and sometimes in exchange for free or discounted use of the CarFAX database. This database is populated via unsuspecting consumers visiting those shops to obtain maintenance or repair services. Without notice, or permission thereof, consumer information is then uploaded to CarFAX on an agreed upon and regular schedule; data is usually in the CarFAX database within 2-3 days of the consumer's visit.

As a result of the above, automobile owners who are seeking, or who already have, insurance with specified companies are being rated, and possibly even being denied coverage, in part based on the CarFAX information that is obtained. Consumers are never advised of this practice, or provided an opportunity to object to, or opt out of, this third party sharing of information. In fact, the shops believe that because they are not providing owner names, addresses, or other specific personally identifiable information (i.e., birth date, social security numbers, driver's license numbers, etc.), they have a right to give that information to CarFAX. In addition, insurance companies are denying culpability as well because they say they are not involved in the original exchange of the information, merely third party beneficiaries thereof. This said, all the parties involved readily agree that this process assists them in either insuring, or further selling, or buying, the vehicle in question when maintenance records, mileage, and other vehicle-specific information (i.e., accident repairs) are stored via a third party vendor. However, those same parties readily admit that they never contemplated such easy access to this information, and are merely taking advantage of a loop-hole in the system. In fact, CarFAX, which is a non-California-domiciled company, is also taking advantage of this loop-hole in California law, and all seem to be conspiring to the detriment of California's residents.

Consequences:

This unbridled process is harming consumers in a number of ways, including, but not limited to, the ability to re-sell those vehicles and/or acquire reasonable automobile insurance thereon. When insurance companies use the CarFAX data to rate, or even deny coverage to, these unsuspecting consumers, and, consumers are finding it difficult to sell their vehicles with damaging information posted to CarFAX, this process should deserve much greater scrutiny. To complicate things further, consumers do not have the ability to easily rebut the information on CarFAX, correct errors to the data, or defend themselves against the improper use of such information (i.e., like they would for medical records), particularly if they are not even aware of the practice. Finally, it is an incorrect presumption by the shops that such information is NOT personally identifiable because the VIN eventually, and inextricably, is traced back to the current or new owner of the vehicle, who then struggles in dealing with its improper use and disclosure. It is uncontroverted that vehicles do not repair themselves; consumers (usually the owners) are taking them in to shops to get repaired. As such, the activities and services of those consumers are being tracked without their express permission, and in violation of the spirit of California's privacy laws.

Conclusion:

All of the above is a breach of confidential information that is the exclusive property of the consumer (the owner of the VIN information), and the entire process, as described above, should be unlawful. Therefore, the Attorney General should consider non-public information, tied to California consumers' VIN, as personal information that should be protected from disclosure, and allow every consumer the right to know of its third-party use and prospective dissemination prior to any disclosure, and with the full opportunity to "opt out" if they so wish.

Thank you for your time in reading these comments regarding the CCPA.

Please be so kind as to acknowledge receipt of this email. Thank you.

Message

From: Fitzsimon, Leo [REDACTED]
Sent: 3/8/2019 10:56:06 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Rudolph, Matthew [REDACTED]
Subject: HERE Technologies
Attachments: HERE Technologies CA AG Letter.pdf

Dear Privacy Regulations Coordinator:

Attached please find the written comments of HERE Technologies submitted in response to preliminary activities by the Attorney General in the CCPA rulemaking process. If you should have any questions about our filing or need additional information from us, please do not hesitate to contact either me or HERE's Privacy Officer Matthew Rudolph (copied).

Thank you for the opportunity to provide comments and for considering HERE's views.

Best regards,

Leo Fitzsimon



Leo Fitzsimon

HERE Technologies

Government Relations – Americas

1250 H Street, NW



Washington, DC 20005





March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA90013

Re: California Consumer Privacy Act Rulemaking

Dear Attorney General Xavier Becerra:

HERE Technologies ("HERE") respectfully submits these comments regarding preliminary rulemaking activities by your office as part of the development of implementing regulations for the California Consumer Privacy Act ("CCPA" or "Act"). We appreciate the opportunity to provide our views on the Act itself and our recommendations for improving outcomes for both industry and California consumers.

About HERE Technologies

HERE Technologies is a global leader in digital location technology. Our products and services enable people, enterprises and cities around the world to harness the power of location and create innovative solutions that make our lives safer, more efficient, productive and sustainable. We transform information from devices, vehicles, infrastructure and many other sources into real-time location services that play a key role in how we move, live and interact with one another. HERE's vision is to create an autonomous world for everyone, based on open availability of the vast amounts of data that will be generated by the hundreds of billions of connected devices in our increasingly connected world.

HERE Technologies is fully committed to respect privacy and to comply with all applicable laws covering data protection and privacy. As a company which is already subject to robust privacy regulations such as the European General Data Protection Regulation, we support and are prepared to comply with consumer privacy protections like those represented in the CCPA. We are, however, concerned that some elements of the proposed CCPA will have detrimental effects on the functioning of our location services and on the benefits of these services for our end users. Moreover, some of the proposed requirements risk hampering innovation and may therefore have a negative impact on the further development and maximization of location services in California.

We wish to highlight the following key aspects of the CCPA that are of particular concern to HERE Technologies and the location services we provide:

Scope of Personal Data

As a provider of location services across multiple industries from transportation, to logistics, to media, as well as to public sector entities, HERE processes location data in many different use cases, which may or may not involve personal data. A location could relate to a person, or a parcel, or a sensor or other internet-enabled devices.

HERE seeks clarity regarding the degree to which location information must be associable to a specific individual or household to constitute personal information within the scope of the CCPA. HERE would



support concepts which rely on a combination of the location data with personal identifiers or other factors which result in it actually being possible to associate the location data with a particular individual or household. HERE believes that this interpretation is supported by the existing statutory language and would merely require clarification within the pending regulations to be issued by the California Attorney General. HERE looks forward to contributing to the discussions surrounding anonymization, de-identification, and the definition of “personal information”.

HERE therefore supports issuance of regulations which define “personal information” based on actual associability of the data to a specific individual or household, rather than blanket definitions relying on data types.

Guidance for Multi-Provider Service Offerings

HERE is concerned that the limited data sharing methods outlined by the CCPA will restrict the development of joint or multi-party service offerings. One factor that has led to the vibrant digital ecosystem currently enjoyed by California consumers is the ability of separate businesses to combine and leverage their independent services into new and creative solutions.

The CCPA recognizes three types of transfers: sale to third parties, disclosure to service providers for business purposes, and disclosures to third parties at the direction of a consumer. HERE believes that this third type of transfer, disclosure at the direction of the consumer, represents a way to permit the consumer to be fully informed of how their data is being used and disclosed, while still providing consumers with the benefits that collaboration and cooperation between technology providers can foster.

HERE believes that so long as businesses provide adequate transparency and choice to consumers, it is possible for businesses to continue to offer these multi-party services in a way which respects the privacy of consumers. HERE would encourage the California Attorney General to focus on issuing guidance for what it means for a consumer to “direct” disclosure of their data in a way that permits flexible but transparent interaction between platform providers.

The potential adverse impact of an inflexible data sharing regime is particularly visible when considering use cases which involve Machine-to-Machine (M2M) communications, such as in connected and/or autonomous vehicles and internet of things applications. In these use cases, exchange of data involves communication between multiple actors, such as vehicles, infrastructure and road users, requiring near real-time communication in order to have a meaningful impact on efficiency and traffic safety.

Because multiple independent actors are involved in these use cases, it is impractical for them to all act as service providers to one another. Likewise, such interactions should not be regarded as a “sale” of personal data, since they involve multiple voluntary participants within a communications framework. The “directed disclosure” concept reflected in Section 1798.140(t)(2)(A) of the CCPA may provide a workable framework for this type of multi-participant environment, provided that the means of “direction” are sufficiently flexible.



HERE believes that providing clear up-front notice and choice to consumers represents the best way to balance consumer protections and consumer control with the flexibility needed to encourage the continued growth of innovative service models.

This is analogous to how HERE operates in compliance with EU Regulations. In that context, HERE operates many of its services as a “data controller”, which means that HERE takes direct responsibility to end users of its products for its processing of their personal information. This relationship is established by placing strict requirements on use of HERE services to ensure that end users are informed of how HERE will process their data. HERE has demonstrated its commitment to ensuring transparency to its end users through engaging in workshops with its customers, offering terms and guarantees directly to end users, and validating notice and consent implementations for certain collection activities.

HERE therefore requests that the determination of whether an individual “directs” disclosure of personal data to third parties includes circumstances where independent services are bundled within a service offering, provided that the user is provided with appropriate transparency regarding the identities and privacy practices of the third parties involved.

Fulfillment of Individual Requests Related to Personal Data

As a global company operating subject to European privacy regulation, HERE already extends rights to consumers who use HERE products globally. These include the right to access and request deletion of personal information held by HERE, the right to be informed about our processing practices, and restrictions on how and to whom we may transfer this data. Accordingly, HERE is positioned well to comply with, and in many cases exceed, the protections provided to consumers under the CCPA.

However, there are several areas where HERE supports regulation clarifying the requirements of the CCPA to provide flexibility for businesses to better support exercise of consumer rights under the CCPA.

Data Retention

HERE seeks clarification that the CCPA does not require businesses to retain specific pieces of personal information solely to meet the 12-month disclosure requirement of the CCPA. The CCPA requires disclosures of specific pieces of data collected cover the 12 months prior to the date of a consumer request. The CCPA includes an exception for data connected to a single transaction, or for data which is maintained in a format which does not “identify or otherwise link” an individual.

One area of ambiguity is information which is related to repeated transactions which the business does not maintain for a full 12 months. HERE believes that one of the best ways to ensure that individual privacy is respected is to adhere to the principles of storage limitation and data minimization. These practices dictate that if a business does not actually need to retain consumer data, the business should dispose of that data as soon as practicable.

HERE requests clarification that businesses are not required to retain 12 months' worth of consumer personal information by issuance of regulation clarifying that deletion of data in the normal course of business is sufficient to meet the obligations imposed under the CCPA.

Toll-Free Number

The CCPA requires that businesses maintain at least two methods to permit consumers to submit requests, including at minimum a toll-free number. This requirement to maintain a toll-free number is unique in comparison to other privacy laws in the United States and globally (including the GDPR). While HERE approves of the desire to make exercise of consumer privacy rights as easy as possible, we believe that fulfilling these requests via a phone number is impractical in many use cases. We also believe that this requirement encourages business practices which impose additional risks on consumers, while providing little corresponding benefit in many cases.

HERE views this as a “know your customer” issue – specifically, many online businesses do not actually know who their customers are, and do not collect sufficient information upon customer sign-up to validate the individual's identity. Rather, individuals are often known only through an email address, device identifier, or even a random identifier such as an account ID. In order to make it possible to link a caller to a specific account or user, the business would have to either collect additional information on user sign-up, or would have to invent an alternative method of authentication, which even where possible will likely require directing the user back to completing actions within the application or device.

Additionally, most requests permitted under the CCPA cannot be completed solely over a phone call. Rather, they would require provision of detailed information which is best consumed in written format such as lists of data types collected, lists of third-party disclosures, and detailed data usage information. As such, we believe that requiring a toll-free number in all cases would serve to introduce additional opportunity for error into the process, without eliminating the need for using other communications methods to complete the request.

HERE would request that the Attorney General take these practical considerations into account in creating regulations regarding how businesses should implement this call center requirement. HERE would encourage a standard which permits businesses to redirect consumers into an electronic workflow, especially where the customer primarily interacts with the business through electronic means. An example of this would be permitting businesses to send confirmatory emails which validate that the requesting individual owns the account in question and provides instructions for exercise of privacy rights via electronic means.

Data Portability

HERE seeks clarity regarding the extent to which the requirement that personal data be “portable” requires interoperability between different service providers.



To the extent that California wishes to encourage interoperability of data portability standards, HERE would support encouraging industry groups to agree on standards for interoperability within their industry. However, such standards do not currently exist, and this would necessarily be a long-term effort requiring significant organization and planning. It would likely be impossible for most businesses to comply with strong interoperability requirements at this point.

HERE supports standards which would allow businesses to deliver access to data held about consumers in a standardized format which can be read using commonly available tools. If interoperability requirements are to be introduced, HERE would request a delayed implementation with an initial period of industry engagement to permit industry stakeholders to agree upon common frameworks for data portability between services.

HERE therefore supports an interpretation of “portability” which does not include interoperability requirements until adequate time has been given for industry groups to decide upon common frameworks.

Method of Delivery of Personal Data

The CCPA requires that responses to requests for access to a consumer’s information be delivered “through the consumer’s account with the business, if the consumer maintains an account with the business”. It is unclear whether this would require a built-in “data take out” mechanism for access to personal data or other automated functionality within a user account, or if a business could fulfill these requests via other methods of communication.

HERE views mandating specific in-account mechanisms for data management to be too restrictive in light of the variety of use cases which exist for products and services dealing with consumer information. For example, in many use cases there are significant limitations due to screen size, connection bandwidth, or data input and output mechanisms to allow for a user to effectively request or receive information within the product or service.

Instead, HERE would support a flexible approach to permit businesses to determine how best the information may be communicated, while still adhering to the content and timing requirements laid out in the CCPA. This may include methods such as email correspondence, secure document exchange portal, or even physical mail if it is appropriate in context.

HERE would welcome clarification from the California Attorney General supporting flexible options for methods to communicate content requested by a consumer.

Conclusion

As noted above, HERE is a global leader in digital location technology and our products and services help consumers, businesses and governments around the world use location data and create innovative solutions that make our lives safer, more efficient, productive and sustainable. As a data-driven company, we are keenly aware of privacy considerations and are fully committed to complying



with all applicable data protection and privacy laws. We hope the foregoing observations and suggestions are helpful as you engage in the process of developing regulations to implement the CCPA and we would be happy to discuss our views with your office at your convenience.

Respectfully submitted,

/s/ Matthew Rudolph

Matthew Rudolph
Privacy Officer
HERE Technologies

Message

From: Kevin McKinley [REDACTED]
Sent: 3/8/2019 4:57:09 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Internet Association Comments on CCPA Initial Rulemaking
Attachments: Internet Association Comments on California Consumer Privacy Act of 2018 Initial Rulemaking.pdf

I have attached Internet Association's CCPA comments.

Thank you,

--



Kevin McKinley

Director, California Government Affairs



INTERNET ASSOCIATION

1303 J Street, Suite 400, Sacramento, CA 95814



March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013
Via email: privacyregulations@doj.ca.gov

Re: *Internet Association Comments on California Consumer Privacy Act of 2018 Initial Rulemaking*

To Whom It May Concern:

Internet Association (“IA”) welcomes the opportunity to comment on the CCPA regulations. IA’s mission is to foster innovation, promote economic growth, and empower individuals through the free and open internet. IA is the only trade association that exclusively represents leading global internet companies on matters of public policy.

IA companies believe trust is fundamental to their relationship with individuals. Our member companies know that to be successful they must meet individuals’ reasonable expectations with respect to how the personal information they provide to companies will be collected, used, and shared. That is why our member companies are committed to transparent data practices, and to continually refining their consumer-facing policies so that they are clear, accurate, and easily understood by ordinary individuals. Additionally, our member companies have developed numerous tools and features to make it easy for individuals to manage the personal information they share, as well as their online experiences.

IA Rulemaking Comments

IA companies support many of the privacy-enhancing concepts that motivated provisions of the CCPA, such as consumer rights to access, deletion, transparency, and choice.¹ Notwithstanding IA’s support for these concepts, IA has significant concerns with how these were implemented in the actual statutory text of the CCPA. For example, in some cases a literal reading of the statutory text creates direct conflicts between provisions. We urge the Attorney General to use care in crafting regulations to pay particular attention to the indications of intent in the text of the CCPA and take a common-sense approach to interpreting the meaning of its provisions. It would be unfortunate if the lack of clarity or conflicts in the statute were amplified in the implementing regulations.

¹ See IA [Privacy Principles for a Modern National Regulatory Framework](#).

**Topic I: Additional Categories of Personal Information**

IA does not believe that additional categories of personal information need to be added at this time.

California Civil Code section 1798.185, subdivision (a)(1), directing the AG to consider additional categories of personal information, was part of the original passage of CCPA in the form of Assembly Bill No. 375 (2017-2018 Reg. Sess.). At that time, the definition of personal information contained a list of categories of personal information in section 1798.185, subdivisions (o)(1)(A)-(K). Subsequently, the Legislature passed Senate Bill No. 1121 (2017-2018 Reg. Sess.) which changed this list from *per se* personal information to an instructive list of potential categories of personal information by adding the language “includes, but is not limited to.” This statutory change obviates the need for expanding upon the list.

Furthermore, the list of categories of personal information does not need to be expanded because it is already broad. Some have asserted the definition is appropriate because it is based on current law. However, the definition in the CCPA comes from a narrow California law focused on disposing of physical documents. The definition of personal information in California Civil Code section 1798.80, subdivision (e) takes a broad approach, but in the narrow context of ensuring data is disposed of properly.

The broad definition of personal information in the CCPA creates concrete and easily foreseen risks for California consumers in the specific contexts of access and deletion. As further discussed below, in Topic IV: Submitting and Responding to Consumer Requests, the inclusion of the term “household” creates not only privacy risks for consumers, but very real dangers to their physical safety. Even if “household” was not included in the definition of the personal information explicitly, the inclusion of specific identifiers which do not always trace back exclusively to a single consumer, for example an Internet Protocol address, create the potential that a single individual could access or delete the personal information—*e.g.*, biometrics, geolocation, search history—for another consumer, simply because there is a shared IP address. Even if the legislature had not included “household” in the definition of personal information, between the arguably low standard² required to correlate information to a consumer and the definition of the term “unique personal identifier” the statute would still arguably have the practical effect of allowing individuals *other than the specific consumer to whom personal information relates* to obtain access to or deletion of personal information based on anything from a former romantic relationship or being roommates to using a business center at a hotel or a wifi network at a coffee shop. Many of the specific types of identifiers included in the definition of “unique identifier” are also not always individually identifying as recognized by the inclusion of the terms “family or device.” For example, telephone numbers are recycled, devices may be shared, and cookies can be placed based on a one-time log-in to a website on a borrowed device.

² See, *e.g.*, “capable of being associated with” in definition of personal information. (Civ. Code, § 1798.140, subd. (o)(1).)



For these reasons, IA respectfully requests that the Attorney General carefully consider the impact of the arguably overbroad definition of “personal information” and craft regulations that clarify that businesses are not required to respond to access and deletion requests in ways that require the businesses to make determinations as to which common identifier is associated with a specific individual or respond to requests in ways that may negatively impact other consumers.

Topic II: Updating the Definition of Unique Identifiers

IA does not believe any additional unique identifiers should be added through regulations and reiterates its comments to Topic I, above, on whether the listed categories of personal information should be expanded as the concerns are equally applicable to unique identifiers, as is also described above. For these reasons, IA respectfully requests that the Attorney General carefully consider the impact of the arguably overbroad definition of “personal information,” including the definition of “unique identifiers,” and craft regulations that clarify that businesses are not required to respond to access and deletion requests in ways that require the businesses to make determinations as to which common identifier is associated with a specific individual or respond to requests in ways that may negatively impact other consumers.

Topic III: Exceptions for State and Federal Laws

Please see below, IA’s comments to Topic IV, Question 2. Complying with Consumer Requests, Compliance with Federal and State Laws, for input that may be relevant to this Topic.

Topic IV: Submitting and Complying with Consumer Requests

This topic poses two unique questions: 1) what methods should be available for consumers to submit requests to businesses; and 2) how should businesses comply with such requests.

Question 1. Submitting Consumer Requests

IA supports the apparent intent of Civil Code section 1798.130 to provide consumers reasonable choices in how they exercise their rights under the CCPA.³ The CCPA specifies that the two methods must include a toll-free number and, if the business has a website, a web address.⁴ IA notes that it is unfortunate that the approach adopted in CCPA is prescriptive and technology-specific rather than focused on achieving the best privacy outcomes for consumers in a manner that would remain relevant over time.⁵

³ For example, Civil Code section 1798.130, subdivision (a)(1) provides that a business shall, “in a form reasonably accessible to consumers,” “make available to consumers two or more designated methods for submitting requests for information.”

⁴ Civ. Code, §1798.130, subd. (a)(1).

⁵ IA notes requiring use of toll-free numbers also presents significant security concerns. Cyber criminals are increasingly using robocalling, voice phishing and caller ID spoofing to craft attacks that are being used to scam



In other areas the Legislature has recognized that flexibility will drive positive outcomes for consumers. In California's automatic renewal law, the Legislature provided a non-exhaustive list of options, including toll-free number, email, or "another cost-effective, timely, and easy-to-use mechanism" for consumers submitting cancellation requests for subscription services.⁶ This language strikes a better balance of easy access for consumers and flexibility in implementation for businesses.

In drafting CCPA regulations, IA recommends focusing on the key outcomes for consumers including that the methods for exercising their rights under CCPA should be: easy to locate and easy to use, free⁷ (where a request is not manifestly unfounded or excessive under the CCPA), fit for purpose, secure, and appropriate to the context of the relationship with the business.

IA urges the Attorney General to consider the ease of submission and obtaining a response when specifying any further requirements for consumer requests. IA believes the guiding principle should be the manner in which the consumer is accustomed to interacting with the business. For example, in the online context, many consumers already use and benefit from account settings or control centers where they can make choices about how to interact with a business and can easily change contact information, notification settings, and privacy settings with a few clicks. They already benefit from being able to access and/or delete their personal information directly from such areas within a mobile app or website. Likewise, in the offline context, if a consumer's primary model of interaction with a business is face to face in a physical location, a consumer may expect to interact with the business at a physical location rather than online. Regulations should seek to enhance rather than to change normal consumer/business relationships or impose obligations that would run counter to consumer expectations that have developed based on how certain businesses operate.

Question 2. Complying with Consumer Requests

The question of how businesses should comply with consumer requests can also be broken into two distinct parts. First, as a practical matter, the question may seek to elaborate on the requirements for responding to consumer requests that is laid out at Civil Code section 1798.130, subdivision (a)(2). IA does not see a need for much elaboration on the statutory language regarding responding to consumer requests. However, to the extent the Attorney General intends to provide further guidance through regulations, IA reiterates its comments in response to Question 1 of this Topic, above. Responses to consumer requests should be allowed to be provided in a manner that is easy for the consumer and appropriate to the context of the interaction between the consumer and the business.

unsuspecting users who have traditionally trusted the telephone. See, e.g., Dennis Fisher, [Cybercriminals Turn to Phone for Easy Scams](#), Digital Guardian (last accessed Mar. 8, 2019). Businesses who provide toll-free numbers for consumer use have also been targeted by robocalling and theft of service scams. See, e.g., Steven Melendez, [Why 800 Numbers Are Getting Their Own Robocalls](#), FastCompany (last accessed Mar. 8, 2019).

⁶ Bus. & Prof. Code, § 17602, subd. (b).

⁷ IA supports at least one free method for exercising consumer rights, but recognizes in certain instances that extremely low cost options may be reasonable additional alternatives to offer consumers (e.g., the cost of a postage stamp).



There are more complicated considerations related to compliance with consumer requests, particularly for access, but also for deletion and potentially opt-out. With respect to such rights, it is imperative that any regulations promulgated by the Attorney General appropriately account for the exemptions in section 1798.145. More specifically, the following addresses IA's concerns with the exemptions related to compliance with state and federal laws, not adversely impacting the rights of other consumers, and unlinked and deidentified data.

Compliance with Federal and State Laws

As noted in the CCPA, additional guidance on exceptions related to compliance with federal and state laws may be necessary to appropriately set expectations for consumers and to provide constructive guidance to businesses on how to resolve tensions between legal obligations.⁸ The CCPA contains a clear exemption that states that “the obligations imposed on a business by this title shall not restrict a business’s ability to: (1) Comply with federal, state, or local laws.”⁹ This exemption applies to federal and state laws forbidding the disclosure of the “contents of communications” and other personal information without appropriate legal authorization, and IA seeks clarification from the AG that those laws govern over the CCPA.

IA member companies are subject to numerous federal and state laws designed to protect the privacy of consumers by prohibiting unauthorized disclosure of specific types of personal information, as that term is defined in CCPA.¹⁰ For example, Penal Code section 631(a) prohibits the disclosure of the contents of communications obtained through “interception” without the consent of all parties to the communication. This provision has been applied to real-time communications services, even where the communication may be stored or accessible on a communications service provider’s network. A business should not be compelled to produce private communications to a consumer in response to an access request in violation of the Penal Code.

IA would also like to note that as electronic communications have become more pervasive in the lives of consumers, the definitions that apply to electronic communications privacy statutes have been the subject of evolving and sometimes conflicting law. This has particularly been the case in terms of the definitions of “interception”¹¹ and “contents of communications.”¹² In addition, court cases have re-examined statutory protections to determine whether they continue to meet constitutional

⁸ See Civ. Code, § 1798.185, subd. (a)(3).

⁹ Civ. Code, § 1798.145, subd. (a)(1).

¹⁰ See, e.g., 18 U.S.C. §§ 2510 *et seq.* (the Wiretap Act), 18 U.S.C. §§2701 *et seq.* (the Stored Communications Act), 18 U.S.C. §2710 (the Video Privacy Protection Act); Cal. Penal Code §631 (interception of communications); Cal. Civ. Code, §§ 1798.90-1798.90.05 (California Reader Privacy Act).

¹¹ See, e.g., *Steve Jackson Games, Inc. v. United States Secret Service* (5th Cir. 1994) 36 F.3d 457; *Fraser v. Nationwide Mut. Ins. Co.* (3d Cir. 2003) 352 F.3d 107; *Konop v. Hawaiian Airlines, Inc.* (9th Cir. 2002) 302 F.3d 868; *United States v. Steiger* (11th Cir. 2003) 318 F.3d 1039; *United States v. Jones* (D.D.C. 2006) 451 F. Supp. 2d 71; *Cf. United States v. Councilman* (1st Cir. 2005) 418 F.3d 67.

¹² See, e.g., *In re: Zynga & Facebook Privacy Litigation*, Nos. 11-18044; 12-15619 (9th Cir. May 8, 2014); *Cf. United States v. Forrester* (9th Cir. 2008) 512 F.3d 500, 510, fn.6.



standards in light of changes to the use of technology.¹³ This, at least in part, led to the passage of the groundbreaking California Electronic Communications Privacy Act in 2015.¹⁴

Federal law protects the contents of communications both in transit, 18 U.S.C. Section 2511, and in storage, 18 U.S.C. Section 2702. Federal cases have interpreted “contents of communications” to include types of information specifically included within the definition of “personal information” in CCPA, such as search history and web browsing history.¹⁵ These types of information are particularly at risk in the context of access requests based on “households,” “devices,” and “unique identifiers.” CCPA should not be interpreted to require businesses to violate federal criminal law for a myriad of legal reasons, not the least of which is the clear exemption for legal compliance in CCPA itself.

Both California and federal law also address privacy protections for specific types of material that are covered by the definition of personal information inclusion of “commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consumer histories or tendencies.”¹⁶ For example, the California Reader Privacy Act, Civil Code sections 1798.90-1798.90.5, protects purchase, renting, or borrowing books. The federal Video Privacy Protection Act, 18 U.S.C. Section 2710, protects a consumer’s viewing history. These are just two examples where sharing purchase history with someone other than the individual to whom it directly pertains could conflict with other state or federal civil and criminal laws.

In order to protect consumer privacy and to avoid conflicting obligations under CCPA regulations and other state and federal privacy laws, the Attorney General should make it clear that a consumer is only entitled to access certain types of personal information when that personal information pertains solely to the consumer who is making the request. For example, the Attorney General could require that consumers who submit access requests provide one of a list of specific identifiers which distinctly relate to a specific natural person and verify that they are the specific natural person associated with that identifier.¹⁷ The consumer would then be able to obtain the personal information linked to that identifier, to the extent it is technically feasible for a business to conduct a search of its records of personal information based on that specific identifier. Additionally, the Attorney General could specify specific identifiers where there is a high risk of disclosure of other consumers’ personal information, such that those identifiers should not be used to respond for purposes of an access request. IA also asks that the Attorney General establish safe harbor practices, so that businesses who

¹³ See, e.g., *Carpenter v. United States* (2019) 138 S. Ct. 2206; *United States v. Jones* (2012) 565 U.S. 400; *United States v. Warshak* (6th Cir. 2010) 631 F.3d 266.

¹⁴ Pen. Code, §§ 1546-1546.4. In describing the need for CalECPA, the Bill Analysis states: “SB 178 updates existing federal and California statutory law for the digital age and codifies federal and state constitutional rights to privacy and free speech by instituting a clear, uniform warrant rule for California law enforcement access to electronic information, including data from personal electronic devices, emails, digital documents, text messages, metadata, and location information. Each of these categories can reveal sensitive information about a Californian’s personal life: her friends and associates, her physical and mental health, her religious and political beliefs, and more.” Senate Committee on Public Safety, Bill Analysis, p. 12 (March 23, 2015).

¹⁵ See, e.g., *Pen Register Application* (D.Mass. 2005) 396 F.Supp.2d 45.

¹⁶ Civ. Code, § 1798.140, subd. (o)(1)(D).

¹⁷ Verification of consumer requests is discussed further, *infra*, in Topic VII.



comply with these or other guidelines promulgated by the Attorney General will not face liability as a result of doing so, including, for example, in cases where a request that meets all of the guidelines and requirements turns out to be the work of an identity thief. Additionally, where potential liability may exist for responses to requests that cannot be addressed through a safe harbor in state regulations,¹⁸ the Attorney General should confirm that businesses are not required to respond to requests.

Rights of Other Consumers

The CCPA states that “the rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.”¹⁹ This exemption applies to all of the requests that a consumer may make to a business under the CCPA. As discussed in IA comments to Topic I and this Topic in relation to compliance with state and federal laws, this exemption is a critical protection for consumer rights as a result of the broad definition of personal information, including the broad definition of the term unique identifier. By including such broad definitions, CCPA creates a risk that the exercise of a consumer’s right to access could result in the violation of another consumer’s privacy rights in their own personal information as provided in statute²⁰ and the state Constitution.²¹ IA reiterates its recommendation, above, that the Attorney General promulgate regulations (and corresponding safe harbors) that specifically limit the risk that one consumer’s access request could result in the disclosure of another consumer’s private information -- regardless of whether those consumers are members of a “household,” a “family,” or have at some point shared a device, a browser, an IP address, telephone number or any other identifiers which are not specifically tied to a natural person.

IA notes that this issue also creates the risk that exercise of rights to deletion and opt-out could be implemented in ways that are overly broad and impact the rights and freedoms of other consumers. For example, if a consumer is able to request deletion of personal information including, for example, their name or online identifier, that could result in the deletion of content posted in newspapers and other media resulting in censorship. This risk was specifically contemplated by the legislature through the inclusion of an exception to the right to delete in Civil Code section 1798.105(d)(4), which provides protection for the right of the business to “exercise free speech” or the “right of another consumer to exercise his or her right of free speech.” Overly broad implementation of the right to delete could also result in malicious deletion of accounts, information, and content by other consumers if such rights can be accessed based on an identifier which is not specifically tied to a natural person. This is another risk that the Attorney General should draft regulations to protect against.

¹⁸ As may be the case for certain state and federal privacy laws. See, e.g., 18 U.S.C. § 2710(c) & (f) (creating a civil action against providers for violations and preempting state laws that require disclosures prohibited by the Section).

¹⁹ Civ. Code, § 1798.145, subd. (j).

²⁰ See, e.g., footnote 10, *supra*.

²¹ See California Constitution, Article I, Section 1.



Deidentified and Unlinked Data

Another area of concern for businesses is the manner in which that Attorney General may draft regulations regarding compliance with consumer requests and the potential impact on data that is not held in a manner that identifies consumers. The construction of the CCPA demonstrates a clear legislative intent to exempt “deidentified” data, but poorly constructed provisions risk creating confusion.

There is ample evidence in the statutory text of the CCPA that information that is not linked to particular consumers should not be treated as personal information for purposes of responding to consumer requests. First, “deidentified” is defined in such a way that it is the direct opposite of “personal information.” Deidentified information is information that “cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.”²² Personal information is defined as simply the opposite as information “that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”²³ Thus, information that complies with the requirements of the definition of deidentified, should not be viewed as “personal information” for the purposes of the CCPA. The CCPA goes further to underscore that the obligations of the statute to do not apply to information that is not personally identifiable. The exemptions in Civil Code section 1798.145, subdivision (a) state that “the obligations imposed on businesses by this title shall not restrict a business’s ability to” “collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.”²⁴ The Legislature repeated in section 1798.145, subdivision (i) that a business is not “require[d] to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.” In addition to these broad exemptions, section 1798.100, subdivision (e) states that a business is not required to “reidentify or otherwise link information that is not maintained in a manner that would be considered personal information” to comply with a consumer request for access. This exact language is repeated in section 1798.110, subdivision (d)(2) pertaining to consumer deletion requests. IA member companies support the laudable goal of encouraging companies to use privacy enhancing techniques to minimize the amount of personal information collected, processed, stored, and disclosed about consumers. The CCPA should reduce the risk to consumers from potential inadvertent disclosure, unauthorized acquisition, and from unnecessary privacy intrusions. In addition, it should ensure that businesses are not forced to link or combine data in such a way that it creates “personal information” solely to enable compliance with a consumer request under CCPA. As is clear from the above provisions, the CCPA did not intend for businesses to take steps to combine information and make more information identifiable than is done in the normal course of business.

The Attorney General should interpret the CCPA in a manner consistent with the clear intent of the statute. Specifically, references that are not in parallel construction with this “linkable” standard

²² Civ. Code, § 1798.140, subd. (h).

²³ *Id.* at 1798.140, subd. (o)(1).

²⁴ Civ. Code, § 1798.145, subd. (a)(5).



should not jeopardize the operation of these sections. For example, the language in Civil Code section 1798.130, subdivision (a)(3)(A) which says, “associate the information provided by the consumer” must be read in a manner consistent with the carve-outs for non-personally identifiable information, and should not force businesses to engage in the linking or association of data not otherwise linked or associated by the business with a consumer.

Topic V: Uniform Opt-Out Logo

Civil Code section 1798.135 imposes very specific requirements on businesses that are required to offer consumers an opt-out to the sale of their personal information. It requires a “clear and conspicuous link” on the homepage, with the title “Do Not Sell My Personal Information,” that goes to a webpage that enables a consumer or their representative to opt-out.²⁵ Another link must be included in the business’s privacy policy or California-specific description of consumer rights.²⁶ As in other areas of the CCPA that adopt a prescriptive approach to compliance,²⁷ IA recommends focusing on the key privacy outcomes for consumers including whether the opt-out method is: easy to locate, easy to use, free, fit for purpose, secure, and appropriate to the context of the relationship with the business.

IA believes the guiding principle should be that the location and function of the opt-out mechanism should be appropriate in the context for which the consumer is accustomed to interacting with the business. For example, in the online context, many consumers already use and benefit from account settings or control centers where they can make choices about how to interact with a business and can easily change contact information, notification settings, and privacy settings with a few clicks. They already benefit from being able to access and/or delete their personal information directly from such areas within a mobile app or website. Existing opt-outs are frequently available in the context of these and other privacy settings. Businesses should be allowed to include any new opt-outs in the locations where consumers are most likely to go look for them. This certainly includes an online provider’s privacy policy or California-specific privacy policy, but it may also include help centers or settings. As we have cautioned previously, regulations should not seek to change the consumer/business relationship or impose obligations that would run counter to consumer expectations that have developed based on how certain businesses operate. This would confuse consumers and may overly burden communities who have established methods of interacting with consumers.

IA also notes that the Attorney General should interpret the vague term “homepage” contained in section 1798.135, subdivision (a) and defined in section 1798.140, subdivision (l) to be the specific web page navigated to when the top level domain web address is entered in a web browser. The inclusion of “and any Internet Web page where personal information is collected” in the definition runs directly contrary to established and common understanding of the term. Since navigating to any webpage on the Internet results in the communication of personal information, as defined in the CCPA, the

²⁵ *Id.* at 1798.135, subd. (a)(1).

²⁶ *Id.* at 1798.135, subd. (a)(2).

²⁷ See, *supra*, comments to Topic IV, Question 1.



addition of this language is confusing and would conflict with the plain meaning of the term “homepage” and the intent of the legislature.

Topic VI: Notices and Information to Consumers Regarding Financial Incentives

IA member companies agree with the intent of the section 1798.125, subdivision (a), in that consumers should not be discriminated against because of decisions to exercise their rights under the CCPA. However, IA notes that there is conflicting language in the CCPA, and the specific examples of “discrimination” listed in subparagraphs (A)-(D) fail to recognize and properly account for the practical impacts that the exercise of certain consumer rights may have on the ability of a business to continue to provide services to consumers who exercise them. This has resulted in significant confusion regarding the proper interpretation of this provision of the CCPA.

For example, if a consumer exercises the right to delete their personal information, such as their billing information, a business will not be able to charge the consumer for subscription services, such as music or video services. However, an arguable reading of section 1798.125, subdivision (a)(1)(A) would be that a business cannot deny a consumer a service, even a fee service, based on the deletion of personal information even if that results in the consumer defaulting on payment.

The California Legislature may have intended to solve for this absurd result in paragraph (2) of the subdivision, which states “[n]othing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer’s data.” But the provisions remain confusing.

IA recommends that the Attorney General listen carefully to the public hearing testimony and written comments received when drafting regulations regarding non-discrimination and financial incentives. The ability to provide financial incentives could be one way that a business that is reliant on consumer personal information to deliver goods or services may disclose and obtain consumer consent to their essential business practices. However, IA notes that the financial incentive provision includes that same confusing language contained in paragraph (a)(2) regarding the value to the consumer of the consumer’s data.²⁸

IA urges the Attorney General to draft regulations related to this provision in such a way that consumers who exercise their rights are not unfairly penalized or subjected to unfair or misleading financial incentive programs and that simultaneously allows businesses that require personal information to provide goods, services, and data-driven features (e.g. in product recommendations based on past viewing, listening or purchasing history) are not forced to invent new business models, create new fee-based services to replace previously free services, or to shutter their businesses altogether.

²⁸ Civ. Code § 1798.125, subd. (b)(1).



Topic VII: Verification of Consumer Requests

As discussed extensively above, in implementing the provisions of the CCPA, the Attorney General should focus on the intent of the CCPA to raise the level of privacy protections afforded to California consumers. There are risks that are inherent in any system that involves disclosure of personal information, particularly in the context of a broadly drafted law like the CCPA. IA has already noted the risks of taking a broad approach to access rights and the risks of disclosing personal information in response to requests based on an identifier that does not distinctly identify a natural person. It is worth raising this risk again in the context of verification, because it may be difficult for a consumer to adequately verify their ownership and control over specific types of identifiers which are not necessarily tied to a specific person. For example, a California driver's license would not be sufficient to support a request for access to all personal information associated with an IP address. In this context, even if a consumer were required to demonstrate that the IP address is a static IP address for which the individual consumer making the request is the subscriber, there could be a substantial risk of privacy violations of other consumers, for example, if the subscriber were a landlord of a multi tenant building. It would therefore be more protective of consumer privacy to require consumers, if allowed to use an identifier which is not distinctly tied to their specific identities, to prove that the identifier is exclusively for that particular consumer's use.

Another context specific variable IA recommends the Attorney General bear in mind is that the types of information that businesses will have about consumers will vary considerably based on business model and the nature of the request. Some online services do not require "real names" and, therefore, have to rely on other data points rather than legal names, mailing addresses, or other more traditional personal identifiers. For example, demonstrating control over an online account and being able to successfully respond to security questions with appropriate answers may be the most reliable form of verification. On the other hand, for companies with billing information, legal names and proof of identity may be reliable forms of verification. Similarly, some companies may not have information demonstrating that a particular consumer is in fact a California resident and eligible to make a request under CCPA.

In addition, in instances where a consumer authorizes a third party to exercise their rights under the CCPA, it is essential that the consumer providing the authorization not only execute appropriate documentation to establish that the individual working on their behalf has their authorization, but also provides the third party they have authorized with the information or technical tools which will be essential for that individual to step into the shoes of the consumer and to complete the verification process in the same manner that the consumer would have if they were to complete the process on their own. Where traditional forms of identification and identity verification are not available, it is critical to allow businesses reasonable discretion to be able to respond to requests appropriately. Even with the appropriate documentation, whether a power of attorney or an appointment by a court to act on behalf of the consumer, if the agent cannot provide adequate verification that the consumer on whose behalf they act is the account holder or the natural person to whom the personal



information pertains it would be unsafe and should therefore not be required for a business to disclose information.

As a general rule, it would be most protective of consumer privacy and security to grant reasonable discretion to the responding company as to how to authenticate a consumer request, rather than prescriptive measures that could be circumvented or become outdated.

Topic VIII: Other Considerations for Regulations

Definition of Sale

To the extent that the Attorney General is considering promulgating regulations related to “sale” of data, IA urges that any rules be crafted narrowly to avoid unintended consequences that might include activities that were not intended to be covered by the law and which may restrict services to California consumers which they value greatly and which enhance their daily lives. For this reason, the concept of “sale” should be given its plain meaning to align with the intent of the sponsor of the legislation.

12 Month Look Back

CCPA states that when responding to a consumer’s request for access to their personal information that the response “shall cover the 12-month period preceding the business’s receipt of the verifiable request.”²⁹ IA recommends that the Attorney General consider whether regulations should clarify this provision, so that it is clear that it does not act as a data retention mandate. Requiring businesses to affiliate data with specific consumers for a 12-month period may conflict with existing pro-privacy data retention practices, that provide for—on a schedule shorter than 12 months—properly disposing of or deidentifying personal information once it has served the purpose for which it was collected. To guard against this unintended outcome, this provision should be read to require businesses to produce information processed during the 12 months preceding the request that the business is able to specifically link to the requesting consumer at the time the verified request is processed.

Definition of Consumer

IA agrees with comments made during the public hearings urging clarification that CCPA does not apply to natural persons who are acting in their capacity as employees or as business owners when engaging with businesses.³⁰ Further, IA also supports clarifications recommended that would clarify that employment data is outside the scope of the CCPA.³¹

Another appropriate topic for regulations is to address how a business is to determine whether a consumer is a California resident for purposes of the CCPA, and consider establishing a safe harbor for

²⁹ Civ. Code, § 1798.130, subd. (a)(2).

³⁰ Testimony of Dominique Shelton, DOJ Public Forum on the California Consumer Privacy Act, Transcript at 28:22-29:17 (January 8, 2019).

³¹ *Id.*



businesses that rely on consumer representations regarding their state of residency. In many cases, businesses may not have sufficient information to determine residency and rather than requiring companies to collect and store information they do not need, it would be preferable to allow them to rely on a consumer's unverified representation that they are—or are not—a California resident. Businesses that rely on consumer representations should qualify for a safe harbor to protect them from any potential liability that could exist if the consumer's representation is false.

In all other circumstances, businesses that are obligated to comply with the CCPA will need guidance on how to determine residency. Residency determinations are not typically business functions, and are more commonly performed by the state government, and can vary depending on the context, including evaluating one's: tax obligations,³² eligibility to obtain a driver's license,³³ voting rights,³⁴ and entitlement to benefits like in-state tuition rates³⁵ and other protections³⁶ of state law. In all of these circumstances, the determinations can be complicated by consumers moving into and out of state, splitting time between locations, or not maintaining forms of identification that are generally indicative of residency. It is an appropriate role for the Attorney General to determine what forms of proof are adequate proxies for proof of residency.

In addition, the Attorney General should address how businesses should determine the relevance of residency in determining their obligations under CCPA. Given how mobile the U.S. population is, it is easy to anticipate that an individual could provide personal information to a business while residing outside California and later become a resident. One can also easily imagine the inverse of this situation, where a California resident provides personal information to a business and later leaves the state and becomes a resident of another state. Presumably once the individual is no longer a California resident, they would become protected by the privacy laws of their state of residence and no longer be covered by CCPA.

IA members believe that these types of practical questions are matters of urgency for clarification as businesses design compliance systems and processes and train personnel in anticipation of the CCPA compliance deadline.

Internet Association looks forward to continued engagement and cooperation in this rulemaking process. If you have any questions please do not hesitate to contact Kevin McKinley, Internet Association's Director, California Government Affairs, at [REDACTED]

Respectfully submitted,

³² https://www.ftb.ca.gov/forms/2015/15_1031.pdf

³³ https://www.dmv.ca.gov/portal/dmv/detail/dl/residency_requirement

³⁴ https://elections.cdn.sos.ca.gov/regulations/hava_id_regs_from_barclays_3_3_06.pdf

³⁵ <https://www.ucop.edu/residency/>

³⁶ <https://www.dhcs.ca.gov/formsandpubs/forms/Forms/mc214.pdf>

Message

From: Jay L. Hack [REDACTED]
Sent: 3/18/2019 3:23:34 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Is it consumer or is it commercial?

I have spent the last 43 years representing banks and thus privacy of consumer information is something I have spent a lot of time on. There is one gnawing question that, to my knowledge, has never been answered, and I am just asking you to answer it in your regulations so I know what to say to my clients.

The question first arose, for me, when I was teaching seminars on the inter-agency privacy regulations under Gramm Leach Bliley about 20 years ago. The president of a bank stood up and asked, "A customer has a regular consumer deposit account with us. He is also the CEO of a commercial customer that borrowed money from us. When his company applied for a loan, he offered himself as a guarantor and provided personal information to us to complete a commercial transaction. We never collect that type of information for normal consumer deposit accounts. Is the information that we collected regarding a commercial loan transaction covered by the GLB rules just because the person also happens to have a consumer account with us?" Not knowing the answer, I called the FDIC attorney who was on the interagency team that drafted the regulations and I asked him. There was no answer for about five seconds and then, I kid you not, he said, "Oh shit, we never thought of that."

The question gets even more complicated because what happens if the CEO has no personal account at the bank when the commercial loan is originated, but he likes the service at the bank, so a few months later, he opens a personal account.

In both of these situations, assuming that the CEO resides in California, the CEO is a consumer, defined in the statute as, "a natural person who is a California resident . . ." It is not clear to me from the statute whether it applies to information collected from the CEO in connection with a purely commercial transaction. Literally, I think the answer is yes, which means that everyone engaging in a transaction with a business that gets information about the principals of the business must give the initial notice and otherwise comply with the CCPA as it relates to California residents. See, for example, the data collection requirements under the FinCEN drill down rule.

<https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule>.

I would greatly appreciate it if your final rules address this issue.

In addition, I have an entirely unrelated question regarding the extra-territorial reach of the new law. Let's take the following hypothetical. A resident of California comes to New York to attend Cornell University and right outside her dorm is a local bank with only one branch, in Ithaca, New York. She opens an account at the branch. Is it the Department of Justice's position that the New York bank, with no physical presence in California, is "doing business" in California merely because the student's parent can access the deposit account on the Internet, view transactions, and use the account to pay bills using ordinary Internet bill pay software? Is the answer different if the bank is a large multinational bank with offices in California but the account is opened at a branch in Ithaca, New York and the student gives her dormitory address in New York as the address for sending statements on the account?

Jay L. Hack, Esq.

Gallet Dreyer & Berkey, LLP

845 Third Avenue

New York, New York 10022

[REDACTED]

[REDACTED]

For regular updates on legal issues, check out my Banking and Financial Institutions Law Blog at <https://www.gdblaw.com/blog?practiceID=4985>.

For more information about our firm, please visit our web site at www.gdblaw.com

Message

From: Alan McQuinn [REDACTED]
Sent: 3/8/2019 7:05:26 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Daniel Castro [REDACTED]
Subject: ITIF Comments on the CCPA Preliminary Rulemaking
Attachments: 2019-comments-ccpa.pdf

To Whom it May Concern,

Please accept the attached comments from the Information Technology and Innovation Foundation (ITIF) on the California Justice Department's rulemaking process for the California Consumer Privacy Act (CCPA).

Thank you.

Alan McQuinn

Senior Policy Analyst | Information Technology and Innovation Foundation
[REDACTED]

March 8, 2019

Mr. Xavier Becerra
Attorney General
Department of Justice
State of California
300 S. Spring St.
Los Angeles, CA 90013

RE: The California Consumer Privacy Act, Assembly Bill 375, Rulemaking Process

Dear Attorney General Becerra,

The Information Technology & Innovation Foundation (ITIF) is pleased to submit these comments in response to the California Justice Department's rulemaking process for the California Consumer Privacy Act (CCPA).¹ CCPA establishes new consumer data protection rights and creates new requirements for businesses collecting and handling personal information. ITIF is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington, and in the states. Through its research, policy proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation, and productivity.

At the outset, it is important to note that while ITIF supports the California Attorney General's efforts to bring regulatory certainty and clarity to California businesses and consumers regarding how the new rules will affect them, the State of California has significantly increased the regulatory costs and complexity on businesses by enacting a sweeping state-level data privacy law. Businesses operating online often find themselves subject to duplicative and conflicting laws because many countries claim jurisdiction over their activities.² Subnational governments, like states, should not compound the problem by adding their own layer

¹ "California Consumer Privacy Act (CCPA)," *Office of the Attorney General of California*, accessed February 19, 2019, <https://oag.ca.gov/privacy/ccpa>.

² Daniel Castro and Robert Atkinson, "Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy" (Information Technology and Innovation Foundation, September 2014), <http://www2.itif.org/2014-crossborder-internet-policy.pdf>.

of additional rules and regulations, especially in areas already regulated, like data protection. Doing so across all states is unsustainable because it would introduce unnecessary and unreasonable compliance costs on businesses, making it more difficult for businesses to scale nationally and thereby undermining U.S. competitiveness. Given the threat to the digital economy of multiple state laws and Congress's ongoing efforts to develop national data privacy legislation, the Attorney General's office should make clear that it supports a single federal law that preempts states.

The California Department of Justice is currently going through its preliminary rulemaking activities and anticipates publishing a Notice for Proposed Regulatory Action on CCPA this fall.³ Moreover, the California Attorney General has recently endorsed legislative changes to the CCPA.⁴ ITIF welcomes the opportunity to provide input on how the California Attorney General on both the current statute and proposed amendments to minimize compliance costs and damage to digital innovation while ensuring consumer protections.

While the California Department of Justice continues to pursue its obligations under the CCPA, there are several factors it should consider:

- Do not enforce CCPA outside of California
- Clarify exemptions for data protected by existing laws
- Reform, but do not remove, the 30-day cure
- Provide businesses with guidance on compliance
- Adjust transparency and access requirements
- Do not prohibit beneficial incentives to data sharing
- Do not expand the private right of action

BACKGROUND

California has a number of privacy laws already in statute, including those that require companies to disclose what data has been used for direct marketing, give notice to consumers in the event of a data breach, and

³ "CCPA Public Forum," *Office of the California Attorney General*, accessed February 25, 2019, <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-ppt.pdf>.

⁴ "Attorney General Becerra, Senator Jackson Introduce Legislation to Strengthen, Clarify California Consumer Privacy Act," *Attorney General Xavier Becerra*, press release, February 25, 2019, accessed March 6, 2019, <https://oag.ca.gov/news/press-releases/attorney-general-becerra-senator-jackson-introduce-legislation-strengthen>.

provide greater protections for health data than those offered by federal law. Adding to these laws, California passed the CCPA in June of 2018, which will go into effect on January 1, 2020.⁵

CCPA makes several changes to California privacy statute. It expands the definition of personal data from traditionally protected categories, such as health data and social security numbers, to include new types of information, such as location data, device identifying numbers, and biometric information.⁶ It requires businesses to notify consumers of what personal data they are using and how they are using it.⁷ It also provides users with the ability to opt out of having their personal information shared with a third party.⁸ Californians can also request that businesses delete their personal data.⁹ Businesses are prohibited from discriminating against consumers that exercise their rights under the act, such as by charging a different price or providing a different level or quality of goods or services, but they can offer consumers financial incentives to allow personal data collection.¹⁰

CCPA has several enforcement provisions. The act expands Californian consumers previous right of action by allowing them to sue for damages if their personal information “is subject to an unauthorized access and exfiltration, theft or disclosure as a result of the business’ violation of the duty to implement and maintain reasonable security procedures and practices.”¹¹ Consumers are entitled to penalties of between \$100 and \$750 per incident in damages.¹² However, before consumers can bring a lawsuit, businesses have a 30 day grace period to address the violation and provide consumers with an express written statement saying the issue has been fixed and further violations will not occur.¹³ Regarding government enforcement, CCPA gives the Attorney General broad authority to enforce the act, with fining authority of \$2,500 per violation or \$7,500 for each intentional violation.¹⁴ However, here again businesses have a 30-day grace period to fix the problem.

⁵ The attorney general is required to publish final regulations for the law before July 2020, which will go into effect six months later.

⁶ California Consumer Privacy Act, California Civil Code, § 1798.140.

⁷ California Civil Code, § 1798.115.

⁸ California Civil Code, § 1798.120.

⁹ California Civil Code, § 1798.105.

¹⁰ California Civil Code, § 1798.125.

¹¹ California Civil Code, § 1798.150 (a).

¹² California Civil Code, § 1798.150 (a)(1)(A).

¹³ California Civil Code, § 1798.150 (b).

¹⁴ California Civil Code, § 1798.155 (b).

Businesses can also seek out the opinion of the Attorney General for guidance about how to comply with the CCPA.¹⁵

In recent weeks, the Attorney General has supported a bill to make changes to the CCPA. Introduced by California State Senator Hannah-Beth Jackson, SB 561 would significantly change these enforcement provisions.¹⁶ First, the bill would expand individual's right of action to all violations under the act. Second, it would remove the 30-day cure for enforcement by the Attorney General. Finally, it would remove the ability of businesses to seek advice from the Attorney General regarding compliance with CCPA. These changes would negatively affect the welfare of both Californian businesses and residents.

The rulemaking process is set to help the California Department of Justice clarify several things with the CCPA, including: 1) categories of personal information, 2) definitions of unique identifiers, 3) exceptions to CCPA, 4) submitting and complying with requests, 5) uniform opt-out buttons, 6) notices and information to consumers, including financial incentive offerings, and 7) verification of consumer requests.¹⁷

DO NOT ENFORCE THE CCPA OUTSIDE OF CALIFORNIA'S JURISDICTION

CCPA applies to many businesses that handle personal data about Californians. The law applies to businesses operating in California if they generate an annual gross revenue of \$25 million or more, if they annually receive or share personal information of 50,000 California residents or more, or if they derive at least 50 percent of their annual revenue by "selling the personal information" of California residents.¹⁸ In effect, this means that businesses with websites that receive traffic from an average of 137 unique Californian IP addresses per day could be subject to the new rules. The CCPA does not apply to nonprofits or the small number of businesses that do not meet any of these thresholds.

If the Attorney General broadly interprets which entities this law applies to, it would create administrative costs for many businesses nationwide that have little to no relationship with the state. For example, a company operating out of Maine with a revenue of \$26 million could be subject to these rules if it has a single Californian customer. Or an online media business based in Florida that averages 150,000 visitors per day

¹⁵ California Civil Code, § 1798.155 (a).

¹⁶ California Consumer Privacy Act of 2018: Consumer Remedies, S.B. 561, https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201920200SB561.

¹⁷ "CCPA Public Forum."

¹⁸ California Civil Code, § 1798.140.

worldwide could be subject to this law if 150 of those visitors come from California. The result of this would be an incentive for some companies outside of California to stop selling to California residents, or block them from their website, just as the EU's General Data Protection Regulation led some U.S. companies to block Europeans from their sites.¹⁹

Moreover, if other states follow California's lead, many online businesses, large and small, would face multiple state laws. For example, Californian businesses might be subject to 49 additional state laws. Such an outcome would impose unreasonable compliance costs on businesses, subject them to conflicting laws from other states, and threaten the viability of a national market for digital services.

Instead, the Attorney General should use its discretion to apply this statute only to businesses with a significant presence in the state. This could mean businesses that have offices, employees, bank accounts, physical property, or substantial marketing in California, or those that engage in significant business activity within the state. Moreover, in its final rulemaking, the Attorney General should explicitly state the parameters in which it will subject out-of-state businesses that fall outside of these criteria to enforcement actions. By doing so, the state can clarify the requirements for businesses with nexus in California without impeding on other states' jurisdictions. If the Attorney General does not believe it has the discretion to limit its application of CCPA in this way, it should recommend that the state legislature amend the law.

CLARIFY EXEMPTIONS FOR DATA PROTECTED BY EXISTING LAWS

The CCPA exempts certain information already covered under certain federal laws, such as financial information covered by the Gramm-Leach-Bliley Act (GLBA), driving information covered by the Driver's Privacy Protection Act (DPPA) of 1994, credit information covered by the Fair Credit Reporting Act, health information covered by the Health Insurance Portability and Availability Act (HIPAA) of 1996, and certain types of personal information covered by California statute, such as the California Financial Information Privacy Act (CFIPA).²⁰

Even with these exemptions, however, CCPA will create additional compliance costs for businesses already covered by rigorous privacy rules. For example, even though financial services companies are already subject

¹⁹ Daniel Castro and Alan McQuinn, "GDPR Freeloaders: Why Other Countries Should Fight Back," *Information Technology and Innovation Foundation*, August 16, 2018, accessed March 7, 2019, <https://itif.org/publications/2018/08/16/gdpr-freeloaders-why-other-countries-should-fight-back>.

²⁰ California Civil Code § 1798.145.

to GLBA and CFIPA, the law does not exempt these companies from its obligations. This includes CCPA requirements to make disclosures to consumers for certain personal non-public financial information (i.e., data not covered by GLBA) and to provide certain rights to consumers, such as the consumers right to stop the business from sharing their personal information and the right to access.²¹ The Attorney General should clarify these exemptions to industries with privacy regulations already in statute or harmonize state privacy regulations targeting sensitive types of information across industries. The overall goal should be to reduce the compliance burden on organizations, especially those already subject to federal or state data privacy regulations. If the Attorney General does not believe it has the authority to clarify these exemptions, it should call on the state legislature to amend the law.

REFORM, BUT DO NOT REMOVE, THE 30-DAY CURE

During enforcement of CCPA by the Attorney General, businesses are only in violation of the title if they fail to remedy an alleged violation within 30 days after being notified of alleged noncompliance.²² However, the Attorney General, through its support of SB 561, is seeking to remove this provision, known as a “30-day cure,” arguing that it would be able to secure more civil penalties and thus increase enforcement. Specifically, the Attorney General has said it needs to raise \$57.5 million in civil penalties to cover the cost of CCPA enforcement.²³

This is the wrong approach. The goal of data privacy legislation should not be to maximize fines on the private sector, but rather to increase consumer protections while minimizing costs to the economy and preserving innovation. The 30-day cure is a useful provision that should be preserved because it allows companies to focus on compliance by giving them an opportunity to address alleged harms. This means that companies can still innovate quickly as long as they are responsive to any potential violations. This flexibility is especially important in the digital economy—which California specializes in—where companies iterate quickly on products and services. New technologies, consumer offerings, and business models are continuing

²¹ Timothy Tobin and Roshni Patel, “California Consumer Privacy Act: The Challenge Ahead – The Interplay Between CCPA and Financial Institutions,” *Hogan Lovells*, December 7, 2018, accessed February 25, 2019, <https://www.hldataprotection.com/2018/12/articles/consumer-privacy/california-consumer-privacy-act-the-challenge-ahead-the-interplay-between-the-ccpa-and-financial-institutions/>.

²² California Civil Code, § 1798.155.

²³ Janine Anthony Bowen et al., “Overview of the new California Consumer Privacy Law,” *BakerHostetler*, January 1, 2019, accessed March 6, 2019, <https://www.dataprivacymonitor.com/wp-content/uploads/sites/5/2019/01/Overview-of-the-New-California-Consumer-Privacy-Law.pdf>.

to emerge. In such an environment, consumer protection regulation needs to ensure that it is not so strict and punitive as to harm innovation, especially in cases where there was no intent to do harm and where no harm occurred. This provision would allow companies to work with the Attorney General to resolve any alleged problems and make consumers whole without exposing those companies to high legal fees.

The 30-day cure should not be a free pass for misbehavior. For example, if a company intentionally commits consumer harm, but fixes the problem within 30 days, they should still be subject to enforcement. Surely, the Attorney General would not want CCPA to inadvertently create a sanctuary for those committing material consumer harms. In addition, the CCPA does not specify how the Attorney General should enforce similar violations of the act that occur after the 30-day window. For example, imagine a vulnerability in a company's system leads to a data breach, and while the company takes action to fix the initial problem and makes customers whole, two months later there is a second data breach based on a different bug that causes consumer harm. Would the Attorney General treat these issues separately with 30-day compliance windows, or would the company be immediately subject to penalties for the second violation? The Attorney General's office should clarify its policies around enforcement of this provision.

Rather than seek to remove the 30-day component entirely, the Attorney General should seek an update to the CCPA that clarifies the 30-day cure. The CCPA should give the Attorney General discretionary authority to bring enforcement actions based on two factors: the extent to which a company acted intentionally or negligently, and the extent to which a company's action caused real, substantial consumer harm.²⁴ The act should still give businesses that did not act intentionally or negligently, or did not cause substantial consumer harm, a period of time to fix their compliance issues. Importantly, the Attorney General should not subject companies to punitive measures for actions they take in good faith that did not cause consumer harm because doing so would force companies to prioritize regulatory compliance rather than preventing consumer injury. This would create perverse incentives for Californian businesses, such as by pushing them to hire privacy lawyers to rewrite their online terms of service to minimize legal exposure from a data breach rather than hiring security experts to remedy cybersecurity vulnerabilities.²⁵

²⁴ Daniel Castro and Alan McQuinn, "How and When Regulators Should Intervene" (Information Technology and Innovation Foundation, February 2015), <http://www2.itif.org/2015-how-whenregulators-intervene.pdf>.

²⁵ Ibid.

PROVIDE BUSINESSES WITH GUIDANCE ON COMPLIANCE

The CCPA enables businesses to seek the opinion of the Attorney General for guidance on how to comply with its provisions.²⁶ However, the Attorney General supports SB 561 which would remove this provision.²⁷ The Attorney General argues it should not need to “provide, at taxpayers’ expense, businesses and private parties with individual legal counsel on CCPA compliance.”²⁸

Again, the Attorney General has misplaced priorities. If the goal is to increase compliance with data privacy rules, the Attorney General should welcome the opportunity to clarify to industry what practices are acceptable or not acceptable. Providing this information would also allow the Attorney General to outline permissible conduct without resorting to expensive and time-consuming enforcement actions. To do otherwise would create a chilling effect on innovation, as California businesses would be unable to go to market with a clear sense of risk of non-compliance with CCPA of a new product or service.

This type of relief is not an unheard-of practice. For example, many different agencies—both federal and state—offer the ability to send letters to companies, called no-action letters, saying that agency will not bring enforcement actions against a particular product or service.²⁹ The goal of these alternatives to enforcement is to reduce regulatory risk for companies and signal to the market what type of behavior is acceptable. By letting companies come to the Attorney General when their products and services do not fit neatly into predetermined guidelines within the CCPA, it will enable the regulator to have a more flexible and nuanced approach to unconventional technologies and business models—ensuring Californians’ privacy is protected while also enabling innovation to proceed apace. The Attorney General should not seek to remove this positive provision of CCPA.

ENSURE TRANSPARENCY AND ACCESS REQUIREMENTS ARE NOT BURDENSOME

The CCPA gives users rights to transparency—ensuring organizations disclose how their information is used, the purposes for which it is used, with whom it is shared, users’ rights under the law, and more—and a right

²⁶ California Civil Code, § 1798.155 (a).

²⁷ S.B. 561.

²⁸ “Attorney General Becerra, Senator Jackson Introduce Legislation to Strengthen, Clarify California Consumer Privacy Act,” *Attorney General Xavier Becerra*.

²⁹ For example, see the Securities and Exchange Commission’s (SEC) policy on No-Action Letters. “No Action Letters,” *U.S. Securities and Exchange Commission*, March 23, 2017, accessed March 6, 2019, <https://www.sec.gov/fast-answers/answersnoactionhtm.html>.

to access their information.³⁰ It mandates that businesses promptly take steps to disclose and deliver, free of charge, consumers' personal information.³¹ The right of transparency and access have clear benefits for consumers because it allows users with strong privacy preferences to make more informed choices. These provisions also will enable the California Justice Department to hold companies accountable for their promises.

However, the cost of providing data access could be substantial for many organizations, especially for large, old, and complex data sets, and data sets that are not digitized (e.g., stored on paper in filing cabinets).³² Therefore, the Attorney General should use a reasonableness standard to interpret this statute. This right should be limited to require data controllers disclose whether they have data about a specific individual, the type of information collected, the policies governing that data collection, and with what other entities the organization has shared the data. This right should not apply to proprietary data, which is data about an individual that is inferred or computed by an organization. For example, companies construct online advertising profiles for consumers based on many different sources of observed personal information, such as direct-mail responses, search history, and demographic information. Finally, the right should only apply to sensitive categories of data. For example, patients should continue to be able to get access to their medical records at no cost, and consumers should have access to their utility usage data. Requiring access to nonsensitive data, such as publicly available personal information, device identifiers, and stored IP addresses, will only raise compliance costs with limited usefulness to the consumer. If the Attorney General does not believe it has the authority to limit these access requirements, it should recommend that the state legislature amend the law.

The Attorney General should also work to align the costs of this regulation with its benefits. Currently, the CCPA does not allow businesses to recoup any costs for providing consumers with any information required under the statute.³³ The Attorney General should call on the California legislature to allow companies to charge search, review, and duplication costs for providing data access—similar to what the federal government can charge individuals for requests made under the Freedom of Information Act.

³⁰ California Civil Code, § 1798.100.

³¹ *Ibid.*

³² Alan McQuinn and Daniel Castro, "A Grand Bargain on Data privacy Legislation for America" (Information Technology and Innovation Foundation, January 2019), 38-39, <http://www2.itif.org/2019-grand-bargain-privacy.pdf>.

³³ California Civil Code, § 1798.130 (2).

Moreover, many organizations do not have a process to easily verify someone's identity.³⁴ Poor verification of requests for personal information poses a substantial privacy risk to consumers. Therefore, the Attorney General should specify the permitted processes by which organizations can verify the identity of individuals requesting a copy of their data.

DO NOT PROHIBIT BENEFICIAL INCENTIVES TO DATA SHARING

CCPA prohibits businesses from denying goods and services or offering a different level of quality of service when users exercise their rights under the law.³⁵ The law does allow certain covered entities to offer different prices, rates, levels, or quality of goods and services to users if that difference is directly related to the value of the user's data. Covered entities can only offer this incentive program if they receive affirmative consent from the user prior to their participation in the program and allow them to opt out at any time. Moreover, CCPA forbids using this practice in an unjust, unreasonable, coercive, or usurious way.

Unfortunately, laws like the CCPA that restrict businesses from offering discounts to customers who share their data, including for targeted advertising, hurt both users and companies.³⁶ Companies benefit from these relationships by monetizing data through advertising (usually in ways that do not divulge personally identifiable information to advertisers) and realizing lower customer acquisition costs.³⁷ Consumers get direct benefits through lower prices as well as better and more customized offerings. Society also benefits from greater levels of efficiency in advertising with less money spent on poorly targeted ads.

Moreover, by restricting companies from limiting services or increasing prices for consumers who opt-out of sharing personal data, CCPA enables free riders—individuals that opt out but still expect the same services and price—and undercuts access to free content and services. Someone must pay for free services, and if individuals opt out of their end of the bargain—by allowing companies to use their data—they make others pay more, either directly or indirectly with lower quality services. CCPA tries to compensate for the drastic

³⁴ See the following article written by a Californian florist. Jim Relles, "Another Voice: The New California Privacy Law Will Hurt Sacramento Small Businesses," *Sacramento Business Journal*, February 28, 2019, accessed March 7, 2019, <https://www.bizjournals.com/sacramento/news/2019/02/28/another-voice-the-new-california-privacy-law-will.amp.html>.

³⁵ California Civil Code, § 1798.125.

³⁶ McQuinn and Castro, "A Grand Bargain on Data privacy Legislation for America," 26-30.

³⁷ Alan McQuinn, "No, Internet Users Are Not Paying With Their Data," *Inside Sources*, August 7, 2018, accessed March 7, 2019, <https://www.insidesources.com/no-internet-users-not-paying-data/>.

reduction in the effectiveness of online advertising, an important source of income for digital media companies, by forcing businesses to offer services even though they cannot effectively generate revenue from users. Online advertising is most effective when advertisers can serve relevant ads. Targeted ads based on information about a user (e.g., browsing history) help deliver higher-value ads. If regulations reduce the effectiveness of targeted ads, websites—especially those offering free services—will get less revenue.³⁸ In effect, by enabling users to access online services without providing the information necessary for companies to monetize those services, the CCPA could create a free-rider problem for online services.

Reducing the effectiveness of advertising may result in some companies, particularly those with thin margins, switching to a fee-for-service or subscription business model, wherein customers would have to pay for services that used to be free.³⁹ While this change would mean slightly lower living standards for everyone who switches, many low- and middle-income Californians would simply lose access to beneficial services they would not wish to pay for or could no longer afford. Moreover, because a subscription-based model would result in reduced revenues, it would also likely decrease the quality, breadth, and variety of content.

To mitigate against the risk created by prohibiting businesses from penalizing users that do not consent to data sharing, the Attorney General should interpret this statute to only apply to companies charging discriminate prices or those that offer a substantially different product or service to users that choose to opt-out. The Attorney General should not consider companies blocking users from accessing services to be a violation of this provision or from charging them a reasonable market price. Moreover, the Attorney General should clarify publicly that businesses are allowed to take either of these actions. Companies should not be forced to give free services to individuals that exercise their right to not contribute their data and thus deprive companies of the revenue necessary to operate those services. They should also be permitted to charge consumers a fair market price for any of their services.

³⁸ Alan McQuinn and Daniel Castro, “Why Stronger Privacy Regulations Do Not Spur Increased Internet Use” (Information Technology and Innovation Foundation, July 11), <https://itif.org/publications/2018/07/11/why-stronger-privacy-regulations-do-not-spur-increased-internet-use>.

³⁹ Alan McQuinn, “The Detractors are Wrong, Online Ads Add Value,” Information Technology and Innovation Foundation, December 8, 2016, accessed February 20, 2019, <https://itif.org/publications/2016/12/08/detractors-are-wrong-online-ads-add-value>.

DO NOT SEEK TO EXPAND THE PRIVATE RIGHT OF ACTION

The CCPA expands the private right of action in California by giving afflicted parties cause to sue for statutory damages in some cases where their data has been subject to unauthorized access or theft.⁴⁰ The Attorney General has endorsed SB 562, which would expand the private right of action to any violation under the act.⁴¹

Unfortunately, expanding the private right of action to violations of the CCPA that did not cause any consumer harm would make Californians worse off. Innovation by its very nature involves risks and mistakes. If CCPA exposes companies to massive liability every time they make those mistakes—no matter how small or if there is no consumer harm—there may be fewer mistakes, but there will also be significantly less innovation.⁴² This change would actually make Californian consumers worse off overall as money is needlessly diverted to minimizing legal risk rather than lowering prices, offering discounts, or creating new products and services. Legal risk makes companies stop innovating around personal data. For example, grocery stores could stop offering coupons based on purchase history—hurting low-income consumers that use those discounts for frequency bought goods.

This scenario has occurred in Illinois, where a vaguely written law allows consumers to sue companies for using facial recognition technology without their permission, even in cases where there is no proof of actual damages.⁴³ As a result, Illinois has seen a significant rise in largely groundless, class-action lawsuits against tech companies, such as Facebook, Shutterfly, and Snapchat.⁴⁴ Because of the legal risk created by this law, Illinoisans do not have access to many fun and productivity-increasing products that use biometrics

⁴⁰ California Civil Code, § 1798.150 (a).

⁴¹ “Attorney General Becerra, Senator Jackson Introduce Legislation to Strengthen, Clarify California Consumer Privacy Act,” *Attorney General Xavier Becerra*.

⁴² McQuinn and Castro, “A Grand Bargain on Data privacy Legislation for America,” 61-62.

⁴³ Megan Brown, “Illinois: Actual Injury Not Required for Privacy Lawsuit; Inviting Costly Litigation against Innovators,” *Wiley Connect*, January 25, 2019, accessed March 6, 2019, <https://www.wileyconnect.com/home/2019/1/25/illinois-actual-injury-not-required-for-privacy-lawsuit-inviting-costly-litigation-against-innovators>.

⁴⁴ Ally Marotti, “Shutterfly lawsuit tags Illinois as battleground in facial recognition fight,” *Chicago Tribune*, September 21, 2017, accessed March 6, 2019, <https://www.chicagotribune.com/business/ct-biz-biometrics-shutterfly-lawsuit-20170920-story.html>.

technology.⁴⁵ The Attorney General should learn from the mistakes of Illinois and not seek to expand the private right of action to cases where there was no tangible consumer harm.

CONCLUSION

In implementing these rules, the California Attorney General's office should clarify its rules around jurisdiction, CCPA exceptions, and enforcement. It should also interpret these rules to minimize compliance burdens through the transparency and access provisions, as well as allow companies to create disincentives for free riders. To the extent it does not believe it has the authority to use its discretion in these ways, the Attorney General should seek legislative changes to that effect. Moreover, as the Attorney General seeks to amend CCPA, it should not support SB 561, which would reduce the California Department of Justice's flexibility in enforcement and increase compliance costs and legal risk for businesses throughout California.

To reiterate, ITIF believes the regulation of privacy rules affecting national entities should be left to federal authorities working in partnership with stakeholders from states, civil society, and the private sector. Rather than acting alone, California should work with federal policymakers to help create a meaningful U.S. privacy framework that balances consumer protections with support for data-driven innovation.

Sincerely,

Daniel Castro

Vice President, The Information Technology and Innovation Foundation

Alan McQuinn

Senior Policy Analyst, The Information Technology and Innovation Foundation

⁴⁵ Daniel Castro and Michael McLaughlin, "Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence" (Information Technology and Innovation Foundation, February 4, 2019), <https://itif.org/publications/2019/02/04/ten-ways-precautionary-principle-undermines-progress-artificial-intelligence>.

Message

From: Christopher Oswald [REDACTED]
Sent: 1/31/2019 7:45:47 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Eleanor Blume [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Eleanor Blume1d5]; Stacey Schesser [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Stacey Schesser131]; Lisa Kim [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Lisa Kimf4f]; Nicklas Akers [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Nicklas Akers711]
Subject: Joint Ad Trades Letter re CCPA 1.31.2019
Attachments: Joint Ad Trade Letter to AG Becerra re CCPA 1.31.2019.pdf

Dear Attorney General Becerra:

Please find attached a joint letter from the advertising and marketing trade associations regarding CCPA rulemaking.

Thank you for your consideration, please feel free to contact me if you have any questions.

Sincerely,

Chris

Christopher Oswald | SVP, Government Relations

ANA – Association of National Advertisers



[REDACTED] | www.ana.net | @ANAGovRel





January 31, 2019

The Honorable Xavier Becerra
Attorney General, State of California
1300 I Street
Sacramento, CA 95814

Dear Attorney General Becerra:

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies, from small businesses, to household brands, across every segment of the advertising industry, including a significant number of California businesses. Our members engage in responsible data collection and use that benefit consumers and the economy. We believe privacy deserves effective protection in the marketplace.

We strongly support the objectives of the California Consumer Privacy Act (CCPA), but we have notable concerns around the likely negative impact on California consumers and businesses from some of the specific language in the law. We provide this initial comment to provide you with information about the significant importance of a data-driven and ad-supported online ecosystem, industry efforts to protect privacy, and in section III of the letter draw your attention to several areas that can be addressed and improved through the rulemaking process. We will provide more detailed comments over the coming weeks.

I. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth

The free flow of data online fuels the economic engine of the Internet, creating major consumer benefit. For decades, online data-driven advertising has powered the growth of the Internet by funding innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and much more, at little or no cost to the consumer. Companies also collect data for numerous operational purposes including ad delivery and reporting, fraud prevention, network enhancement, and customization. These uses are necessary for a seamless cross-channel, cross-device consumer experience and a functioning digital economy.

As a result of this advertising-based model, the Internet economy in the United States has rapidly grown to deliver widespread consumer and economic benefits. According to a recent study conducted for the Interactive Advertising Bureau (IAB) by Harvard Business School Professor John Deighton, the U.S. ad-supported Internet created 10.4 million jobs in 2016,¹ and

¹ John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017) <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>.



the data-driven ad industry contributed \$1.121 trillion to the U.S. economy that year, doubling its contribution over just four years and accounting for 6 percent of U.S. gross domestic product.²

Consumers have enthusiastically embraced the ad-supported model, and they have actively enjoyed the free content and services it enables. They are increasingly aware that those services are enabled by data collected about their interactions and behavior on the web and in mobile applications, and they support that exchange of value. In fact, a Zogby survey commissioned by the Digital Advertising Alliance (DAA) found that consumers assigned a value of nearly \$1,200 a year to common ad-supported services, like news, weather, video content, and social media. A large majority of surveyed consumers (85 percent) stated they like the ad-supported model, and 75 percent indicated that they would greatly decrease their engagement with the Internet were a different model to take its place.

II. Our Members Have Long Been Champions of Consumer Privacy

Consumer trust is vital to our members' ability to successfully operate in the marketplace, and they take that responsibility seriously by engaging in responsible data practices. A prime example of this commitment is through the Digital Advertising Alliance YourAdChoices Program. The DAA created and enforces a self-regulatory code for all companies that collect or use data for interest-based advertising, based on practices recommended by the Federal Trade Commission (FTC) in its 2009 report on online behavioral advertising.³

The Principles in that code provide consumer transparency and control regarding data collection and use of web viewing data, application use data, and precise location data. Importantly, the YourAdChoices Program and the DAA Principles are a novel kind of industry-led initiative whereby *all* companies engaging in the described practices are subject to established privacy safeguard obligations. Also, the DAA Principles are independently monitored and enforced. To date, more than 90 compliance actions have been publicly announced.

The DAA Principles include rules around the collection and use of web viewing data for advertising and restrictions for purposes beyond advertising;⁴ strong prohibitions on the use of such data for eligibility purposes for employment, insurance, credit, and healthcare treatment;⁵ and detailed guidance around the application of the Principles in the mobile⁶ and cross-device⁷ environments. Most recently, to provide users with increased transparency about the source of

² *Id.*

³ DAA, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009); FTC, *FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising* (Feb. 2009).

⁴ DAA, *Self-Regulatory Principles for Multi-Site Data (MSD)* (Nov. 2011).


⁵ DAA, *MSD*, 4-5 (Nov. 2011); DAA, *Application of Self-Regulatory Principles to the Mobile Environment*, 31-32 (Jul. 2013).

⁶ DAA, *Application of the Self-Regulatory Principles to the Mobile Environment* (Jul. 2013).

⁷ DAA, *Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices* (Nov. 2015).



the political advertising they see online, the DAA released guidance on the application of the Principles of transparency and accountability to political advertising.⁸

The main avenue through which consumers receive disclosures and choices is through the DAA's YourAdChoices icon , which is served in or near ads over a trillion times per month worldwide. The YourAdChoices icon provides transparency outside of the privacy policy, and clicking on it allows consumers to access simple, one-button tools to control the future collection and use of data for interest-based advertising. Consumer awareness and understanding of the program continues to increase, and a 2016 study showed more than three in five consumers (61 percent) recognized and understood what the YourAdChoices Icon represents.⁹

The effectiveness of the Self-Regulatory Program also has been recognized by the United States government. At a 2012 White House event, Obama Administration officials including the then FTC Chairman and Secretary of Commerce publicly praised the DAA's cross-industry initiative. The DAA approach has also garnered kudos from the leadership at the FTC under both recent administrations for the program's pioneering privacy work.¹⁰

III. Consumers & Businesses Would Benefit from Clarification Concerning Certain CCPA Provisions

While our members strongly support the CCPA's intent to give consumers a choice about how their personal data is shared, we are concerned about the negative impact of certain sections of the CCPA and believe the law could be clarified through rulemaking to provide improved consumer protection and guidance to business. Such issues as the scope of the definition of personal information, the potential elimination of loyalty programs due to the non-discrimination requirements, and others continue to be not only problematic for the advertising community, but will also result in unintended harm to consumers. We highlight a few of our concerns here, and will provide more detailed comments on these points and others in the coming weeks.

- **Section 1798.115(d)** of the CCPA prohibits a company from selling consumer personal information that it did not receive directly from the consumer unless the consumer has received "explicit notice" and is provided an opportunity to exercise the right to opt out of that sale. **We urge the AG to recognize that a written assurance of CCPA compliance is sufficient and reasonable.**

⁸ DAA, *Application of Self-Regulatory Principles of Transparency & Accountability to Political Advertising*, (May 2018).

⁹ DAA, *Consumers' recognition of the AdChoices Icon -- and understanding of how it gives choice for ads based on their interests -- continues to rise* (Sep. 29, 2016) <https://digitaladvertisingalliance.org/blog/icon-you-see-yeah-you-know-me-0>.

¹⁰ The White House recognized the Self-Regulatory Program as "an example of the value of industry leadership as a critical part of privacy protection going forward." The DAA also garnered kudos from then-Acting FTC Chairman Maureen Ohlhausen who stated that the DAA "is one of the great success stories in the [privacy] space." In its cross-device tracking report, the FTC staff also praised the DAA for having "taken steps to keep up with evolving technologies and provide important guidance to [its] members and the public. [Its] work has improved the level of consumer protection in the marketplace."



- **Sections 1798.105 and 1798.120** of the CCPA allow consumers entirely to opt out of the sale of their data or delete their data; but the law does not explicitly permit a business to offer a consumer the choice to delete or opt out regarding some, but not all, of their data. **We request that the AG clarify that businesses may offer reasonable options to consumers to choose the types of “sales” they want to opt out of, the types of data they want deleted, or to completely opt out—and not have to just provide an all-or-nothing option.**
- **Section 1798.110(c)** of the CCPA arguably requires a business’ privacy policy to disclose to a consumer the specific pieces of personal information the business has collected about that consumer. **We ask the AG to clarify that a business does not need to create individualized privacy policies for each consumer to comply with the law.**

Without clarification and adjustments, these and other ambiguities in the law could result in reduced choice and privacy for consumers, rather than expanding it, as the law intended. We stand ready to work with you to find solutions to these and other issues as you prepare for its implementation. To the extent that there are needed changes in the CCPA to protect consumer privacy and other important interests that cannot be rectified by this rulemaking, but are better suited for legislation, we urge you to make such recommendations to the California Legislature.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
[REDACTED]

Christopher Oswald
SVP, Government Relations
Association of National Advertisers
[REDACTED]

Clark Rector
Executive Vice President-Government
Affairs
American Advertising Federation
[REDACTED]

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
[REDACTED]

Alison Pepper
Senior Vice President
American Association of Advertising
Agencies, 4A's
[REDACTED]

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
[REDACTED]

Message

From: Daniel Harris [REDACTED]
Sent: 3/8/2019 6:40:29 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Russ Noack [REDACTED] Justin Worrell [REDACTED]
Subject: NAPEO Comments on CCPA Implementation
Attachments: NAPEO Comments on CCPA Implementation.pdf

To Whom It May Concern:

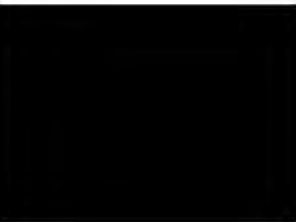
On behalf of the National Association of Professional Employer Organizations (NAPEO) and its members, I am sending you our comments on the implementation of California's Consumer Privacy Act of 2018. Please find our letter attached to this message. We thank you for the opportunity to provide feedback and look forward to working with you to address our concerns. Please feel free to contact me if you have any questions.

Regards,

Daniel A. Harris

Vice President, State Government Affairs

National Association of Professional Employer Organizations



Find us on [Facebook](#) and follow us on [Twitter](#)

The information contained in this material is not intended to be considered legal, accounting or tax advice and should not be acted upon as such. Also, the content of this e-mail is for the use of the intended recipient. If you have received this communication in error, please notify the author by replying to this e-mail

CCPA00000891

immediately and then delete the email and its contents from your system. Be aware that forwarding, copying, or disclosing the content to any other person than the intended recipient is prohibited.



707 North St. Asaph Street
Alexandria, Virginia 22314

F 703 836.0976
www.napeo.org

March 8, 2019

Electronic Delivery

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Re: Comments on CCPA Implementation

Dear Sir or Madam:

On behalf of the National Association of Professional Employer Organizations (NAPEO), I am writing to provide comments on the implementation of the California Consumer Privacy Act (CCPA). NAPEO is the largest trade association for professional employer organizations (PEOs), which provide comprehensive HR solutions for small and mid-sized businesses. NAPEO represents approximately 300 PEO member companies that provide services to over 175,000 businesses employing more than 3.7 million workers nationwide. In California, NAPEO has over 60 California member PEOs who handle approximately \$30 billion dollars in worksite wages annually.

PEOs generally provide payroll, benefits, regulatory compliance assistance, and other HR services to their clients. Client employers have on average 10-15 workers. They tend to grow faster, have lower employee turnover, and are less likely to go out of business than small businesses that do not use a PEO.

NAPEO and its members operating in the state of California appreciate the Attorney General's willingness to hear from stakeholders whose core business functions would be affected in a negative way should the CCPA become effective absent additional clarification. We remain supportive of the law's underlying objective to protect consumers and are hopeful to work with your office, local leaders, and fellow stakeholders to find a balance point between these protections and allowing our members to operate and continue to provide valuable services to their clients.

Our primary concern is that certain ambiguities and broad definitions within the CCPA place our membership in a tenuous position with regard to the CCPA's interplay with existing legal obligations. Specifically, we are concerned that the definitions of "sale", "personal information", and "consumer" may result in an inconsistent implementation of the law, which in turn could weaken privacy protections for

individuals such as employees and may result in inconsistent application of privacy protections. We thank you for the opportunity to provide comment and offer the following thoughts for your consideration:

SALE OF PERSONAL INFORMATION

The CCPA defines “sale” to include any *data transfer*¹ “for monetary or other valuable consideration.” [emphasis added]. Additionally, the new law would authorize a consumer to opt out of the sale of personal information by a business and would prohibit the business from discriminating against the consumer for exercising this right.

We believe the definition of “sale” is ambiguous and it is unclear whether monetary consideration must be received for the actual purchase of personal data, as opposed to another business arrangement where the data is not the subject of the exchange. The inclusion of the phrase “other valuable consideration” creates uncertainty as to the scope of a “sale” by suggesting that any ordinary course business transaction in which personal data must be exchanged in order for one party to provide the necessary services, such as in the case of the relationship between a PEO and its clients. Without clarity, the term may include many types of routine data sharing for businesses and could negatively impact employers. Additionally, the right to opt out of any “sale” could also disrupt the normal functioning of a PEO’s routine business operations, including employer payroll operations.

RIGHT TO ACCESS PERSONAL INFORMATION

The CCPA grants a consumer a right to request a business to disclose the categories and specific pieces of personal information that it collects about the consumer. Further, it requires a business to make disclosures about the information and the purposes for which it is used.

Access to personal information in the employment context is already established in California’s Labor Code, which provides that employees have the right to access their personnel files and records, including payroll records. NAPEO also believes the definition of “personal information” is ambiguous in that it does not have to identify a “consumer” and could be interpreted to mean a particular consumer *or household*. The inclusion of “household” could be interpreted to allow a spouse to gain access to employee records, even when that person is not entitled to do so under current law.

Additionally, the CCPA’s definition of “consumer” is “a natural person who is a California resident”. It is possible, given the broad definition, that “consumer” could be interpreted to include employees (who may not necessarily have a customer relationship with a business). This is highly problematic for many reasons should an employee choose to exercise their rights under the CCPA.

¹ Please note that, by “data transfer,” we are referring to the broad description of disclosures used in the definition of “sale” – “selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business....”

RIGHT TO DELETE PERSONAL INFORMATION

The CCPA grants a consumer the right to request deletion of personal information and requires the business to delete upon receipt of a verified request.

The right to have personal employment records deleted would conflict with many federal and state laws, which require employers to maintain detailed records of many employer-related functions. For example, the California Labor Code requires employers to maintain detailed records reflecting virtually all activity with respect to employment. This information includes: hiring, enrollment in employee benefits such as health insurance and retirement savings plans, documentation of hours worked, wages earned, deductions from pay, and many other related matters. Similarly, federal and state tax laws require employers to maintain detailed employee records. It would be problematic if a PEO would have to delete any employment-related records as employers must be able to protect their workforces, and substantiate all such activity. Any request for deletion of employment records should be substantially limited to records not required to be maintained by law.

* * * * *

Thank you for your consideration of NAPEO's requests. The Attorney General is given broad authority to write regulations to further the purposes of the CCPA. We believe that broad and ambiguous definitions may result in an inconsistent implementation of the law, which in turn could defeat its purpose. We urge the Attorney General's office to clarify these points during rulemaking. Should you have any questions with respect to the issues discussed herein or NAPEO's position on such matters, please contact me at [REDACTED]

Sincerely,

Daniel A. Harris
Vice President, State Government Affairs
NAPEO

Message

From: Danielle Coffey [REDACTED]
Sent: 3/8/2019 1:46:40 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Tanya Forsheit [REDACTED]
Subject: News Media Alliance Comments
Attachments: NMA California AG Comments FINAL.pdf

Please find attached News Media Alliance comments regarding CCPA.

Danielle

Danielle Coffey

SVP, Strategic Initiatives / Counsel

News Media Alliance

[REDACTED]

March 8, 2019

The Honorable Xavier Becerra
Attorney General, State of California
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Dear Attorney General Becerra:

A thriving free and independent press is an essential part of any healthy democracy. Only the media can cast light on the inner workings of power and equip the citizenry to exert democratic control at all levels from local to federal. A well-designed comprehensive privacy law should protect individual privacy rights without stifling the free flow of information and news organizations' ability to deliver essential information to the people of the State of California.

The News Media Alliance ("Alliance") is the voice of the news media industry. Its membership represents over two thousand (2,000) diverse news organizations in the United States—from the largest news groups and international outlets to hyperlocal news sources, from digital to print news. The Alliance respectfully submits the following comments and urges the Attorney General to carefully consider the significant negative consequences the California Consumer Privacy Act ("CCPA") will have on the freedom of the press and consumers in the absence of critical clarifications that can be included as part of this rulemaking and in related industry guidance.

I. The Rules Must Clarify the Scope of the Protections for Journalism Set Forth in the Act.

The role of journalism in our country serves the core mission of informing the public, which is critical to a healthy democracy and a civic society. Today, maybe more than ever, readers of local and national news depend on reporters who spend countless hours uncovering facts and acting as the watchdogs of those in power. Newsrooms commit tremendous capital and resources to those efforts, prioritizing the output of quality journalism over short-term gain.

In the digital advertising ecosystem, in which news publishers participate in order to help sustain the business of news, there are systematic flaws that have been recognized by lawmakers related

to data collection and unexpected uses of that data. The news media industry commends the intent of the statute and offers its support in shaping implementation to reflect the primary goals of the CCPA.

Legislators properly recognized noncommercial newsgathering activities that were protected through a September 2018 amendment to the CCPA as a step in the right direction. News publishers further request recognition of commercial activities that are necessary to sustain journalism, conditioned upon a limitation of the secondary uses of that data. This would maintain the integrity of the CCPA’s intention to target certain unexpected uses of personal data while still protecting journalism.

Such a distinction would also avoid the unintended consequences that occurred with General Data Protection Regulation (“GDPR”) in which advertising technology providers asserted themselves as independent controllers of the consumers’ data, pushed their transparency obligations off to the publishers, and left it a mystery as to how they might be using the consumers’ data in other unidentified ways. In this perverse twist of the law, advertising technology providers managed to continue the secondary uses and at the same time interfere with the trusted reader-publisher relationship. This behavior can and should be prevented in the CCPA.

A. The California Legislature Properly Recognized the Importance of Noncommercial Newsgathering Activities in Furtherance of Quality Journalism.

The First Amendment to the U.S. Constitution and the California Constitution¹ protect a free and independent press. The text of the CCPA explicitly recognizes these constitutional protections by excluding newsgathering from the definition of “commercial purposes”² and by exempting newsgathering activities from the CCPA’s requirements:

The rights afforded to consumers and the obligations imposed on any business under [the CCPA] shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.³

¹ California Constitution Art. I, §2.

² “‘Commercial purposes’ do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.” CIV. CODE §1798.140(f).

³ CIV. CODE §1798.145(k). Section 2(b) of Article I of the California Constitution states as follows: “A publisher, editor, reporter, or other person connected with or employed upon a newspaper, magazine, or other periodical publication, or by a press association or wire service, or any person who has been so connected or employed, shall not be adjudged in contempt by a judicial, legislative, or administrative body, or any other body having the power to issue subpoenas, for refusing to disclose the source of any information procured while so connected or employed for publication in a newspaper, magazine or other periodical publication, or for refusing to disclose any unpublished

Because of this language and clear intent of the legislature to exempt journalism from the Act's requirements, it is our understanding that the definition of "sale" was intended to exclude these constitutionally protected noncommercial activities.⁴ However, this is not evident based on the current broad definition of sale, and as a result we suggest the clarifications discussed in more detail directly below.

B. The CCPA Should Also Support Commercial Activities that Support Quality Journalism and Prevent Unintended Secondary Uses.

The Attorney General has the authority to adopt regulations under Civil Code section 1798.185(a)(3) "[e]stablishing any exceptions necessary to comply with state or federal law...". The freedom of the press is protected under federal and state law and should not be crippled by the inability of news media organizations to share information that comes from/is directly related to a consumer's interaction with the publisher with those critical to the creation and distribution of information to the people.

Ever since Benjamin Day started publishing the first popularly affordable newspaper when he founded the ad-supported New York Sun in 1833, advertising has been a vital component of the press's business model, essentially subsidizing access to journalism. Advertising is the backbone of the free Internet, but it also is the reason news organizations can survive in the digital era. In the United States, circulation has plummeted over the past 24 years from a high of nearly 60 million in 1994 for print subscription to 35 million for combined print and digital distribution today.⁵ Between 1994 and 2014, newsroom employment declined by 40%.⁶

If and when readers exercise their "Do Not Sell" rights, first-party news publishers should still be able to use advertising technology service providers to support journalism — however, those service providers should not be allowed to make any manner of secondary use of the personal information outside of well-defined essential purposes such as security and debugging.

information obtained or prepared in gathering, receiving or processing of information for communication to the public. ¶ Nor shall a radio or television news reporter or other person connected with or employed by a radio or television station, or any person who has been so connected or employed, be so adjudged in contempt for refusing to disclose the source of any information procured while so connected or employed for news or news commentary purposes on radio or television, or for refusing to disclose any unpublished information obtained or prepared in gathering, receiving or processing of information for communication to the public."

⁴ CIV. CODE §1798.140(t)(1) ("Sale" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communication orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or to a third party for monetary or other valuable consideration.)

⁵ Douglas McLennan and Jack Miles, *A Once Unimaginable Scenario: No More Newspapers*, THE WASHINGTON POST (March 21, 2018),

https://www.washingtonpost.com/news/theworldpost/wp/2018/03/21/newspapers/?utm_term=.d7650756a7e0.

⁶ *Id.*

The Attorney General should adopt rules to align the journalism noncommercial exception with the provisions governing “sales” of information in the interest of supporting low cost and widely available journalism. The Alliance supports providing consumers with greater control, choice, and transparency concerning their personal information. However, without appropriate rules and guidance, the CCPA is likely to cripple the business model of many news organizations, which are largely supported by advertising revenue, and risks depriving many consumers of access to such news and information. In 2017, 31% of newspapers revenue came from digital advertising.⁷

The Attorney General should also clarify in its rulemaking that any sharing of personal information by a news organization with another business – required to be a “service provider” – to support reduced cost and widely available journalism online, even if done in exchange for money or other value, is not a sale – or, at a bare minimum, subject to the exclusion for journalism built into the definition of “commercial purposes.”

These clarifications would provide numerous benefits to consumers and the free press. Preventing third parties from using personal information for unexpected secondary purposes would match consumers’ expectations since their information would remain entirely under the control of the party with which they are deliberately interacting, the news organization.

In order to avoid the unintended consequences that occurred with GDPR, such an interpretation would reinforce the consumer-trusted first party relationship and avoid others asserting that same relationship – which, based on experience, we know they will do. For example, just before implementation of GDPR, on March 22, 2018, Google notified news publishers that it would assert itself as an independent controller with respect to the personal data of the news publishers’ end users and would unilaterally make decisions regarding how that personal data, collected by news publishers, would be used in providing advertising services. Google nonetheless expected its publisher customers to obtain legally valid consent on behalf of the publisher itself *and* Google.

II. The Attorney General Should Issue Regulations Supporting Financial Incentives Related to Personal Information and Confirming that Discounts and/or Service Enhancements Will Not Be Prohibited as Discriminatory.

Section 1798.125 is internally inconsistent. On the one hand, subsection (a) prohibits a business from discriminating against a consumer because the consumer exercised any of its rights, including by denying goods or services to the consumer, charging different prices or rates for goods or services, including through the use of discounts or other benefits, providing a different

⁷ Pew Research Center on Journalism and Media available at <http://www.journalism.org/fact-sheet/newspapers/>.

level or quality of goods or services to the consumer, or “suggesting” that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

On the other hand, subsection (a)(2) states that nothing in the law shall prohibit a business from charging a consumer a different price or rate, or from providing a different level of quality of goods or services to the consumer, if that difference is “reasonably related to the value provided to the consumer by the consumer’s data.”⁸ Subsection (b) also gives businesses the right to offer financial incentives, including payments to consumers as compensation, for the collection, sale, or deletion of their personal information.⁹

The Attorney General should issue regulations reconciling the ability to tie different prices or rates that are “reasonably related to the value provided by” the information under 1798.125(a)(2), and the ability to offer incentives for the sale of personal information under 1798.125(b)(1). News organizations should be allowed to charge more for providing access to sites and applications to consumers who opt-out and effectively demand ad-free products. If news organizations are forced to discontinue incentive programs, the low-income populations will be denied access to news as only the premium services unsupported by advertisements will be available.

The legislature has already recognized that freedom of the press requires significant exemptions from the requirements of the CCPA in order to avoid the erosion of an independent and diverse media. The Attorney General should take simple steps, outlined above, to ensure the legislation is implemented and enforced consistent with those intended protections of the press.

III. Additional Concerns That Are Not Specific to the News Industry Include a Potentially Expanded Private Right of Action and Adjustments Needed to Various Definitions.

A. The Attorney General is Best Equipped to Enforce the Privacy Provisions of the Act and Should Not Relinquish Its Role to Self-Interested Private Attorneys.

The Alliance strongly encourages the Attorney General, in its role as the top privacy enforcer in the State of California, to advocate for the strengthening of that critical role through the

⁸ It seems highly likely that this includes a typo, somehow not addressed in the September 2018 technical amendments, and should read “reasonably related to the value provided to the **business** by the consumer’s data.”

⁹ Repeating the apparent typo mentioned supra. note 8, subsection (b) states that financial incentives may also include offering a different price, rate, level, or quality of goods or services, if the difference is related to the “value provided to the consumer by the consumer’s data.” No one appears to understand or know what is meant by “value provided to the consumer by the consumer’s data.”

elimination of the ability of plaintiffs' lawyers, who do not have the expertise or breadth and depth of experience that the Attorney General, to dictate public policy through the filing of private actions.

As noted by Professor Danielle Citron¹⁰ in her groundbreaking paper on the privacy policymaking of state attorneys general:

State attorneys general have been nimble privacy enforcement pioneers Career staff have developed specialties and expertise growing out of a familiarity with local conditions and constituent concerns. Because attorneys general are on the front lines, they are often the first to learn about and respond to privacy and security violations. . . . Given the important role that attorneys general have played in addressing privacy and data security issues, their enforcement power should not be curtailed or eliminated without careful consideration.¹¹

Moreover, the CCPA was designed to enhance the Attorney General's powers beyond those available today. Under the CCPA, the Attorney General has the ability to seek fines and penalties ranging from \$2,500 to \$7,500, *all of which* financial penalties (including the proceeds of any settlement) must be deposited directly in the Consumer Privacy Fund, to *fully offset* any costs incurred by the state courts and the Attorney General in connection with the CCPA.¹² Even a single action by the Attorney General against an organization intentionally violating the Act with respect to the personal information of only one million consumers (a small number when it comes to data brokers) could net a settlement of hundreds of millions of dollars for the People of California. By contrast, a class action lawsuit in the same situation would likely result in substantial payments to *the lawyers*, small payments to individual claimants, and *nothing* to the State.

It is critical that the Attorney General use its own authority to pursue and collect these funds from bad actors and not allow plaintiffs' class action lawyers with no privacy experience to appropriate the role of "privacy cop" in order to line their own pockets with funds that should be used to protect the fundamental constitutional privacy rights of the People of the State of California.

¹⁰ Morton & Sophia Macht Professor of Law, University of Maryland Carey School of Law; Affiliate Scholar, Stanford Center on Internet & Society; Affiliate Fellow, Yale Information Society Project; Senior Fellow, Future of Privacy Forum.

¹¹ Danielle K. Citron, The Privacy Policymaking of State Attorneys General, 92 Notre Dame L. Rev. 747, 750, 800 (2017), available at: <https://scholarship.law.nd.edu/ndlr/vol92/iss2/5>.

¹² CIV. CODE §1798.155(c).

B. The Regulations Should Clarify the Application of Ambiguous Definitions.

There are a number of definitions in the Act that, without clarification through this rulemaking, will result in detriment to news organizations and, consequently, consumers.

i. Definition of Personal Information

Current Definition of Personal Information: (1) “Personal information” is defined to mean information that identifies, relates to, describes, *is capable of being associated with*, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household ...”

While the definition does not include publicly available information, “publicly available” is itself defined to mean only information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information [sic].” The definition of “publicly available” also does not apply to data that is “used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.”¹³

The Attorney General has authority to adopt regulations to that would “[u]pdat[e] as needed additional categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (o) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, privacy concerns.”¹⁴

The Attorney General can and should use this opportunity to put in place regulations that recognize how technology actually works in 2019. While the language “capable of being associated with” could mean that *everything* is personal information,¹⁵ the Attorney General should issue regulations that reflect reality and narrow the scope of “personal information” from

¹³ CIV. CODE §1798.140(o).

¹⁴ CIV. CODE § 1798.185(a).

¹⁵ Researchers have demonstrated for years the ability to easily reidentify individuals based on allegedly “anonymized” information sets. Natasha Singer, “With a Few Bits of Data, Researchers Identify ‘Anonymous’ People,” New York Times, January 29, 2015, available at <https://bits.blogs.nytimes.com/2015/01/29/with-a-few-bits-of-data-researchers-identify-anonymous-people/> (“Even when real names and other personal information are stripped from big data sets, it is often possible to use just a few pieces of the information to identify a specific person, according to a study [‘Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata’] . . . in the journal Science”). Even amateurs have successfully undertaken experiments to do the same at little expense. *Id.* (In the fall of 2014, “a reporter at Gawker was able to reidentify Kourtney Kardashian, Ashlee Simpson and other celebrities in an ‘anonymized’ database of taxi ride records made public by New York City’s Taxi and Limousine Commission”).

what could *theoretically* be associated with a consumer to that which is *reasonably likely* to be so associated *without disproportionate time and effort*. Without such common sense narrowing, businesses will have no basis upon which to identify and classify information that must truly be protected consistent with the new law and with respect to which consumers must be afforded rights.

The Attorney General should also use this opportunity to align the carve-out for “publicly available information” with constitutional parameters. Publicly available information should include information that *is, in fact, publicly available*, in posted stories and articles, and not just that information “lawfully made available from federal, state, or local government records.”

ii. Definition of Business

Current Definition of Business: “Business” means (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers’ personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information, that does business in the State of California, and that satisfies one or more of the following thresholds: (A) Has annual gross revenues in excess of twenty-five million dollars (\$25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185. (B) Alone or in combination, annually buys, receives for the business’s commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices. (C) Derives 50 percent or more of its annual revenues from selling consumers’ personal information.¹⁶

There is no definition of what is meant by “doing business” in the State of California. Without guidance, regional news organizations that transact business with vendors in California, that have in excess of \$25,000,000 in revenue, and that collect only nominal amounts of personal information of California consumers (since that definition in its current form includes vendor representatives), would be swept into the scope of the CCPA and therefore deterred from transacting *any* business in California. The Attorney General should provide guidance as to what “doing business” means in relation to the CCPA and clarify that “annual gross revenue” refers to revenue received from California consumers, not worldwide revenue.

¹⁶ CIV. CODE §1798.140(c).

iii. Definition of Homepage

Current Definition of Homepage: “Homepage” is defined to mean the introductory page of an Internet Web site and any Internet Web page where personal information is collected. In the case of an online service, such as a mobile application, homepage is defined to mean the application’s platform page or download page, a link within the application, such as from the application configuration, “About,” “Information,” or settings page, and any other location that allows consumers to review the notice required by subdivision (a) Section 1798.145, including, but not limited to, before downloading the application.¹⁷

The Attorney General should issue rules to clarify that the definition of homepage will not be interpreted to mean every page of a website or application.

iv. Definition of Consumer

Current Definition of Consumer: “Consumer” means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.¹⁸

This broad definition could be read to include employees and individual business representatives, even though they are not in fact “consumers” as that term is commonly understood. The unintended consequence would be to endow personnel, freelance journalists, and vendors who are California residents with privacy rights designed for those who have a true consumer relationship with a business. This would also create tension with existing California and federal laws in the employment and fraud prevention space, among others, designed to protect employees and businesses alike. The recently proposed Washington state Privacy Act (Senate Bill 5376) explicitly excludes employees and contractors from its scope, and the Attorney General should interpret the CCPA in the same way.

The definition of “consumer” is also problematic because California residence is defined by tax provisions that deem an individual a resident even if he or she is temporarily located outside of California. As such, “businesses” that commonly use IP addresses, billing addresses or delivery addresses to determine the location of a consumer will be stymied in their ability to determine whether an individual is even covered by the CCPA. The Attorney General should issue rules approving the use of location indicators such as IP address as a proxy for residency, so that “businesses” are not forced to apply the CCPA to individuals located in each of the fifty states and the law does not risk being found unconstitutional.

¹⁷ CIV. CODE §1798.140(l).

¹⁸ CIV. CODE §1798.140(g).

v. Definition of Business Purposes

Current Definition of Business Purposes: The current definition of “business purposes” includes a list of seven activities that are business purposes.¹⁹ The Attorney General should consider clarifying in its rulemaking that this list is exemplary and not exhaustive.

C. The Attorney General Should Issue Practical Guidance on the Meaning of a “Verifiable Consumer Request”

The CCPA requires the Attorney General to establish rules and procedures to govern a business’s determination that a request for information received by a consumer is a verifiable consumer request, “including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business’s authentication of the consumer’s identity.”²⁰ The Attorney General should clarify that a “verifiable consumer request” includes a request obtained from the email addresses or other identifier the covered business has in its records as the current email address or identifier of the individual making the request.

D. The Attorney General Should Issue Practical Guidance on an Icon in Lieu of “Do Not Sell” Language.

Publishers support the creation of a universal opt-out icon for interest-based advertising, noting possible consumer confusion and additional compliance costs associated with the lack of a common method as well as the benefit of using a standardized icon to increase of consumer transparency (as suggested by the EU Article 29 Working Party 's guidance on Transparency).

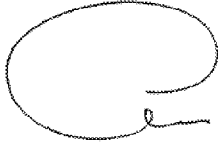
¹⁹ CIV. CODE §1798.140(d).

²⁰ CIV. CODE §1798.185(a)(7).

IV. Conclusion

We appreciate the consideration of these comments of the news media industry and we offer our continued support for this effort to enhance the privacy protections of our readers while maintaining the ability to support quality journalism.

Sincerely,

A handwritten signature in black ink, appearing to read 'D. Chavern', with a large, stylized 'D' and a trailing flourish.

David Chavern
President & CEO
News Media Alliance

Message

From: Keating, David [REDACTED]
Sent: 3/8/2019 4:56:31 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: [REDACTED]
Subject: NRF & CRA Joint Comments on CCPA
Attachments: NRF-CRA Comments to AG re CCPA (Submitted 3-8-2019).pdf

On behalf of the National Retail Federation and the California Retailers Association, I am submitting the attached comment letter as part of the pre-rulemaking process of the Office of the Attorney General under the California Consumer Privacy Act.

Sincerely,

David Keating

David C. Keating

Alston & Bird LLP

[REDACTED]

www.alstonprivacy.com

NOTICE: This e-mail message and all attachments may contain legally privileged and confidential information intended solely for the use of the addressee. If you are not the intended recipient, you are hereby notified that you may not read, copy, distribute or otherwise use this message or its attachments. If you have received this message in error, please notify the sender by email and delete all copies of the message immediately.



March 8, 2019

Via Email to PrivacyRegulations@doj.ca.gov

California Department of Justice
Attn: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, California 90013

Re: NRF & CRA Joint Comments on CCPA during the Pre-Rulemaking Process

Dear Attorney General Becerra:

The National Retail Federation and California Retailers Association appreciate the opportunity to jointly submit comments to the California Department of Justice as part of the Attorney General's pre-rulemaking process under the California Consumer Privacy Act (CCPA). The Attorney General's Office has an enormous responsibility regarding the CCPA to fulfill within a very short timeframe. The purpose of these comments is to provide the perspective of the retail industry on several of the areas within the Attorney General's rulemaking authority relating to the new privacy standards established by the CCPA.

The National Retail Federation is the world's largest retail trade association. Based in Washington, D.C., NRF represents discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the nation's largest private-sector employer, supporting one in four U.S. jobs — 42 million working Americans. Contributing \$2.6 trillion to annual GDP, retail is a daily barometer for the nation's economy.

The California Retailers Association is the only statewide trade association representing all segments of the retail industry including general merchandise, department stores, mass merchandisers, restaurants, convenience stores, supermarkets and grocery stores, chain drug, and specialty retail such as auto, vision, jewelry, hardware and home stores. CRA works on behalf of California's retail industry, which currently operates over 418,840 retail establishments with a gross domestic product of \$330 billion annually and employs 3,211,805 people—one fourth of California's total employment.

A. THE ATTORNEY GENERAL'S AUTHORITY UNDER THE RULEMAKING PROCESS

The CCPA designates the Office of the Attorney General as an essential partner in the development and enforcement of the new law. The statute expressly authorizes businesses to request

advisory opinions from the Attorney General.¹ The Attorney General's office has broad enforcement authority and the ability to recover sizable penalties for violations of the Act.² Consumers must effectively seek Attorney General approval before proceeding with private civil actions under the CCPA.³

The CCPA also requires the Attorney General to "solicit broad public participation and adopt regulations to further the purposes of the [statute]."⁴ The statute provides several examples of areas to be addressed as part of this rulemaking activity. These areas are listed in the Public Forum Materials⁵ published by the Attorney General's Office for the instant pre-rulemaking process. Our comments cover the following listed areas:

1. Categories of Personal Information (*See* Part B.3(b).)
2. Exceptions to CCPA (*See* Part B.1.)
3. Submitting and Complying with Requests (*See* Parts B.3(b), B.3(d).)
4. Notices and Information to Consumers, including Financial Incentive Offerings (*See* Part B.1.)

The CCPA makes clear that the topics set out in the statute are not an exclusive list. The law states that the Attorney General "shall . . . adopt regulations to further the purposes of this title, **including, but not limited to**, the [listed] areas."⁶ We accordingly have included additional discrete areas⁷ that we suggest the Attorney General should include in its rulemaking efforts in order to "further the purposes of the [CCPA]."⁸ If, in the Attorney General's determination, he lacks the authority to address these concerns in the rulemaking, we would appreciate his efforts to work with the legislature to support statutory amendments that would address these additional discrete areas.

B. COMMENTS ON DISCRETE AREAS OF THE CCPA

1. Preserving Consumer Benefits from Customer Loyalty and Discount Programs

Protecting consumer privacy is one of retailers' highest priorities. Retailers know that establishing long-term relationships with their customers requires more than just providing the merchandise they want at the prices they are willing to pay. Successful retailers win their customers' trust and provide a satisfying shopping experience so that consumers continue to shop with them time and again. A critical element of establishing that trusted relationship lies in how retailers act as reliable stewards of the information their customers share with them when shopping.

Retailers have a long history of nurturing customer relationships and meeting consumer expectations for high quality service. Whether offering goods online or in store, retailers use customer data to provide personalized experiences that consumers value. Customers, in turn, expect retailers to process their personal data responsibly and seamlessly when they are shopping. To meet

¹ Cal. Civ. Code § 1798.155(a).

² Cal. Civ. Code § 1798.155(b).

³ Cal. Civ. Code § 1798.150(b)(2).

⁴ Cal. Civ. Code § 1798.185(a).

⁵ <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-ppt.pdf>

⁶ Cal. Civ. Code § 1798.185(a) (emphases added).

⁷ *See* Parts B.2, B.3(a) and B.3(c) below.

⁸ Cal. Civ. Code §§ 1798.185(a), (b).

these high customer expectations, retailers invest heavily in technology and spend years developing appropriate methods to comply with state, federal and global data protection regulations in ways that further their customer relationships and do not frustrate them.

In short, retailers use consumer data for the principal purpose of serving their customers as they wish to be served. Retailers' use of personal information is not an end in itself but primarily a means to achieving the goal of improved customer service. This differentiates retailers' principal use of customer data from businesses – such as service providers, data brokers and other third parties unknown to the consumer – that primarily collect, process and sell consumer data as a business-to-business service.

An important way that many businesses, including retailers, develop lasting relationships with their customers is by providing tailored service and lower prices than their competitors in the same industry sector. “Club” discount cards, airline travel frequent-flyer rewards, hotel repeat-stay programs, retail discount coupons, advanced product release programs, exclusive V.I.P. customer experiences and other forms of customer loyalty and discount programs are ubiquitous across industry and highly popular among consumers as well. According to a recent study published by Forrester Research, 72% of American adults online belong to at least one loyalty program.⁹ The average number of loyalty program memberships that each adult has is nine.¹⁰

Although the authors of A.B. 375 stated during the bill's consideration that it was not their intent to eliminate consumer loyalty programs, the retail industry is concerned that offers of common loyalty program features and practices could be challenged as alleged violations of the CCPA's restrictions on discrimination.¹¹ The CCPA thus puts extraordinary pressure on these customer-favored programs by creating a significant liability risk for businesses which provide rewards or other benefits, such as preferred service or pricing, to customers who sign up for these programs.

If not addressed in the rulemaking or by statutory amendment, the CCPA's existing express prohibition on “charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties”¹² would create a substantial risk of liability for retailers and other consumer-facing businesses that offer loyalty programs, particularly where some of their customers choose not to participate (*i.e.*, by exercising a right under the CCPA) and a claim may be made that the business then violated the CCPA's nondiscrimination section by offering discount prices or better levels of service to its other customers who choose to participate.

Although the legislature recognized the unintended consequence and potential impact on loyalty programs that Californians wish to preserve, it failed in its attempt to create a savings clause that insulates these favored programs from other acts of prohibited discrimination and retaliation against consumers who may exercise a right under the CCPA. Because the statutory language fails to fully correct and guard against the unintentional impact on programs that benefit consumers, we urge

⁹ Forrester Research, *How Consumers Really Feel about Loyalty Programs*, May 8, 2017.

¹⁰ *Id.*

¹¹ Cal. Civ. Code § 1798.125(a) (“A business shall not discriminate against a consumer because the consumer exercised and of the consumer's rights under this title, including, but not limited to, by . . . charging different prices or rates for goods or services, including through the use of discounts or other benefits . . .”).

¹² Cal. Civ. Code § 1798.125(a)(1)(B).

the Attorney General to address this concern in its interpretation of Section 1798.25 of the CCPA and to support statutory changes necessary to correct this mistake in the law.

One way the CCPA currently fails to protect customer loyalty programs is its creation of a novel and uncertain comparative valuation test for hundreds of thousands of businesses – mostly small and mid-sized businesses serving Californians – that already offer discounted goods or preferred services to customers. This new legal mechanism to justify common commercial behavior regarding discounts and service sets a potential litigation trap to be tested in the courts, requiring legal resources most small and mid-sized businesses do not have simply to preserve what are essentially discounts and preferred service programs for their customers.

Under the CCPA, as currently drafted, any practices or programs through which businesses provide preferred service or pricing to their customers who want them, when other customers exercising rights do not wish to participate, are permitted to keep these programs only so long as they can prove that the “value” of the personal information to the participating consumer used by the business is met by an equivalent value in discounts or benefits received by them.¹³ This is a legal equation fraught with such ambiguity that it invites an infinite array of “economic” opinions for state courts to weigh in potentially protracted class action litigation.

The value of personal information that may be “priceless” in one consumer’s eyes would never equate subjectively to a reasonable discount on a product. The potential for litigation over this most basic of retail transactions could lead some stores to shut down loyalty programs altogether – or not make them available to Californians – because the CCPA creates an untenable business litigation risk. These stores reasonably could determine that the potential costs of lawsuits testing the meaning of this part of the statute outweighs the potential benefits to the business from providing better service and discounts to their most loyal customers.

For example, assume a consumer requests a retailer to delete any personal information it collected from her.¹⁴ The retailer must comply subject to certain limited exceptions.¹⁵ But what if this same consumer participates in a loyalty program offered by the retailer which provides rewards based on the quantity or dollar value of prior transactions? The data necessary to measure past purchases will no longer be linkable to the consumer, thus impacting the consumer’s entitlement for discounts or rewards under the program. Does this constitute impermissible discrimination under Cal. Civ. Code § 1798.125(a)?

Private label credit cards tied to discounts or coupons provide another example. Assume our consumer opts out of data sales by the retailer pursuant to Cal. Civ. Code § 1798.120. Assume this same consumer has a private label card from the retailer which awards coupons based on monthly spend. Does the retailer sell personal information to the issuing bank when reporting transaction volumes? Does the bank sell personal information to the retailer by issuing coupons to the consumer that the consumer later uses at the store or online?

The retail industry would of course contend these scenarios do not violate the CCPA, but it is likely these questions, and many other similar scenarios raised by common loyalty

¹³ Cal. Civ. Code § 1798.125(a).

¹⁴ Cal. Civ. Code § 1798.105(a).

¹⁵ Cal. Civ. Code § 1798.105(c).

program features and operations, will be resolved only through litigation due to the lack of clarity in Section 1798.125. This concern is heightened by the recent proposal in S.B. 561¹⁶ to amend the CCPA to establish a private right of action with statutory damages for any violation of the law. Plaintiffs' attorneys would have a powerful incentive to initiate class action proceedings to test the bounds of the CCPA.

We urge the Attorney General to consider the potential litigation that could arise over any provision that conditions the offering of a loyalty program on the "value" of personal information in light of the infinite number of "economists" who might be certified by courts as experts to opine on ranges in value that could be as different as night and day for the same data set. The intent of this provision was not to threaten these programs that consumers love. We therefore ask the Attorney General to clarify in its regulations that consumer loyalty programs and practices providing better prices or service to customers who desire them are exempt from the nondiscrimination provisions of Cal. Civ. Code 1798.125(a) and are not required to meet the financial incentive program standards of Section 1798.125(b). Such clarification would ensure that the CCPA does not lead to the obsolescence of loyalty programs for Californians.

2. Right-Sizing CCPA Enforcement and Penalties to the Severity of the Violation

(a) Proposed Policy Considerations for Interpreting the Text of the CCPA's Private Right of Action and Statutory Damages

The CCPA establishes a new private right of action and statutory damages for certain data security incidents that result from the business's failure to satisfy its statutory duties with respect to information security.¹⁷ Claimants may recover damages of between \$100 and \$750 per consumer per incident or actual damages, if greater.¹⁸ Courts are not authorized to award damages less than \$100 per consumer, per incident. Some quick calculations make clear that this restriction on judicial discretion can result in enormous and financially ruinous damage awards without regard to the size of the business, the circumstances of the breach, or mitigating factors such as the good faith or level of cooperation of the business.

For example, an online business that has one million California customers (a modest number by e-commerce standards) could face a *minimum* of a one billion dollar fine for a violation of the data security provision in light of the \$100 per consumer per incident calculation established by statute. A statutory penalty such as this far exceeds any penalty seen anywhere else in the world for privacy violations. Under the European Union's General Data Protection Regulation (GDPR), for instance, a company's annual total global revenue would need to be at least \$25 billion to be at risk of facing a one billion dollar fine.

We respectfully request that the Attorney General consider establishing a rule that creates a per-incident cap on the aggregate statutory damages a business may face under the CCPA. The capped amount could be established by reference to the size of the business – a model that would align with the approach adopted by the GDPR.¹⁹ The GDPR authorizes EU data protection

¹⁶ S.B. 561 (Cal. 2019).

¹⁷ Cal. Civ. Code § 1798.150(a)(1).

¹⁸ Cal. Civ. Code § 1798.150(a)(1)(A).

¹⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

authorities to assess administrative fines, but these fines are capped at the greater of €20 million or 4% of global annual revenue.²⁰ Uncapped statutory damages calculated based solely on the number of consumers creates virtually unlimited financial exposure for businesses that are not malicious or reckless bad actors, but rather are the victim of often highly sophisticated financial fraud and computer crimes that lead to data security breaches.

In addition, minimum statutory damages (currently set at \$100 per consumer, per incident) create the potential for ruinous financial impact when a different response may be more appropriate. Consider a recent situation in Germany in which a hacker acquired account passwords that a German social media company, Knuddels, had maintained in clear text.²¹ The hacker used these account credentials to steal the information of approximately 1.91 million users, including 808,000 email addresses. Under the CCPA, Knuddels could face statutory damages totaling between \$191 million and \$1.423 **billion**.

The outcome under the GDPR was different, however. The company in Germany was motivated to exhibit significant cooperation with the regulator and to implement recommendations and guidelines of the data protection authority. The regulator in response ultimately assessed a fine of €20,000. Knuddels remained in business, and customer data protections were enhanced. We think this is a more reasonable and practical approach that encourages companies to cooperate with regulators and allows the regulators to assess fines based on the entirety of the facts related to a statutory infringement. We therefore request the Attorney General through the rulemaking process establish a rule that removes the \$100 per consumer, per incident floor on statutory damages. This would afford the courts the discretion to consider the circumstances surrounding a breach, including any mitigating factors, in assigning a damage award to a business.

We look forward to working with the Attorney General to address these concerns with the CCPA's private right of action and statutory damages, and appreciate his consideration of the alternative solutions offered above. If the Attorney General believes that a cap or removal of the minimum statutory amount is warranted but beyond his rulemaking authority, then we would respectfully request the Attorney General support efforts in the legislature to make such statutory modifications as necessary to address the concerns raised above.

(b) Concerns with Provisions of S.B. 561 that would Amend the CCPA's Enforcement Section

The Attorney General has announced support for S.B. 561, introduced in the State Senate on February 22, 2019. This bill, if enacted into law, would (a) expand the CCPA's private right of action and statutory damages to apply to *any* violation of the Act, however minimal; (b) remove the period of time in which businesses may cure alleged noncompliance before being deemed in violation of the law; and (c) withdraw the right of businesses to seek advisory opinions from the Attorney General. While we believe the CCPA's provision on seeking advisory opinions provides a very useful mechanism for delivering helpful guidance to California consumers and businesses, we are more concerned that the proposed extension of the private right of action and the inability to cure

²⁰ GDPR, Art. 83(5). Less significant infringements are subject to a cap equal to the greater of €10 million or 2% of global annual revenue. GDPR, Art. 83(4).

²¹ <https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/02/LfDI-34.-Datenschutz-Tatigkeitsbericht-Internet.pdf>

alleged noncompliance (i.e., the first two elements of S.B. 561 noted above) would create disproportionate liability risk and financial harm to the retailers and other businesses in California. We therefore respectfully request the Attorney General consider the potential consequences of S.B. 561, in the form as introduced, and the policy concerns it raises.

(i) *Expanding the Private Right of Action and Statutory Damages to the Entire CCPA Would Create Disproportionate and Misplaced Liability Risks for Businesses*

A private right of action applying to the entirety of the CCPA is incapable of addressing the fact that not every violation of the CCPA will be equal, and that the consequences and impact on consumers may vary greatly depending on the nature of the violation, the size and nature of the company, the data that was implicated and other factors. The CCPA already allocates greater liability – in the form of the private right of action that exists today – to data security breaches. Other violations of the Act, though, are subject to enforcement by the Attorney General. We believe the Attorney General’s oversight here can provide for a more even-handed approach to CCPA enforcement, particularly with respect to the untested privacy provisions that businesses will need to address through new compliance programs under the statute.

With respect to data security breaches, where the CCPA already provides a private right of action, it should be noted that businesses have had over 15 years of experience with breach notification law in California and there is greater familiarity with the relevant legal standards. Maintaining the role of the Attorney General to exercise prosecutorial discretion with enforcement of a new comprehensive statute requiring extensive modifications to customer data systems and processes is vital to ensuring that CCPA enforcement and penalties are proportionate to the alleged violations of the Act.

This distinction between major and minor violations of a privacy law have precedent and are also consistent with the approach adopted by the GDPR. More significant violations of the GDPR are subject to administrative fines capped at the greater of €20 million or 4% of global annual revenue. Less significant violations, though, are subject to a cap equal to the greater of €10 million or 2% of global annual revenue. In this way, the GDPR attempts to right-size the range of penalties to the severity of the potential violation of the rules.

Expanding the private right of action to the entire law will make it more difficult for well-intentioned businesses to balance CCPA compliance with consumer privacy and data security requirements in the face of potential litigation over how they interpret and implement mechanisms in the face of competing requirements of the law. Here are two examples for your consideration that illustrate this point:

- (A) *Identify verification for data access requests:* As businesses that have tried to do so are keenly aware, it is very challenging to verify the identity of customers in a manner that is not overly burdensome to the consumer and does not require a customer to provide even more sensitive information about themselves (e.g., a copy of their driver license or passport) to authenticate who they are. In efforts to improve identity verification, businesses are trying to find the correct balance between the consumer’s ability to easily access data and their right to privacy. For example, a customer-friendly way to verify identity is to have a customer provide an email address to which the business can then

send a verification message. Since this is not the most secure or reliable way to verify identity, however, the retailer using this process may mask sensitive data fields like credit card numbers. With a private right of action potentially being extended to the verification practices businesses adopt to comply with the CCPA, an enterprising plaintiff's lawyer will allege that the business in the example above failed to provide the actual data to the consumer – the data that was masked – even though there is no harm to the customer from such security measures but rather a benefit in terms of security. This scenario could leave businesses forced either to provide the sensitive data to a person that may not be the actual customer, or to put in place more burdensome identify verification requirements to ensure that it only sends data to verified customers after a more thorough process.

- (B) *Deleting data that is contained in logs and backups*: Retaining security logs is a proven method for putting a business in position to quickly identify potential data breaches and prevent them. Security logs often include personal information, especially given the very broad definition of what constitutes personal information under the CCPA. If businesses were to prematurely begin to delete these security logs for fear of facing frivolous lawsuits, the personal information of these customers will be less secure as a result. The CCPA exempts certain security logs from the data deletion requirement but the language is too narrowly crafted. As it stands, it may be difficult for businesses to demonstrate which security logs are truly needed to detect security incidents and which are kept for other reasons.

In these instances, it is critical that Attorney General oversight – and not private rights of action – are the enforcement mechanism to ensure that well-meaning businesses acting in good faith to comply with the CCPA's competing requirements will not be hamstrung in their implementation. The enforcement mechanism should not leave such businesses feeling forced – for fear of facing unwarranted plaintiffs' actions – to require consumers to engage in more burdensome practices to verify their identity than might otherwise be required. Without a private right of action, businesses could have greater certainty in these situations that the Office of Attorney General understands the technical difficulties in compliance and the reasonable efforts of businesses to get it right. This would permit greater innovation in complying with the CCPA – to the benefit of consumers – by removing the threat of litigation from every aspect of compliance.

The privacy standards established in the CCPA are new, not entirely clear (as evidenced by the legislature granting a right for businesses to request advisory opinions from the Attorney General), and have not been tested in the courts. The retail industry, like other California businesses, is deeply concerned about the prospect for class action litigation exposure arising from good faith business practices in this "grey area" or bankrupting levels of statutory damages that courts have no discretion to lower from simply immaterial, technical violations that do not cause harm to consumers. We submit that enforcement of new, comprehensive data privacy provisions in California is a field much more suited to informed Attorney General oversight and enforcement than to enterprising class action lawyers.

(ii) *Elimination of a 30-Day Right to Cure Alleged Violations Creates Disincentives for Businesses*

The CCPA grants businesses the right to cure alleged statutory violations “[i]n the event a cure is possible.”²² Successfully curing a practice within thirty days after notice of the violation bars an individual action or class action for statutory damages. This approach provides a strong incentive for potential plaintiffs to disclose their complaint clearly to potential business defendants. More importantly, it also provides a strong and effective incentive to businesses to quickly address alleged violations within the thirty-day time frame. Without the right to cure under the CCPA, trial lawyers will continue their practice of sending vague demand letters or filing broad complaints of alleged violations that often rely on “information and belief” claims and do not give well-intentioned businesses enough information to address any alleged violations that may be legitimate compliance issues. Businesses will also be reasonably concerned that remediation measures could be used against them in the resulting lawsuit. This may create a financial disincentive to acknowledge and fix issues that impact the privacy rights of consumers – something that would be more likely if the 30-day right to cure were maintained.

We appreciate the Attorney General’s consideration of the concerns discussed above with these two elements of S.B. 561. We submit that the introduction of a broad private right of action will have a disproportionate impact on businesses without corresponding benefit to consumers. Further, the elimination of the thirty-day cure prior may put consumers in a worse position by chilling businesses’ efforts to innovate and work cooperatively with the Attorney General on compliance.

3. Clarifying the CCPA’s Key Definitions

We respectfully request that the Attorney General, under its authority granted in the CCPA, use the rulemaking process to provide much-needed clarity to consumers and industry alike on certain key definitions in the statute before the law would take effect. We have focused on the following four definitions that our members believe are the most pressing ones to get right so that businesses may comply with the CCPA having much greater certainty as to the scope of the law than they presently have.

(a) The Definition of “Sell,” “Selling,” “Sale” or “Sold”

The CCPA defines a “sale” of personal information in a manner that captures any arrangement in which a business not only sells but “rent[s]” or “mak[es] available” personal information “for monetary or other valuable consideration.”²³ The breadth of this definition captures many types of data-sharing arrangements that are necessary in today’s retail environment, are not viewed by consumers as a “sale” of data, and do not implicate the policy issues underlying the CCPA’s “do not sell” right. For example:

²² Cal. Civ. Code § 1798.150(b)(1).

²³ Cal. Civ. Code § 1798.140(t)(1).

- A small retailer may use a customer list to mail coupons on behalf of different brands stocked in its store. Has the retailer “ma[de] available” to the brands its personal information for “valuable consideration”?
- Retailers continue to invest in digital operations to survive and grow in an increasingly competitive industry. This requires engagement with digital advertising and analytics firms that routinely require the ability to retain data to improve their products and services. Does such retention constitute a “sale” under the CCPA?
- Fraud detection and prevention technologies are also essential in ecommerce operations. The CCPA permits the sharing of personal information to enable a vendor to detect fraudulent or illegal activity.²⁴ But fraud detection providers routinely retain the ecommerce information they process for customers to enhance their own databases for use to deliver services to other businesses. Once again, it’s unclear how this beneficial practice to consumers may be interpreted under the CCPA – if it is a “sale” of data from which consumers may opt out, they would have less anti-fraud protection (*i.e.*, a perverse result.)

We submit that these scenarios do not and should not qualify as sales of personal information. Absent clarification of the definition of “sale” by the Attorney General through its rulemaking authority, these questions can only be answered definitively by the courts. We therefore respectfully request that the Attorney General exercise his authority to establish under the CCPA a narrowly-tailored interpretation of the definition of “sale” that requires monetary consideration.

(b) The Definition of “Consumer”

The traditional definition of a consumer is an individual who is purchasing or interested in the purchase of goods or services for personal, family or household purposes.²⁵ The CCPA, however, defines a consumer as any resident of the State of California.²⁶ This means that the California Consumer Privacy Act applies not only to personal information about consumers in the traditional sense, but also to data about employees, contractors and other individuals.

One consequence of this provision – which could be a mere statutory drafting error – is that businesses will now be required to create and publish employee privacy policies on their Internet home page.²⁷ The extension of the CCPA to employees also creates profound issues relating to the deletion of data. Employees cannot operate in an environment of anonymity, which is anathema to existing law with respect to expectations of privacy in the workplace.

We therefore respectfully request the Attorney General clarify the definition of “consumer” to exclude employees under the authority granted to him in Cal. Civ. Code § 1798.185(b) to promulgate regulations generally “as necessary to further the purposes” of the CCPA.

²⁴ Cal. Civ. Code § 1798.140(d)(2).

²⁵ *See, e.g.*, 15 U.S.C. § 2301(3).

²⁶ Cal. Civ. Code § 1798.140(g).

²⁷ Cal. Civ. Code § 1798.130(a)(5).

(c) The Definition of “Personal Information” and its Inclusion of “Households”

Whether data constitutes “personal information” is the threshold for determining if consumer data is subject to the requirements of the CCPA. Clarity and precision in the definition of personal information is critical for retailers and other businesses to build effective privacy compliance programs under the new law. Any proposal to introduce new categories of personal information or otherwise to interpret the definition pursuant to Cal. Civ. Code 1798.185(a)(1) should therefore be undertaken only with great care.

The GDPR can serve as a helpful reference point in the Attorney General’s consideration of the proper interpretation of this definition. The Regulation defines personal data as information relating to an identified or identifiable natural person.²⁸ The CCPA, however, extends beyond this generally-accepted global definition of personal information to include information that can be linked to a “household” – an undefined term in the CCPA that commonly refers to a dwelling with one or more individuals who may be related or unrelated in a familial sense. This has caused significant confusion and, worse, creates a host of implementation concerns when it comes to determining which data is covered by the CCPA.

It is notable that the statute does not define a household because most businesses do not think of their customers in these terms with respect to protecting and honoring requests regarding consumer information. Many retailers and other businesses are therefore, for the first time, trying to identify information in their control that could be linkable to “households,” a term which presumably includes multiple persons.

Most importantly, a definition of personal information that includes data linkable to a household will create challenges for businesses to honor consumer requests for access, portability and deletion of personal information. Businesses are concerned that producing information linkable to a household may result in data getting into the wrong hands. For example, if a college fraternity or religious order constitutes a household, and any member of the household has the right to request specific pieces of information linked to the household, it may create even greater privacy risks and harms to consumers (i.e., other members of the household). Other scenarios can be envisioned where roommates or families with adult children living at home with their parents create similar risks of harm to *individual* privacy.

Retailers and other businesses are therefore faced with an impossible choice – produce specific pieces of personal information in response to a request that relates to multiple individuals living together in a household, which likely results in a privacy incident, or do not produce the information at the risk of being subjected to an Attorney General enforcement proceeding or a class action lawsuit, should S.B. 561 become law as presently drafted.

For these reasons, we strongly urge the Attorney General to take all steps necessary, pursuant to Cal. Civ. Code 1798.185(a)(1), to resolve the uncertainty of this definition and to address the potential of greater privacy harms that may result by establishing through its rulemaking that the definition of personal information relates to identified persons and excludes “households.”

²⁸ GDPR, Art. 4(1).

(d) The Meaning of “Specific Pieces of Information.”

As noted in the examples above, consumers may request and, upon receipt of a verifiable consumer request, a business must disclose to the consumer “the categories and specific pieces of information the business has collected” about the consumer.²⁹ The statute is not clear whether this means businesses must describe both the “categories” and the “specific pieces” of personal information in their possession, or whether the language requires businesses to describe the categories and provide access to the specific pieces of information.

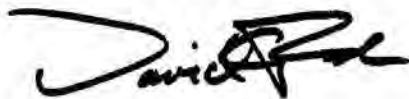
While many interpret the text of the CCPA to provide for the latter, the lack of clarity creates a significant risk of liability for retailers and other businesses, particularly if S.B. 561 is enacted into law. We therefore request the Attorney General, pursuant to his rulemaking authority under Cal Civ. Code §§ 1798.185(a)(7) and 1798.185(b), clarify that the obligation to disclose “specific pieces of information” means businesses must disclose the *categories* of personal information in the business’s control relating to the consumer, subject to applicable conditions and exceptions, rather than to describe each individual piece of information it holds on a consumer.

* * * * *

We appreciate your review of our comments in this letter and look forward to the Attorney General’s continued efforts through the rulemaking process. For any questions or feedback your Office may have concerning our comments, or for more information regarding the concerns of the retail industry more broadly, please contact Paul Martino of the National Retail Federation and Pamela Williams of the California Retailers Association.

Thank you again for the opportunity to provide our views for your consideration at this preliminary stage of the rulemaking process. We look forward to working with you and your staff to address the concerns outlined above.

Sincerely,



David French
Senior Vice President
Government Relations
National Retail Federation



Rachel Michelin
President
California Retailers Association

²⁹ Cal. Civ. Code §§ 1798.100(a), 1798.100(d), 1798.110.

Message

From: Rich, Diana [REDACTED]
Sent: 3/7/2019 2:27:26 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: OPPOSE Expansion of CCPA to Workers' Compensation
Attachments: CCPA (Final) Attny General Comment Letter - Work Comp. (3-6-19).pdf

For your consideration. Please oppose this measure.



Get the FBM Mobile App Today!
Watch this [video](#) to learn more.

- Track orders and view details
- Map my truck functionality
- Find local branches
- Special offers

Download on the App Store
GET IT ON Google Play

March 6, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

VIA US MAIL and EMAIL

TO WHOM IT MAY CONCERN:

The following comments are submitted on behalf of (list workers' compensation medical and ancillary service providers here.)

**The Attorney General Should Exempt the Workers' Compensation System
From the California Consumer Privacy Act**

An Exception From CCPA is Necessary to Comply With the California Constitution
and State Laws Governing the Workers' Compensation System

- 1) The workers' compensation system is established and regulated pursuant to the state Constitution.**
- 2) Pursuant to its constitutional mandate, the Legislature has enacted a comprehensive workers' compensation system by statute.**
- 3) Sufficient privacy protections exist in the workers' compensation system.**
- 4) Workers' compensation is a comprehensive statutory medical, legal and adjudicatory system that is incompatible with the provisions of the CCPA.**
- 5) A regulatory exception from CCPA is needed in order to comply with the comprehensive constitutionally mandated and legislatively enacted workers' compensation system.**

Workers' compensation is a heavily regulated industry, with an extensive body of statutory and constitutional laws governing it. We strongly believe that exempting workers' compensation from the CCPA is appropriate, and we respectfully urge this action be taken as it is "...*necessary to comply with state law*..."

Suggested regulatory language is provided as follows:

Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code does not apply to medical or personal information collected by a business, medical provider network, third party administrator, insurer or other third-party entity for the purpose of providing medical treatment or administering claims pursuant to Division 4 (commencing with Section 3200) of the Labor Code.

Thank you for your consideration.

Sincerely,

Diana J. Rich
Risk Manager and Consultant to Employers


Message

From: Ratican, Sari (Perkins Coie) [REDACTED]
Sent: 3/8/2019 9:31:34 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Shelton Leipzig, Dominique (Perkins Coie) [REDACTED]; Amlani, Natasha (Perkins Coie) [REDACTED]; Ratican, Sari (Perkins Coie) [REDACTED]
Subject: Perkins Coie's Comments on Rulemaking Regarding the California Consumer Privacy Act
Attachments: FINAL 2019_03_08_Perkins Coie Comments (Financial Services Industry).pdf; FINAL 2019_03_08 Perkins Coie Comments (General Industry).pdf

To the Office of the Attorney General:

On behalf of Perkins Coie, LLP, please find attached the following comment reports regarding the California Consumer Privacy Act:

- Perkins Coie Comments (Financial Services Industry)
- Perkins Coie Comments (General Industry)

We wish to thank the Office of the Attorney General for giving the public this opportunity to comment and participate in the process.

Kind regards,

Sari

Sari Ratican | Perkins Coie LLP



PERKINScoie

NOTICE: This communication may contain privileged or other confidential information. If you have received it in error, please advise the sender by reply email and immediately delete the message and any attachments without copying or disclosing the contents. Thank you.



Perkins Coie Comments to the California Attorney General's Office for CCPA Rulemaking: Financial Services

March 8, 2019

DOMINIQUE SHELTON LEIPZIG

PARTNER



SARI RATICAN

SENIOR COUNSEL



NATASHA AMLANI

ASSOCIATE



Executive Summary

Perkins Coie submits the comments herein to the California Attorney General's ("AG") office as part of the AG's rulemaking process for the California Consumer Privacy Act ("CCPA").

These comments in this report pertain to the financial industry. The CCPA correctly exempts institutions that are covered by the Gramm-Leach-Bliley Act ("GLBA") and the Fair Credit Reporting Act ("FCRA") from its provisions. This makes sense. The financial services sector has a long history of privacy protections. It is one of the most heavily regulated industries. The GLBA has been the cornerstone of financial privacy requirements for the past 20 years. As the CCPA correctly recognizes, by excluding GLBA- and FCRA-covered data, there is no need to regulate institutions that are already subject to the high bar imposed by decades of established financial privacy laws enforced by multiple regulators.

Each comment is presented in four parts: (1) a header that synthesizes the issue or concern with the current law, (2) the text and citation to the relevant CCPA section, (3) an illustrative use case to demonstrate the issue or concern with the current law, and (4) proposed regulatory language to address or mitigate the issue or concern raised.

We have organized comments into the Section 1798.185 AG rulemaking mandates and address the issues germane to financial institutions.

Contacts:

DOMINIQUE SHELTON LEIPZIG

PARTNER



SARI RATICAN

SENIOR COUNSEL



NATASHA AMLANI

ASSOCIATE



Biographies



DOMINIQUE SHELTON LEIPZIG | PARTNER | LOS ANGELES, CA

www.perkinscoie.com/DSheltonLeipzig/

Privacy and cybersecurity attorney Dominique Shelton co-chairs the firm's Ad Tech Privacy & Data Management group. She provides strategic privacy and cyber-preparedness compliance counseling, and defends, counsels and represents companies on privacy, global data security compliance, data breaches and investigations with an eye toward helping clients avoid litigation. Dominique frequently conducts trainings for senior leadership, corporate boards and audit committees regarding risk identification and mitigation in the areas of privacy and cyber.

She leads companies in legal assessments of data security, cyber-preparedness and compliance with such regulations as the California Confidentiality of Medical Information Act (CMIA), HIPAA, the Video Privacy Protection Act (VPPA), the Children's Online Privacy Protection Act (COPPA) and the NIST Cybersecurity Framework.

Dominique has significant experience leading investigations related to data and forensic breaches. She has steered investigations for a range of companies, including national retailers, financial institutions, health and wellness enterprises, media companies and others.

Dominique also advises companies on global privacy and data security, particularly on the EU's General Data Protection Regulation (GDPR). Her background includes advising on European, Asian and South American privacy and security compliance projects for U.S.-based and overseas companies. In addition, she counsels on strategies for related legal compliance and vendor management in cross-border transfers.



SARI RATICAN | SENIOR COUNSEL | LOS ANGELES, CA

www.perkinscoie.com/SRatican/

Sari Ratican's global privacy and data protection practice focuses on providing practical advice tailored to each client's unique needs. Her advice reflects her extensive in-house experience as the first Chief Privacy Officer for Amgen, Inc., the world's largest biotechnology company, where she built and implemented the company's global privacy program across more than 75 countries.

Sari is a Certified Information Privacy Professional (EU and U.S.) and has been actively involved in several global privacy and data protection organizations including the International Association of Privacy Professionals, the International Pharmaceutical Privacy Consortium, and the International Medical Device Privacy Consortium.

In addition to global privacy and data protection matters, Sari has extensive experience in disciplines including healthcare fraud and abuse, compliance and ethics. Prior to specializing in global privacy and data protection, Sari was in private practice as a corporate healthcare lawyer and was also Legislative Counsel for the American Medical Association's Government Relations Department, where she worked with national and state professional medical associations on various legislative matters at the state and federal levels.



NATASHA AMLANI | ASSOCIATE | LOS ANGELES, CA

www.perkinscoie.com/NAmlani/

Natasha Amlani has experience with privacy counseling, litigation and data breach response. She counsels clients on compliance efforts with state, federal and international privacy laws and regulations, including the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). Natasha is also familiar with the Stored Communications Act and helps global technology companies respond to subpoenas and other requests for user information.

Natasha earned her J.D. from UCLA School of Law, where she was a representative on the UCLA Privacy and Data Protection Board, served as executive articles editor for the UCLA Journal of Law & Technology, received Moot Court Honors and volunteered at the law school's reentry legal clinic. Natasha also spent time as an internet public interest opportunities program clerk at the Electronic Privacy Information Center in Washington, D.C.

TABLE OF CONTENTS

	Page
I. ATTORNEY GENERAL MANDATE: UPDATE CATEGORIES OF PERSONAL INFORMATION (§ 1798.185(A)(1)).....	1
A. ISSUE: THE CALIFORNIA CONSUMER PRIVACY ACT (“CCPA”) EXEMPTS PROCESSING SUBJECT TO THE GRAMM-LEACH-BLILEY ACT (“GLBA”), SO CLARIFICATION IS NEEDED THAT THE CCPA DEFINITION OF “PERSONAL INFORMATION” DOES NOT APPLY TO INSTITUTIONS SUBJECT TO THE GLBA	1
1. Current Law: § 1798.145(e).....	1
2. Problem with Current Law:	2
3. [Proposed] Regulatory Solution to Problem	2
II. ATTORNEY GENERAL MANDATE: UPDATE DEFINITION OF UNIQUE IDENTIFIERS (§ 1798.185(A)(2))	3
III. ATTORNEY GENERAL MANDATE: ESTABLISH EXCEPTIONS TO COMPLY WITH STATE OR FEDERAL LAW (§ 1798.185(A)(3)).....	3
A. ISSUE: FINANCIAL INSTITUTIONS’ FRAUD PREVENTION ACTIVITIES ARE COVERED BY THE EXEMPTION OF FINANCIAL ACTIVITIES IN THE CCPA	3
1. Current Law: § 1798.105(d)(2).....	3
2. Problem with Current Law:	3
3. [Proposed] Regulatory Solution to Problem	3
B. ISSUE: CLARIFICATION THAT THE GLBA EXEMPTION COVERS THE CORE ACTIVITIES OF FINANCIAL INSTITUTIONS.....	4
1. Current Law: § 1798.145(e).....	4
2. Problem with Current Law:	4
3. [Proposed] Regulatory Solution to Problem	4
C. ISSUE: THE FAIR CREDIT REPORTING ACT EXEMPTION IN THE CCPA IS DESIGNED TO ENCOMPASS THE ACTIVITIES OF FINANCIAL INSTITUTIONS	4
1. Current Law: § 1798.145(d)	4
2. Problem with Current Law: Financial Institutions Often Provide Information for Identity Verification That Do Not Determine a Decision and Are Not in a Consumer Report but Nevertheless Prevent Fraud	5
3. [Proposed] Regulatory Solution to Problem	5
D. ISSUE: THE GLBA AND HIPAA EXEMPTIONS ARGUABLY MAY NOT FULLY EXEMPT WORKERS’ COMPENSATION AND PROPERTY AND CASUALTY INSURANCE BUSINESSES FROM CCPA REQUIREMENTS ...	5

TABLE OF CONTENTS

(continued)

	Page
1. Current Law: § 1798.145(c).....	5
2. Problem with Current Law: Inconsistent Business Obligations	5
3. [Proposed] Regulatory Solution to Problem	5
E. ISSUE: FRAUD EXEMPTION SHOULD BE CLARIFIED TO CONFIRM IT COVERS ALL OF THE FRAUD PREVENTION LAWS AND REGULATIONS BUSINESSES USE TO KEEP CONSUMER INFORMATION SAFE	6
1. Current Law: § 1798.105(d)(2) and (8); § 1798.140(d)(2); § 1798.145(a)	6
2. Problem with Current Law: Fraud Exemption Does Not Enable Proactive Fraud Prevention or Compliance with State/Federal Regulations	7
3. [Proposed] Regulatory Solution to Problem	7
F. ISSUE: BUSINESSES SHOULD NOT BE REQUIRED TO MAKE DISCLOSURES IN VIOLATION OR CONFLICT WITH FEDERAL LAW	8
1. Current Law: § 1798.145(a)(1) and § 1798.196	8
2. Problem with Current Law: Privacy Protections are Undermined	8
3. [Proposed] Regulatory Solution to Problem	8
G. ISSUE: NARROW DEFINITION OF “PUBLICLY AVAILABLE INFORMATION” DOES NOT PROTECT PRIVACY AND ARGUABLY IMPEDES THE OPERATIONS OF ESTABLISHED BUSINESSES THAT PROVIDE SOCIETAL AND STATE BENEFITS	9
1. Current Law: § 1798.140(o)(1)(K)(2).....	9
2. Problem with Current Law: The Law Blocks Legitimate and Beneficial Business Functions.....	9
3. [Proposed] Regulatory Solution to Problem	10
H. ISSUE: CCPA’S “COMPLIANCE WITH LAWS” EXEMPTION IN § 1798.145(A) SHOULD INCLUDE CALIFORNIA EXECUTIVE ORDERS AND PARTICIPATION IN VOLUNTARY GOVERNMENT PROGRAMS....	10
1. Current Law: § 1798.140(t)(1); § 1798.140(x); § 1798.145(a)	10
2. Problem with Current Law: Risks Disincentivizing Participation in Voluntary Regulatory Programs Beneficial to California and its Residents	11
3. [Proposed] Regulatory Solution to Problem	11
IV. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES RELATING TO CONSUMER OPT-OUT RIGHTS (§ 1798.185(A)(4)).....	11
A. ISSUE: THE CCPA SHOULD BE CLARIFIED TO MAKE CLEAR THAT IT DOES NOT PERMIT CONSUMERS TO OPT OUT OF THE SALE OF DATA FOR FRAUD PREVENTION PURPOSES	11

TABLE OF CONTENTS

(continued)

	Page
1. Current Law: § 1798.120(b), § 1798.140(t)(2)(C), § 1798.140(v), § 1798.140(d); § 1798.105(c); § 1798.105(d)(2).....	11
2. Problem with Current Law: Operational Challenges to Compliance and Cybersecurity Risks	12
3. [Proposed] Regulatory Solution to Problem	12
V. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES: (1) TO FACILITATE AND GOVERN THE SUBMISSION OF A CONSUMER OPT-OUT REQUEST; AND (2) FOR THE DEVELOPMENT AND USE OF A RECOGNIZABLE AND UNIFORM OPT-OUT LOGO OR BUTTON (§ 1798.185(A)(4)(A) AND (C))...	13
A. ISSUE: CREATE A SANCTIONED “DO NOT SELL” LOGO FOR CONSUMERS TO EASILY RECOGNIZE HOW TO OPT OUT OF THE SALE OF THEIR PERSONAL INFORMATION	13
VI. ATTORNEY GENERAL MANDATE: ESTABLISH RULES, PROCEDURES AND EXCEPTIONS RELATING TO NOTICES AND INFORMATION TO CONSUMERS, INCLUDING FINANCIAL INCENTIVE OFFERINGS (§ 1798.185(A)(6)).....	13
VII. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES FOR VERIFYING CONSUMER REQUESTS AND OTHER NECESSARY REGULATIONS TO FURTHER PURPOSES OF THE TITLE (§ 1798.185(A)(7))	13
A. ISSUE: SAFE HARBOR FOR PRIVATE RIGHT OF ACTION NEEDED FOR PERSONAL INFORMATION SECURED USING BLOCKCHAIN	13
1. Current Law: § 1798.150(a)(1)	13
2. Problem with Current Law: Does Not Promote Innovative Security Techniques	13
3. [Proposed] Regulatory Solution to Problem	14
B. ISSUE: REASONABLE SECURITY AND PRIVATE RIGHT OF ACTION ..	14
C. ISSUE: DEFINITION OF “SALE” FOR VALUABLE CONSIDERATION NEEDS TO BE CLARIFIED REGARDING EXCHANGES OF INFORMATION AMONG AFFILIATED COMPANIES	14
1. Current Law: § 1798.140(t)(1).....	14
2. Problem with Current Law:	14
3. [Proposed] Regulatory Solution to Problem	15
D. ISSUE: DEFINITION OF “SALE” NEEDS TO BE CLARIFIED SO IT DOES NOT DISINCENTIVIZE BENEFICIAL BUSINESS PROGRAMS.....	15
1. Current Law: § 1798.140(t)(1).....	16
2. Problem with Current Law:	16
3. [Proposed] Regulatory Solution to Problem	17

I. ATTORNEY GENERAL MANDATE: UPDATE CATEGORIES OF PERSONAL INFORMATION (§ 1798.185(A)(1))

A. ISSUE: THE CALIFORNIA CONSUMER PRIVACY ACT (“CCPA”) EXEMPTS PROCESSING SUBJECT TO THE GRAMM-LEACH-BLILEY ACT (“GLBA”), SO CLARIFICATION IS NEEDED THAT THE CCPA DEFINITION OF “PERSONAL INFORMATION” DOES NOT APPLY TO INSTITUTIONS SUBJECT TO THE GLBA

1. Current Law: § 1798.145(e)

a) The CCPA states that “[t]his title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (“GLBA”) (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code). This subdivision shall not apply to Section 1798.150.”

b) The GLBA regulates financial institutions’ management of “nonpublic personal information,” which is defined as personally identifiable financial information—i.e., information that is provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution.¹ Under the GLBA, personally identifiable financial information includes cookie information that is collected by the financial institution.² However, the GLBA’s definition of “personally identifiable financial information” does not include “aggregate” or “blind data”—i.e., data that “does not contain personal identifiers such as account numbers, names, or addresses.”³ Under the GLBA, the term “consumers” is defined as “an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual.”⁴

c) In contrast, under the CCPA, “personal information” includes, among other things, online identifiers, IP addresses, browsing history, search history, and geolocation. The CCPA even includes inferences drawn from personal information⁵ and “unique *pseudonyms*,”⁶ —

¹ 15 U.S.C. § 6809.

² See 16 C.F.R. § 313.3 (o)(2)(i)(F).

³ *Id.* § 313.3(o)(2)(ii).

⁴ 15 U.S.C. § 6809.

⁵ § 1798.140(o)(1)(K).

⁶ *Id.* § 1798.140(x) (emphasis added).

notwithstanding the CCPA's recognition that "pseudonymization" renders data "no longer attributable to a specific consumer."⁷

2. Problem with Current Law:

- a) Financial institutions are already subject to strict financial privacy laws through the GLBA and, in California, California's Financial Information Privacy Act.⁸
- b) Because the definition of "personal information" in the CCPA is worded differently than the definition of "nonpublic personal information" in the GLBA, clarification is needed to confirm the CCPA's intent to exclude processing covered by the GLBA.
- c) Financial institutions often have websites that enable third-party cookies for a range of purposes, such as security, anti-fraud, analytics, and digital advertising. These activities are pursuant to the financial institutions' overall activities under the GLBA and therefore should be covered by the GLBA exemption in the CCPA.
- d) Having two different regulatory regimes — including two different definitions of "personal information" — apply to the same financial institution may result in confusing and burdensome compliance efforts, as well as conflicting obligations under the various laws. Clarifying that one compliance regime applies to businesses covered by the GLBA ensures that consumer rights are fully protected under the GLBA.

3. [Proposed] Regulatory Solution to Problem

- a) The AG's office will insert clarification language: "Clarification of § 1798.145(e): All consumer personal information collected, processed, sold, or disclosed by a financial institution, or service providers and third parties acting at the behest of financial institutions, is done 'pursuant to' the GLBA."
- b) The AG's office will insert clarification language: "Clarification of § 1798.145(e): All consumer personal information collected, processed, sold, or disclosed by a financial institution shall be governed by and be 'pursuant to' the GLBA and exempt from the CCPA."
- c) The AG's office will insert clarification language: "Clarification of § 1798.140(o): For purposes of this title, § 1798.140(o) shall not apply to financial institutions or their service providers that process personal

⁷ *Id.* § 1798.140(r) (emphasis added).

⁸ Cal. Fin. Code §§ 4050-4060.

information on their behalf pursuant to GLBA and/or California's Financial Information Privacy Act.”

II. ATTORNEY GENERAL MANDATE: UPDATE DEFINITION OF UNIQUE IDENTIFIERS (§ 1798.185(A)(2))

No separate financial industry comments are included here. We defer to the submission made by the California Chamber of Commerce in this regard.

III. ATTORNEY GENERAL MANDATE: ESTABLISH EXCEPTIONS TO COMPLY WITH STATE OR FEDERAL LAW (§ 1798.185(A)(3))

A. ISSUE: FINANCIAL INSTITUTIONS' FRAUD PREVENTION ACTIVITIES ARE COVERED BY THE EXEMPTION OF FINANCIAL ACTIVITIES IN THE CCPA

1. Current Law: § 1798.105(d)(2)

a) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to: ... (2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity...

b) The other rights in the CCPA do not have an express fraud exemption.

2. Problem with Current Law:

a) Consider a financial institution acting both as a service provider processing personal information and as a business offering new products. In both roles, this financial institution uses personal information for fraud prevention, “know your customer,” anti-money laundering, and anti-terrorism purposes that are not subject to deletion requests as related to fraud under § 1798.105(d)(2). It would be antithetical to permit potential criminals to seek rights to know what data is collected for a fraud purpose or seek access to such material.

3. [Proposed] Regulatory Solution to Problem

a) The AG's office will insert clarification language: “Clarification of § 1798.150(d)(2): The Attorney General will not enforce this title on businesses using personal information for fraud prevention, anti-terrorism, “know your customer,” and anti-money laundering purposes pursuant to state, federal, and local laws, rules, or regulations or in compliance with industry best practices.”

B. ISSUE: CLARIFICATION THAT THE GLBA EXEMPTION COVERS THE CORE ACTIVITIES OF FINANCIAL INSTITUTIONS

1. Current Law: § 1798.145(e)

a) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code). This subdivision shall not apply to Section 1798.150.

2. Problem with Current Law:

a) Consider the situation of a “customer” (as defined by the GLBA) who obtains a loan from a financial institution. A loan guarantor guarantees the loan but does not have a direct relationship with the customer. The loan guarantor should still be covered under the GLBA exclusion because it may become a customer of the financial institution if the guarantor ultimately assumes the loan.

3. [Proposed] Regulatory Solution to Problem

a) The AG’s office will insert clarification language: “Clarification of GLBA Exemption under § 1798.145(e): Activities by Loan Guarantors are Part of GLBA Exemption: For purposes of this title, guarantors shall be considered ‘customers’ under the GLBA and activities by guarantors shall be considered within the scope of the GLBA exemption in Cal. Civ. Code § 1798.145(e).”

C. ISSUE: THE FAIR CREDIT REPORTING ACT EXEMPTION IN THE CCPA IS DESIGNED TO ENCOMPASS THE ACTIVITIES OF FINANCIAL INSTITUTIONS

1. Current Law: § 1798.145(d)

a) The CCPA exempts the “sale of personal information to or from a consumer reporting agency if that information is to be reported in or used to generate a consumer report” under the Fair Credit Reporting Act (“FCRA”).⁹

⁹ 15 U.S.C. § 1681 et seq.

2. Problem with Current Law: Financial Institutions Often Provide Information for Identity Verification That Do Not Determine a Decision and Are Not in a Consumer Report but Nevertheless Prevent Fraud

a) Some financial institutions voluntarily “furnish” information for consumer reports and do not “sell” that data. Other financial institutions share information for fraud prevention/FCRA purposes that is never ultimately included in a consumer report or used to make a final determination about employment, insurance, or credit, and therefore does not qualify as a “consumer report.” Nevertheless, this information is used daily to seek a second method of verification through identity verification or account owner verification services to prevent the passing of fraudulent checks, identity fraud, other types of fraud or account abuse, or other undesirable outcomes.

3. [Proposed] Regulatory Solution to Problem

a) Clarification of § 1798.145(d): Safe Harbor for Furnishing Data That May Be Furnished to a Credit Reporting Agency, Used to Verify Identity, and/or Prevent Fraud: The AG will recognize a safe harbor for personal information provided to, from, or held by a consumer reporting agency, or other financial services business engaged in verifying transactions or identity, even if not used to make a determinative decision about issuing credit, employment, insurance, or other final determinations covered by the FCRA.”

D. ISSUE: THE GLBA AND HIPAA EXEMPTIONS ARGUABLY MAY NOT FULLY EXEMPT WORKERS’ COMPENSATION AND PROPERTY AND CASUALTY INSURANCE BUSINESSES FROM CCPA REQUIREMENTS

1. Current Law: § 1798.145(c)

a) GLBA and HIPAA have exemptions for workers’ compensation and property and casualty insurance.

2. Problem with Current Law: Inconsistent Business Obligations

a) The CCPA does not exempt personal information collected by an insurer relating to underwriting a policy or processing a claim for workers’ compensation or property and casualty insurance.

3. [Proposed] Regulatory Solution to Problem

a) The AG’s office will insert clarification language: “Clarification of Workers’ Compensation and Property & Casualty Insurance, § 1798.145(c): The CCPA contemplates business compliance activities associated with exemptions for workers’ compensation and property and

casualty insurance. Data processed ‘pursuant to’ the GLBA will include activities relating to workers’ compensation or property and casualty insurance.”

E. ISSUE: FRAUD EXEMPTION SHOULD BE CLARIFIED TO CONFIRM IT COVERS ALL OF THE FRAUD PREVENTION LAWS AND REGULATIONS BUSINESSES USE TO KEEP CONSUMER INFORMATION SAFE

The fraud exemption does not preclude opt-out or deletion of personal information that is or may be necessary to comply with state, federal, or local laws, rules, and regulations prohibiting fraudulent activity and state, federal, and local anti-corruption, anti-money laundering, export control, and “know your customer” laws, rules, and regulations. Including these in the fraud exemption protects the safety of consumer information and incentivizes businesses to undertake voluntary fraud prevention measures.

1. Current Law: § 1798.105(d)(2) and (8); § 1798.140(d)(2); § 1798.145(a)

a) § 1798.105(d): A business or a service provider shall not be required to comply with a consumer’s request to delete the consumer’s personal information if it is necessary for the business or service provider to maintain the consumer’s personal information in order to: (2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity... (8) Comply with a legal obligation.

b) § 1798.140(d): “Business purpose” means the use of personal information for the business’s or a service provider’s operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are: (2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

c) § 1798.145(a): The obligations imposed on businesses by this title shall not restrict a business’s ability to:

(i) Comply with federal, state, or local laws.

(ii) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(iii) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(iv) Exercise or defend legal claims.

(v) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.

2. Problem with Current Law: Fraud Exemption Does Not Enable Proactive Fraud Prevention or Compliance with State/Federal Regulations

a) Many businesses proactively undertake fraud prevention activities in connection with pre-screening customers for fraudulent activities (e.g., “know your customer” procedures for financial institutions) that are in accordance with regulations promulgated in support of federal, state, or local laws, but are not taken to “comply with federal, state, or local laws,” or “comply with a civil criminal or regulatory inquiry...” (§ 1798.140(a)(1) and (2)). While § 1798.140(a)(1) covers a business’s ability to comply with “laws,” it does not cover a business’s ability to comply with “rules and regulations.”

b) Similarly, while § 1798.140(a)(2) would cover fraud investigations in response to a government inquiry, investigation, or summons; however, many financial institutions affirmatively undertake fraud prevention activities in accordance with best practices that are not in response to a government investigation. Accordingly, the fraud exemption should be clarified to make clear that consumers may not opt-out or delete personal information that is or may be necessary to comply with state, federal, or local rules and regulations prohibiting fraudulent activity and state, federal, and local anti-corruption, anti-money laundering, export control, and “know your customer” rules, and regulations. Data necessary to comply with state, federal, and local laws, rules, and regulations includes firmographic data, linkage data, trade data, and publicly available criminal information related to fraud and illegal activity.

3. [Proposed] Regulatory Solution to Problem

a) The AG’s office will insert clarification language: “Clarification Regarding Fraud Prevention Activities: The CCPA contemplates compliance activities with fraud prevention laws and regulations businesses use to keep consumer information safe. The Attorney General will not enforce this title on businesses when complying with corresponding federal, state, or local laws, rules, and regulations promulgated to prevent, detect, or mitigate fraudulent activity; or when

collecting, using, retaining, selling, authenticating, or disclosing personal information in order to: (i) exercise, defend, or protect against legal claims; (ii) protect against or prevent security incidents; (iii) protect against or investigate, report, or prosecute those responsible for malicious, deceptive, or illegal activity; or (iv) assist another person or government agency to conduct any of the activities specified in this section.”

F. ISSUE: BUSINESSES SHOULD NOT BE REQUIRED TO MAKE DISCLOSURES IN VIOLATION OR CONFLICT WITH FEDERAL LAW

Many practices by financial institutions are subject to federal and/or state regulations or guidance from federal agencies. Federal regulations and guidance issued by federal agencies should be covered by the CCPA exemption for obligations imposed by federal, state, or local laws.

1. Current Law: § 1798.145(a)(1) and § 1798.196

a) § 1798.145(a)(1): The obligations imposed on businesses by this title shall not restrict a business’s ability to (1) comply with federal, state, or local laws.

§ 1798.196: This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.

2. Problem with Current Law: Privacy Protections are Undermined

a) Consider a bank that is following federal agency guidance in connection with its whistleblower program. If an individual made a report to a business subject to federal whistleblowing protections and the alleged wrongdoer is a California resident and wanted to identify who filed the report, the wrongdoer should not be able to misuse the CCPA to make an access request to the business for all personal information about them to try to determine the identity of the individual who made the report. This would be personal information about the alleged wrongdoer because it is linked to their identity and allowing such information to be requested could potentially lead to retaliation and other harms to the whistleblower.

3. [Proposed] Regulatory Solution to Problem

a) The AG’s office will insert clarification language: “Disclosure in Conflict with Federal Law or Regulatory Guidance: The CCPA anticipates that pursuant to paragraph (1) of subdivision (a) of Section 1798.145, a business shall not be required to disclose any personal information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer if such disclosure would violate or conflict with any federal, state, or local regulation or best practice including any guidance issued by a federal, state, or local agency.”

G. ISSUE: NARROW DEFINITION OF “PUBLICLY AVAILABLE INFORMATION” DOES NOT PROTECT PRIVACY AND ARGUABLY IMPEDES THE OPERATIONS OF ESTABLISHED BUSINESSES THAT PROVIDE SOCIETAL AND STATE BENEFITS

Limiting the definition of “personal information” to information from government records “compatible with the purposes for which it is maintained” will restrict many legitimate business purposes, such as assisting the government and consumers with collecting unpaid child support, is a confusing standard difficult to apply in practice and limits use of publicly available data in a way that is, on balance, more harmful than beneficial. Clarifying the definition to confirm that if a government agency does not limit or restrict the use of personal information, businesses may use such information for their business purposes.

1. Current Law: § 1798.140(o)(1)(K)(2)

a) “Personal information” does not include publicly available information defined by the title to mean information that is lawfully made available from federal, state, or local *government records*. “Publicly available” does not mean biometric information collected by a business about a consumer without the consumer’s knowledge. *Information is not “publicly available” if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.* “Publicly available” does not include consumer information that is deidentified or aggregate consumer information. (Emphasis added.)

2. Problem with Current Law: The Law Blocks Legitimate and Beneficial Business Functions

a) As written, “publicly available” information not subject to CCPA obligations is limited only to government records, which is far too narrow for California businesses to continue operating for an appropriate public benefit. For example, for California real estate–related businesses, such as a business that displays the last sale price for houses on its website, the lack of a clear exemption for publicly available information may impede their ability to provide vital services to consumers along with state and local governments, including collection of unpaid child support and collection of state, local, and federal tax liens, as well as coordination with district attorneys and law enforcement authorities, where appropriate. While these may be permissible business purposes under Section 1798.140(a)(4), the AG should clarify that these businesses that operate for a public benefit are not restricted due to the narrow definition of “publicly available.”

3. [Proposed] Regulatory Solution to Problem

a) The AG's office will include clarification as follows: "Publicly Available Information Guidance; § 1798.140(o)(1)(K)(2): 'Publicly available information' is any information that is lawfully made available to the general public from federal, state, or local government records, including disclosures to the general public that are required to be made by federal, state, or local law, rules, or regulations."

b) The AG's office will include clarification as follows: "Government Records Guidance: 'Government records' include any data made available to the public by the government voluntarily or as a matter of law."

c) The AG's office will include clarification as follows: "Use of Public Information Guidance: Under Section 1798.140(o)(2): In the absence of an express use limitation by the government entity holding personal information, data collected subject to Section 1798.140(o)(2) may be used for any legitimate and lawful purpose."

H. ISSUE: CCPA'S "COMPLIANCE WITH LAWS" EXEMPTION IN § 1798.145(a) SHOULD INCLUDE CALIFORNIA EXECUTIVE ORDERS AND PARTICIPATION IN VOLUNTARY GOVERNMENT PROGRAMS

1. Current Law: § 1798.140(t)(1); § 1798.140(x); § 1798.145(a)

a) Section 1798.140(t)(1) states that "sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or *other valuable consideration* (emphasis added).

b) Section 1798.140(x) provides that "unique identifier" or "unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, *unique pseudonym*, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody. (Emphasis added.)

c) Section 1798.145(a) provides that the "obligations imposed on businesses by this title shall not restrict a business's ability to (1) comply with federal, state or local laws."

2. Problem with Current Law: Risks Disincentivizing Participation in Voluntary Regulatory Programs Beneficial to California and its Residents

a) The CCPA should not be misconstrued to limit participation in regulatory credit programs, as it affects electric utilities, automakers, and electric vehicle charging station operators. On January 26, 2018, then-Governor Edmund G. Brown signed Executive Order B-48-18 to boost the use of zero-emission vehicles (“ZEVs”), electric vehicle charging infrastructure, and hydrogen refueling infrastructure in California. This Executive Order B-48-18 requires State entities to build and install 250,000 vehicle charging stations and 200 hydrogen refueling stations by 2025. Additionally, State entities must recommend ways to expand ZEV infrastructure through the Low Carbon Fuel Standard Program. Beginning in 2019, entities may generate credits for renewable energy used for ZEV charging by submitting charging data collected from meters. The California Air Resources Board (“CARB”) requires entities to submit vehicle identification numbers (“VINs”) associated with quarterly charge data to receive credits. However, since VINs are unique identifiers under § 1798.140(x), businesses are concerned that the sharing of VIN-associated data would constitute a sale under § 1798.140(t)(1). But neither CARB nor other participating entities intended to trigger a “sale” of consumers personal information. VIN collection is solely designed to allow auditing and to prevent double-counting of tax credits. If the collection of VIN-associated data is deemed a “sale” under § 1798.140(t)(1), it would disincentivize entities from participating in regulatory credit programs and have adverse consequences for the program’s objectives.

3. [Proposed] Regulatory Solution to Problem

a) The AG’s office shall clarify as follows: “Clarification of § 1798.145(a): Compliance with Laws Exemption: The obligations imposed on businesses by this title shall not restrict a business’s ability to comply with California Executive Orders and participate in voluntary regulatory programs.”

IV. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES RELATING TO CONSUMER OPT-OUT RIGHTS (§ 1798.185(A)(4))

A. ISSUE: THE CCPA SHOULD BE CLARIFIED TO MAKE CLEAR THAT IT DOES NOT PERMIT CONSUMERS TO OPT OUT OF THE SALE OF DATA FOR FRAUD PREVENTION PURPOSES

- 1. Current Law: § 1798.120(b), § 1798.140(t)(2)(C), § 1798.140(v), § 1798.140(d); § 1798.105(c); § 1798.105(d)(2)**

a) Section 1798.120(b) provides that consumers have a right to opt-out of the sale of personal information to third parties: “A business that sells consumers’ personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the “right to opt-out” of the sale of their personal information.”

b) Section 1798.140(t)(2)(C) exempts from the definition of “sale” sharing personal information with a “service provider” for a “business purpose,” as long as: (i) that sharing is disclosed in the business’s terms; and (ii) the personal information is not otherwise collected, sold, or used except to accomplish the business purpose.

c) Section 1798.140(v) additionally requires that the service provider be contractually prohibited from retaining, using, or disclosing the information for any other purpose.

d) Section 1798.140(d)(5) defines “business purpose” to include “performing services on behalf of the business.”

e) Section 1798.140(d)(7) states that a business purpose is to “undertake “activities to verify or maintain the quality or safety of a service or device.”

f) Section 1798.105(c) requires that a business that receives a verifiable deletion request must delete the consumer’s personal information from its records and direct any service providers to delete the consumer’s personal information from their records.

2. Problem with Current Law: Operational Challenges to Compliance and Cybersecurity Risks

a) Financial institutions are not obligated to give consumers notice about how their data may be “sold” to prevent/mitigate fraud, thereby publicly undermining security. The AG should therefore clarify that sharing information to prevent or mitigate fraud is a legitimate business purpose under § 1798.140(d)(7) for which the right to opt-out of sale does not apply.

3. [Proposed] Regulatory Solution to Problem

a) The AG’s office shall clarify as follows: “Clarification of §1798.145 (a) (1)-(3) for Businesses Using Personal Information for Fraud Prevention and Related Purposes: The Attorney General will not enforce this title upon businesses using personal information for fraud prevention, anti-terrorism, “know your customer,” and anti–money laundering purposes pursuant to state, federal, and local laws, rules, or regulations or in compliance with industry best practices.”

V. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES: (1) TO FACILITATE AND GOVERN THE SUBMISSION OF A CONSUMER OPT-OUT REQUEST; AND (2) FOR THE DEVELOPMENT AND USE OF A RECOGNIZABLE AND UNIFORM OPT-OUT LOGO OR BUTTON (§ 1798.185(A)(4)(A) AND (C))

A. ISSUE: CREATE A SANCTIONED “DO NOT SELL” LOGO FOR CONSUMERS TO EASILY RECOGNIZE HOW TO OPT OUT OF THE SALE OF THEIR PERSONAL INFORMATION

This report incorporates the comments submitted to the California Chamber of Commerce.

VI. ATTORNEY GENERAL MANDATE: ESTABLISH RULES, PROCEDURES AND EXCEPTIONS RELATING TO NOTICES AND INFORMATION TO CONSUMERS, INCLUDING FINANCIAL INCENTIVE OFFERINGS (§ 1798.185(A)(6))

This report incorporates the comments submitted to the California Chamber of Commerce.

VII. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES FOR VERIFYING CONSUMER REQUESTS AND OTHER NECESSARY REGULATIONS TO FURTHER PURPOSES OF THE TITLE (§ 1798.185(A)(7))

This report incorporates the comments submitted to the California Chamber of Commerce. In addition, the following remaining comments impacting the financial industry are included below.

A. ISSUE: SAFE HARBOR FOR PRIVATE RIGHT OF ACTION NEEDED FOR PERSONAL INFORMATION SECURED USING BLOCKCHAIN

1. Current Law: § 1798.150(a)(1)

a) Any consumer whose non-encrypted or non-redacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following...[.]

2. Problem with Current Law: Does Not Promote Innovative Security Techniques

a) Based on cryptographic technology, blockchain is a secure form of storing information. Businesses may be averse to using this method if, in the event the chain is compromised, a business will not be deemed to have used reasonable security.

b) In public comments on February 20, 2019, Alistair Mactaggart, the founder of the initiative that pre-dated the CCPA, testified that a carve-out from liability exists under the law for businesses that use encryption. Blockchain uses encryption technology.¹⁰

3. [Proposed] Regulatory Solution to Problem

a) The AG's office will institute a safe harbor for businesses as follows: "Safe Harbor under § 1798.150: The CCPA contemplates business compliance activities associated with personal information secured using blockchain. When a business uses blockchain to protect personal information, a business shall be considered have implemented reasonable security measures in the event the blockchain is compromised."

B. ISSUE: REASONABLE SECURITY AND PRIVATE RIGHT OF ACTION

This report incorporates by reference the comments made by the California Chamber of Commerce regarding reasonable security safe harbors.

C. ISSUE: DEFINITION OF "SALE" FOR VALUABLE CONSIDERATION NEEDS TO BE CLARIFIED REGARDING EXCHANGES OF INFORMATION AMONG AFFILIATED COMPANIES

1. Current Law: § 1798.140(t)(1)

a) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or *other valuable consideration* (emphasis added).

2. Problem with Current Law:

a) Consider the activities of financial institutions that obtain or share information for a variety of purposes for which no monetary payments are made, including with affiliated companies (e.g., emailing lists, understanding their customer base to tailor product offerings, and expanding on existing relationships). This can also lead to the development of new products, services or improvements to existing products. In addition, many companies that solicit new credit card accounts and insurance policies use pre-screening to identify potential customers for the products they offer. Pre-screened offers — sometimes called "pre-approved" offers — are based on information in a consumer's credit report that indicates the consumer meets criteria set by the offeror.

¹⁰ *Understanding the Rights, Protections, and Obligations Established by the California Consumer Privacy Act of 2018: Where should California go from here?* (Feb. 20, 2019).

Usually pre-screened solicitations come via postal mail, but they also may be provided in a phone call or in an email. There are already opportunities for consumers to opt-out of such offers. Business growth and innovation within California would be significantly stifled.

b) Consider also the use of common information systems by affiliated companies, each of which uses and gives their employees access to common information systems, databases, hard-copy storage facilities, etc. From a consumer's perspective, affiliated companies that share common branding are treated as one entity — consumers expect seamless interactions with affiliated companies. These affiliated companies may share data for customer service uses, such as to process an address change sent to one of them or enable a consolidated statement to be sent to the customer. This generates consumer goodwill (consumers wouldn't need to notify seven affiliates under one business as an address change, for example) and creates an opportunity to deepen the consumer relationship. Businesses are concerned that this goodwill would be interpreted as other valuable consideration, and thus a "sale" between affiliates.

c) Also, treating the sharing of information by affiliates as a sale, does not comport with consumer expectations and disincentivizes business activity in California. For example, if a consumer invests in five mutual funds under one common branding, consumers expect to receive one financial statement that incorporates the financial activity of all mutual funds, not five different financial statements from each affiliate. Thus, consumers expect this sharing and may also be confused by the presence of a "Do Not Sell" button on the businesses' home page.

3. [Proposed] Regulatory Solution to Problem

a) The AG's office shall insert clarification language as follows:
"Clarification of Definition of Sell in § 1798.140(t) to Exclude Exchanges of Personal Information by Financial Institutions that are Necessary for Business Operations: The CCPA contemplates business compliance activities associated with exchanges or transfers of personal information. When these are exchanged by financial institutions for non-monetary consideration for their business operations, they are not 'sales' for purposes of this title."

b) "Clarification of Definition of "Sell" in § 1798.140(t):
"Clarification of Definition of "Sell" in § 1798.140(t) to Exclude Sharing of Information Systems by Financial Institutions' Affiliated Companies: The CCPA contemplates that sharing of common information systems by affiliate companies is not considered 'sales' for purposes of this title."

D. ISSUE: DEFINITION OF "SALE" NEEDS TO BE CLARIFIED SO IT DOES NOT DISINCENTIVIZE BENEFICIAL BUSINESS PROGRAMS

1. Current Law: § 1798.140(t)(1)

- a) “Sell,” “selling,” “sale,” or “sold,” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.
- b) For purposes of this title, a business does not sell personal information when:
 - (i) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer’s intent to interact with a third party.
 - (ii) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer’s personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer’s personal information.
 - a. The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met...[.]
 - b. The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.
 - c. The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

2. Problem with Current Law:

- a) Consider the activities of a financial institution that regularly sells loan portfolios or other information to benefit their customers. Loan portfolios are comprised of individual transactions protected by the GLBA exemption. Therefore, the sale of loan portfolios should also be covered by the CCPA’s GLBA exemption. If not, customers may be permitted to block sales of loan portfolios, a regular and legitimate business purpose of

many financial institutions, thereby disrupting the business's regular and normal operations.

b) Consider a business that has a wellness program encouraging employees to participate in activities focused on their well-being. By participating, employees would accrue points, and in response, a business would qualify for reduced insurance premiums. Employee participation is voluntary, and often happens through collection of personal information via a third-party app, with which the business may not have formal agreements. The purpose of wellness programs is to encourage employees to participate in them to develop and maintain good habits. If this is considered a sale, and not simply the sharing with a service provider, it will disincentivize companies from having these types of programs because they will need to place adverse language on internal or external privacy policies (i.e., "Do Not Sell"). Thus, the CCPA's business obligations may disincentivize businesses from implementing such programs to benefit Californian's health or may cause businesses to pass on the additional insurance premium cost to those employees not enrolling in the wellness program, arguably amounting to discrimination against non-participating employees.

c) Many financial institutions receiving personal information as service providers often use such personal information across entities to improve services or products. In addition, financial institutions that are service providers may also create fraud prevention tools by combining information received with information available across the internet to make a predictive algorithm. The creation of the fraud prevention algorithms could be a new use of the received information that was not "necessary to perform the business purpose," one of the requirements for which sharing with a service provider is not considered a "sale" under § 1798.140(t)(2)(C)(ii). In addition, if a business develops algorithms using consumer personal information consistent with its role as a service provider, thereby not violating § 1798.140(t)(2)(C)(ii), but then licenses out the algorithm as a predictive indicator of fraud, for example, licensing this algorithm could be considered a sale of personal information. If either of these scenarios were considered a "sale" of data, California consumers could opt-out of this "sale" requiring businesses to delete their data, thereby harming the business's fraud prevention techniques to identify fraud patterns related to California consumers. It would also disincentivize businesses from creating practical, innovative, and consumer protective products.

3. [Proposed] Regulatory Solution to Problem

a) The AG's office shall insert clarification language as follows: "Clarification of Definition of Opt-Out Rights under § 1798.120": A

financial institution's sale of loans or other financial products will not be considered "sale" subject to "opt-out" rights by consumers.

b) The AG's office shall insert clarification language as follows:
"Clarification of Definition of Sell in § 1798.140(t): Sharing personal information with wellness programs shall be considered sharing with service providers and exempted from the definition of 'sell.'"

c) The AG's office shall insert clarification language as follows:
"Clarification of Definition of Sell in § 1798.140(t)(2)(C): The restriction on service providers' further use of information in this section shall not preclude a service provider's use of predictive algorithms for purposes such as fraud prevention or analytics. Furthermore, these uses shall not be considered "selling" for purposes of this title."

d) The AG's office will insert clarification language: "Clarification of GLBA Exemption under § 1798.145(e): Sales of Loan Portfolios Are Subject to the GLBA Exemption: For purposes of this title, the sale of loan portfolios by financial companies shall be considered to be within the scope of the GLBA exemption in § 1798.145(e)."



Perkins Coie Comments to the California Attorney General's Office for CCPA Rulemaking: General Industry

March 8, 2019

DOMINIQUE SHELTON LEIPZIG

PARTNER



SARI RATICAN

SENIOR COUNSEL



NATASHA AMLANI

ASSOCIATE



Executive Summary

Perkins Coie submits this Report to the California Attorney General's ("AG") office as part of the AG's rulemaking process for the California Consumer Privacy Act ("CCPA"). The observations in this Report are designed primarily to clarify existing law under the CCPA. This Report also incorporates by reference the broader set of comments submitted by the California Chamber of Commerce.

This Report incorporates comments and requests for clarification from businesses across various industries including but not limited to the health/wellness, retail, and semi-conductor industries. Where comments and clarification requests were shared by more than three different industries, they are marked as "General Industry;" however, where such requests were made by fewer than three industries, the specific industry verticals are listed.

Each comment is presented separately in four parts: (1) the header which synthesizes the issue or concern with the current law, (2) the text and citation to the relevant CCPA section, (3) an illustrative use case to demonstrate the issue or concern that requires AG clarification, and (4) proposed regulatory language to solve or mitigate the issue or concern raised.

We have organized comments into the Section 1798.185 AG rulemaking mandates and address the following issues:

- **Establish exceptions to comply with state or federal law:** Requesting clarification to address: (1) executive orders and participation in voluntary government programs in the § 1798.145(a) "compliance with laws" exemption; and (2) entities required to comply with HIPAA and CMIA are not subject to CCPA.
- **Establish rules and procedures related to consumer opt-out rights:** Requesting clarification to address: opt-out requests related to big data and artificial intelligence products that do not identify individual consumers.
- **Establish rules, procedures, and exceptions:** Requesting clarification to address: (1) the \$25 million "business" definition threshold; (2) recordkeeping associated with responding to verifiable consumer requests; (3) business responses to verifiable consumer requests; and (4) deletion of personal information in scientific, historical, or statistical research.

Contacts:

DOMINIQUE SHELTON LEIPZIG

PARTNER



SARI RATCAN

SENIOR COUNSEL



NATASHA AMLANI

ASSOCIATE



Biographies



DOMINIQUE SHELTON LEIPZIG | PARTNER | LOS ANGELES, CA

www.perkinscoie.com/DSheltonLeipzig/

Privacy and cybersecurity attorney Dominique Shelton co-chairs the firm's Ad Tech Privacy & Data Management group. She provides strategic privacy and cyber-preparedness compliance counseling, and defends, counsels and represents companies on privacy, global data security compliance, data breaches and investigations with an eye towards helping clients avoid litigation. Dominique frequently conducts trainings for senior leadership, corporate boards and audit committees regarding risk identification and mitigation in the areas of privacy and cyber.

She leads companies in legal assessments of data security, cyber preparedness and compliance with such regulations as the California Confidentiality of Medical Information Act (CMIA), HIPAA, the Video Privacy Protection Act (VPPA), the Children's Online Privacy Protection Act (COPPA) and the NIST Cybersecurity Framework.

Dominique has significant experience leading investigations related to data and forensic breaches. She has steered investigations for a range of companies, including for national retailers, financial institutions, health and wellness enterprises, media companies and others.

Dominique also advises companies on global privacy and data security, particularly on EU General Data Protection Regulation (GDPR). Her background includes advising on European, Asian and South American privacy and security compliance projects for U.S.-based and overseas companies. In addition, she counsels on strategies for related legal compliance and vendor management in cross-border transfers.



SARI RATICAN | SENIOR COUNSEL | LOS ANGELES, CA

www.perkinscoie.com/SRatican/

Sari Ratican's global privacy and data protection practice focuses on providing practical advice tailored to each client's unique needs. Her advice reflects her extensive in-house experience as the first Chief Privacy Officer for Amgen, Inc., the world's largest biotechnology company, where she built and implemented the company's global privacy program across more than 75 countries.

Sari is a Certified Information Privacy Professional (EU and US) and has been actively involved in several global privacy and data protection organizations including the International Association of Privacy Professionals, the International Pharmaceutical Privacy Consortium, and the International Medical Device Privacy Consortium.

In addition to global privacy and data protection matters, Sari has extensive experience in disciplines including healthcare fraud and abuse, compliance and ethics. Prior to specializing in global privacy and data protection, Sari was in private practice as a corporate healthcare lawyer and was also Legislative Counsel for the American Medical Association's Government Relations Department where she worked with national and state professional medical associations on various legislative matters both at the state and federal level.



NATASHA AMLANI | ASSOCIATE | LOS ANGELES, CA

www.perkinscoie.com/NAmlani/

Natasha Amlani has experience with privacy counseling, litigation and data breach response. She counsels clients on compliance efforts with state, federal and international privacy laws and regulations, including the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). Natasha is also familiar with the Stored Communications Act and helps global technology companies respond to subpoenas and other requests for user information.

Natasha earned her J.D. from UCLA School of Law, where she was a representative on the UCLA Privacy and Data Protection Board, served as executive articles editor for the UCLA Journal of Law & Technology, received Moot Court Honors and volunteered at the law school's reentry legal clinic. Natasha also spent time as an internet public interest opportunities program clerk at the Electronic Privacy Information Center in Washington, D.C.

TABLE OF CONTENTS

	Page
I. ATTORNEY GENERAL MANDATE: ESTABLISH EXCEPTIONS TO COMPLY WITH STATE OR FEDERAL LAW (§ 1798.185(A)(3)).....	1
A. GENERAL INDUSTRY ISSUE: CCPA’S “COMPLIANCE WITH LAWS” EXEMPTION IN § 1798.145(A) SHOULD EXPLICITLY INCLUDE CALIFORNIA EXECUTIVE ORDERS AND PARTICIPATION IN VOLUNTARY GOVERNMENT PROGRAMS	1
1. Current Law: § 1798.140(t)(1); § 1798.140(x); § 1798.145(a)	1
2. Problem with Current Law: Disincentivizes Participation in Voluntary Regulatory Programs Beneficial to California and its Residents	1
3. [Proposed] Regulatory Solution to Problem	2
B. HEALTH INDUSTRY ISSUE: HIPAA HAS AN ESTABLISHED DEIDENTIFICATION STANDARD THAT MEETS REQUIREMENTS UNDER THE CCPA.....	2
1. Current Law: § 1798.140(h); § 1798.145(c)(1).....	2
2. Problem with Current Law: Businesses That Have Deidentified Data Pursuant to HIPAA Standards Should Be Exempt From the CCPA	3
3. [Proposed] Regulatory Solution to Problem	4
II. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES RELATING TO CONSUMER OPT-OUT RIGHTS (§ 1798.185(A)(4))	4
A. ARTIFICIAL INTELLIGENCE (“AI”) INDUSTRY ISSUE: CONSUMER OPT-OUT RIGHTS APPLIED TO BIG DATA SETS AND AI HARMS BUSINESSES AND CONSUMERS.....	4
1. Current Law: § 1798.140(t)(1); § 1798.120(a).....	4
2. Problem with Current Law: May Drive Innovative Businesses Out of California	5
3. [Proposed] Regulatory Solution to Problem	5
III. ATTORNEY GENERAL MANDATE: ESTABLISH RULES, PROCEDURES AND EXCEPTIONS RELATING TO NOTICES AND INFORMATION TO	

TABLE OF CONTENTS

(continued)

	Page
CONSUMERS, INCLUDING FINANCIAL INCENTIVE OFFERINGS (§ 1798.185(A)(6))	5
A. RETAIL INDUSTRY ISSUE: BUSINESSES THAT CREATE AD-SUPPORTED PRODUCTS SHOULD NOT BE REQUIRED TO CREATE A FREE EXPERIENCE IF CONSUMERS DO NOT WANT TO PAY FOR THEIR PRODUCT	5
1. Current Law: § 1798.125(b)(4)	5
2. Problem with Current Law: Overly Burdensome on Businesses and Suppresses Business Innovation	6
3. [Proposed] Regulatory Solution to Problem	6
IV. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES FOR VERIFYING CONSUMER REQUESTS AND OTHER NECESSARY REGULATIONS TO FURTHER PURPOSES OF THE TITLE (§ 1798.185(A)(7))	6
A. GENERAL INDUSTRY ISSUE: CONFUSION EXISTS ABOUT WHETHER THE “BUSINESS” DEFINITION’S \$25M ANNUAL GROSS REVENUE TRIGGER RELATES TO CALIFORNIA-DERIVED REVENUE OR REVENUE DERIVED FROM ALL JURISDICTIONS	6
1. Current Law: § 1798.140(c)(1)(A)	6
2. Problem with Current Law: One of the Three Inclusion Criteria for “Businesses” Covered by the CCPA Includes an Unanswered Question	6
3. [Proposed] Regulatory Solution to Problem	7
B. GENERAL INDUSTRY ISSUE: BUSINESS CHALLENGES WITH RECORDKEEPING RESPONSES TO VERIFIABLE CONSUMER REQUESTS	7
1. Current Law: § 1798.140(y)	7
2. Problem with Current Law: Overly Burdensome on Businesses	7
3. [Proposed] Regulatory Solution to Problem	8
C. GENERAL INDUSTRY ISSUE: A BUSINESS’ RESPONSE TO A VERIFIABLE CONSUMER REQUEST MAY NEGATIVELY IMPACT	

TABLE OF CONTENTS

(continued)

	Page
ANOTHER CONSUMER, THEREBY REDUCING PRIVACY PROTECTIONS AND INCREASING CONSUMER RISK	8
1. Current Law: § 1798.140(y)	8
2. Problem with Current Law: Consumer Safety at Risk.....	8
3. [Proposed] Regulatory Solution to Problem	8
D. HEALTH INDUSTRY ISSUE: THE CCPA EXEMPTION FROM DELETION FOR SCIENTIFIC, HISTORICAL, OR STATISTICAL RESEARCH SHOULD COVER SITUATIONS WHERE THE DATA FROM THE CLINICAL TRIAL IS USED TO DEVELOP NEW LIFE-SAVING PRODUCTS.....	9
1. Current Law: § 1798.140(s).....	9
2. Problem with Current Law: Limitation on Commercial Use Will Stifle Life-Saving Research and New Product Development	10
3. [Proposed] Regulatory Solution to Problem	10

I. ATTORNEY GENERAL MANDATE: ESTABLISH EXCEPTIONS TO COMPLY WITH STATE OR FEDERAL LAW (§ 1798.185(A)(3))

A. GENERAL INDUSTRY ISSUE: CCPA’S “COMPLIANCE WITH LAWS” EXEMPTION IN § 1798.145(A) SHOULD EXPLICITLY INCLUDE CALIFORNIA EXECUTIVE ORDERS AND PARTICIPATION IN VOLUNTARY GOVERNMENT PROGRAMS

1. Current Law: § 1798.140(t)(1); § 1798.140(x); § 1798.145(a)

a) Section 1798.140(t)(1) states that “sell,” “selling,” “sale,” or “sold,” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or *other valuable consideration*. (Emphasis added).

b) Section 1798.140(x) provides that “unique identifier” or “unique personal identifier” means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, *unique pseudonym*, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, “family” means a custodial parent or guardian and any minor children over which the parent or guardian has custody. (Emphasis added).

c) Section 1798.145(a) provides that the “obligations imposed on businesses by this title shall not restrict a business’s ability to (1) comply with federal, state or local laws.”

2. Problem with Current Law: Disincentivizes Participation in Voluntary Regulatory Programs Beneficial to California and its Residents

a) The CCPA should not be construed to limit participation in regulatory credit programs as it affects electric utilities, automakers and electric vehicle charging station operators. In January 26, 2018, Governor Edmund G. Brown signed Executive Order B-48-18 to boost the use of zero-emission vehicles (“ZEVs”), electric vehicle charging infrastructure, and hydrogen refueling infrastructure in California. This Executive Order B-48-18 requires State entities to build and install 250,000 vehicle charging stations and 200 hydrogen refueling stations by 2025. Additionally, State entities must recommend ways to expand ZEV infrastructure through the Low Carbon Fuel Standard Program. Beginning

in 2019, entities may generate credits for renewable energy used for ZEV charging by submitting charging data collected from meters. The California Air Resources Board (“CARB”) requires entities to submit vehicle identification numbers (“VINs”) associated with quarterly charge data to receive credits. Notwithstanding that VINs are unique identifiers under § 1798.140(x), businesses’ sharing of VIN-associated data should not constitute a sale under § 1798.140(t)(1). Neither CARB nor other participating entities intended to trigger a “sale” of consumers personal information. VIN collection is solely designed to allow auditing and to prevent double-counting. If the collection of VIN-associated data is deemed a “sale” under § 1798.140(t)(1), it would disincentivize businesses from participating in regulatory credit programs and have adverse consequences for the promoting renewable energy in California and the government program’s objectives.

3. [Proposed] Regulatory Solution to Problem

a) The AG’s office shall clarify as follows: “Clarification of § 1798.145(a): Compliance with Laws Exemption: The CCPA anticipates that the obligations imposed on businesses by this title shall not restrict a business’s ability to comply with California Executive Orders and participate in regulatory programs.”

B. HEALTH INDUSTRY ISSUE: HIPAA HAS AN ESTABLISHED DEIDENTIFICATION STANDARD THAT MEETS REQUIREMENTS UNDER THE CCPA

1. Current Law: § 1798.140(h); § 1798.145(c)(1)

a) § 1798.140(h) “Deidentified” means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information: (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain. (2) Has implemented business processes that specifically prohibit reidentification of the information. (3) Has implemented business processes to prevent inadvertent release of deidentified information. (4) Makes no attempt to reidentify the information.

b) HIPAA has an established process for deidentification that includes the potential of having an expert conclude that data is deidentified.¹

¹ Office for Civil Rights, U.S. Dept. of Health and Human Services., *Guidance Regarding Methods for Deidentification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy*

- c) 1798.145(c)(1) This title shall not apply to any of the following:
- (1) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).
 - (2) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section

2. Problem with Current Law: Businesses That Have Deidentified Data Pursuant to HIPAA Standards Should Be Exempt From the CCPA

- a) The health industry is one of the most heavily regulated industries in the United States. It is not protective of privacy for healthcare providers that have already deidentified “protected health information” (“PHI”) under HIPAA or “medical information” (“MI”) under the CMIA to reassess whether data already properly deidentified under those long-standing statutes would be considered deidentified under the CCPA. As the CCPA is less proscriptive than HIPAA and CMIA, there is no need for healthcare providers to undertake the burdensome analysis for each data set used, when they have already met the stringent standards for deidentification set forth in HIPAA.
- b) As currently drafted, the CCPA exemption covers PHI and MI; however, if such information is deidentified pursuant to HIPAA/CMIA requirements, it no longer falls within the definition of PHI or MI (under

Rule, available at https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (accessed on March 8, 2019).

HIPAA or CMIA respectively) but should still be exempted under the CCPA.

c) The definition of PHI and MI under HIPAA/CMIA should be deemed to cover personal information under the CCPA such that healthcare providers are exempt in all respects from CCPA, whether or not the definitions of personal information under the CCPA, PHI and MI under HIPAA and the CMIA are worded differently.

3. [Proposed] Regulatory Solution to Problem

a) The AG's office will institute a safe harbor as follows: "Safe Harbor for DeIdentified Information: § 1798.140(h) and § 1798.145(c)(1): Consistent with Civil Code Sections 1798.140(h) and 1798.145(c)(1), an expert statistician's opinion that satisfies the HIPAA Privacy Rule's expert deidentification method (45 C.F.R. §164.514) is sufficient for information to be considered "deidentified" under this title."

b) The AG's office will insert clarification language: "Clarification of Exemption under § 1798.140(h) and § 1798.145(c)(1): For purposes of this title the exemption anticipates that data-related activities of a provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) are exempt from the CCPA."

II. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES RELATING TO CONSUMER OPT-OUT RIGHTS (§ 1798.185(A)(4))

A. ARTIFICIAL INTELLIGENCE ("AI") INDUSTRY ISSUE: CONSUMER OPT-OUT RIGHTS APPLIED TO BIG DATA SETS AND AI HARMS BUSINESSES AND CONSUMERS

1. Current Law: § 1798.140(t)(1); § 1798.120(a)

a) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.

b) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to

sell the consumer's personal information. This right may be referred to as the right to opt-out.

2. Problem with Current Law: May Drive Innovative Businesses Out of California

a) If information is used for models to create algorithms, the algorithm is deidentified and should not be considered personal information.

b) Considering algorithms "personal information" under the CCPA is inconsistent with the statute. Not only will the efficacy of algorithms be impacted, but removing consumer information from big data sets, including those used to create algorithms, will be nearly impossible to do, and the efforts concerning same would be costly and burdensome to implement with no true privacy risk at issue. Many businesses use AI in order to automate functions and lower costs. If removing consumer information in response to opt-out requests were to be read into the CCPA, businesses may find it cost-prohibitive to operate their algorithms in California and may choose to do business elsewhere. As a result, business innovation, and in turn, California consumers, will be harmed.

3. [Proposed] Regulatory Solution to Problem

a) The AG's office shall insert clarification language as follows:
"Clarification of § 1798.120(a): If personal information is used to create a big data or artificial intelligence product and the end product does not identify individual consumers, the data is deidentified, aggregate, and not subject to this title."

III. ATTORNEY GENERAL MANDATE: ESTABLISH RULES, PROCEDURES AND EXCEPTIONS RELATING TO NOTICES AND INFORMATION TO CONSUMERS, INCLUDING FINANCIAL INCENTIVE OFFERINGS (§ 1798.185(A)(6))

A. RETAIL INDUSTRY ISSUE: BUSINESSES THAT CREATE AD-SUPPORTED PRODUCTS SHOULD NOT BE REQUIRED TO CREATE A FREE EXPERIENCE IF CONSUMERS DO NOT WANT TO PAY FOR THEIR PRODUCT

1. Current Law: § 1798.125(b)(4)

a) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

2. Problem with Current Law: Overly Burdensome on Businesses and Suppresses Business Innovation

a) If a business only creates an ad-supported service, it should not be forced to offer a second service free from advertisements just because a consumer opts out of the sale of their data. If the CCPA were to require this, it would be unduly burdensome.

3. [Proposed] Regulatory Solution to Problem

a) The AG's office shall insert clarification language as follows: "Clarification of Financial Incentive Practices; § 1798.125(b)(4): For purposes of this title, creating only an ad-supported product or service and not offering a free service shall not be considered a financial incentive practice that is unjust, unreasonable, coercive, or usurious in nature."

IV. ATTORNEY GENERAL MANDATE: ESTABLISH RULES AND PROCEDURES FOR VERIFYING CONSUMER REQUESTS AND OTHER NECESSARY REGULATIONS TO FURTHER PURPOSES OF THE TITLE (§ 1798.185(A)(7))

A. GENERAL INDUSTRY ISSUE: CONFUSION EXISTS ABOUT WHETHER THE "BUSINESS" DEFINITION'S \$25M ANNUAL GROSS REVENUE TRIGGER RELATES TO CALIFORNIA-DERIVED REVENUE OR REVENUE DERIVED FROM ALL JURISDICTIONS

1. Current Law: § 1798.140(c)(1)(A)

a) § 1798.140(c)(1)(A): "Business" means (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds: (A) Has annual gross revenues in excess of twenty-five million dollars (\$25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185....[.]

2. Problem with Current Law: One of the Three Inclusion Criteria for "Businesses" Covered by the CCPA Includes an Unanswered Question

a) Consider a large, matrixed organization that makes \$25,000,000 outside of California and has only minimal revenue of \$5,000 in California. Since the definition of "business" doesn't specify if the revenue threshold relates only to California-derived revenue, the AG

should clarify that it will focus on companies that generate threshold revenues in California as it relates to the definition of “business.”

3. [Proposed] Regulatory Solution to Problem

a) The AG’s office shall insert clarification language as follows: “Clarification of ‘Business’ Definition; § 1798.140(c)(1)(A): For purposes of this title, the annual gross revenue threshold relates to revenues derived from within California.”

B. GENERAL INDUSTRY ISSUE: BUSINESS CHALLENGES WITH RECORDKEEPING RESPONSES TO VERIFIABLE CONSUMER REQUESTS

1. Current Law: § 1798.140(y)

a) “Verifiable consumer request” means a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer’s behalf.

2. Problem with Current Law: Overly Burdensome on Businesses

a) Consider a scenario in which businesses comply with a consumer request, or do not comply because they assert defenses, and a consumer files a complaint with the AG’s office asserting that a business has not fulfilled its obligation in response to the consumer asserting his/her right. This scenario will subject businesses to burdensome enforcement and investigative activities. To keep unnecessary costs and business impact to a minimum, businesses should be able to satisfy an AG inquiry by providing contemporaneous record(s) of its interactions with requesting consumers to demonstrate compliance with the CCPA (i.e., that it did respond or that it received the request but asserted a defense under the CCPA).

b) Consider also the challenge a business would have proving that it deleted consumer information after receiving a verifiable request if it could not rely on its contemporaneous records for compliance. If the

business deleted the information, it cannot produce the information. Thus, aside from producing its contemporaneous records that it deleted the information, the business may have no other reasonable way of demonstrating compliance.

3. [Proposed] Regulatory Solution to Problem

a) The AG's office shall insert clarification language as follows: "Clarification of 'Verifiable Request' Definition; § 1798.140(y): If a business maintains a contemporaneous record of its interactions with consumers confirming that it has responded or taken appropriate action in response to a consumer or third-party rights request, the AG shall not take enforcement action against the business for failing to respond to a consumer request."

C. GENERAL INDUSTRY ISSUE: A BUSINESS' RESPONSE TO A VERIFIABLE CONSUMER REQUEST MAY NEGATIVELY IMPACT ANOTHER CONSUMER, THEREBY REDUCING PRIVACY PROTECTIONS AND INCREASING CONSUMER RISK

1. Current Law: § 1798.140(y)

a) Incorporate by reference the definition of "verifiable request" from Section IV. B. 1., above.

2. Problem with Current Law: Consumer Safety at Risk

a) Consider an abusive relationship: A consumer's safety or confidentiality may be placed at risk if his/her personal information is revealed as part of another consumer's access request. For example, if a consumer alleges abuse, harassment, or other bad behavior against another consumer, the alleging consumer's personal information (e.g., name, contact information, etc.) may be exposed to the alleged wrongdoer by a business seeking to be in compliance with the CCPA. Scenarios for other compromises to consumer safety and protection are limitless.

3. [Proposed] Regulatory Solution to Problem

a) The AG's office shall provide guidance for businesses as follows: "Guidance for Types of Data Not Returned in Response to a Verifiable Consumer Request; § 1798.140(y): A business shall not disclose: data under attorney-client privilege; data containing material non-public information other than personal information; or data indicating any type of investigation is in progress."

D. HEALTH INDUSTRY ISSUE: THE CCPA EXEMPTION FROM DELETION FOR SCIENTIFIC, HISTORICAL, OR STATISTICAL RESEARCH SHOULD COVER SITUATIONS WHERE THE DATA FROM THE CLINICAL TRIAL IS USED TO DEVELOP NEW LIFE-SAVING PRODUCTS

1. Current Law: § 1798.140(s)

a) “Research” means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer’s interactions with a business’ service or device for other purposes shall be:

- (1) Compatible with the business purpose for which the personal information was collected.
- (2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.
- (3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
- (4) Subject to business processes that specifically prohibit reidentification of the information.
- (5) Made subject to business processes to prevent inadvertent release of deidentified information.
- (6) Protected from any reidentification attempts.
- (7) Used solely for research purposes that are compatible with the context in which the personal information was collected.
- (8) Not be used for any commercial purpose.
- (9) Subjected by the business conducting the research to additional security controls limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

2. Problem with Current Law: Limitation on Commercial Use Will Stifle Life-Saving Research and New Product Development

a) If businesses such as pharmaceutical or biotechnology companies are obligated upon verifiable consumer request to delete consumers' personal information from commercialized research efforts, the resulting research may be improperly powered for important safety, statistical, and efficacy-related analysis and such businesses will likely discontinue enrolling Californians in important life-saving clinical research.

b) If, in order to be exempted from deletion requests in the public health research context, businesses will not be permitted to commercialize (bring the product to market) their researched products, businesses will no longer be incentivized to conduct research in California or enroll Californians in research to find cures for debilitating and deadly diseases.

3. [Proposed] Regulatory Solution to Problem

a) The AG's office shall insert clarification language as follows:
“Clarification to ‘Research’ Definition; § 1798.140(s)(8): ‘(8) [N]ot used for a commercial purpose’ shall be limited only to research using personal information collected from a consumer in the course of his/her interactions with a business’s service or device for purposes unrelated to the scientific, systematic study and observation, including basic research or applied research that is in the public interest.”

Message

From: Kingman, Andrew [REDACTED]
Sent: 3/8/2019 12:18:57 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Pindrop Security Inc. - Comments on California Consumer Privacy Act Rulemaking
Attachments: Pindrop Security - CCPA AG Comments.pdf

Good afternoon,

On behalf of Pindrop Security, Inc., please find attached comments on the California Consumer Privacy Act rulemaking. We would be happy to discuss further at your convenience, and thank you for your attention to this matter.

Respectfully,

Andrew Kingman

Andrew Kingman
Senior Managing Attorney



DLA Piper LLP (US)
33 Arch Street, 26th Floor
Boston, Massachusetts 02110-1447
United States
www.dlapiper.com

Please consider the environment before printing this email.

The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use, disclosure, dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please reply to the sender and destroy all copies of the message. To contact us directly, send to postmaster@dlapiper.com. Thank you.



COMMENTS TO ATTORNEY GENERAL

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 Spring St.
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Re: 1798.185(a)(7) – Multifactor Authentication 2.0

Introduction

As California ushers in a new era of consumer privacy with the California Consumer Privacy Act's (CCPA) passage, the Attorney General and other policymakers should take advantage of this moment by reassessing what constitutes effective security for authenticating requests for access to consumer information. With increased transparency in how companies handle consumer information comes a concurrent responsibility for businesses, government, and non-profits to incorporate protections from the persistent efforts of fraudsters, hackers, and other scammers who every minute are trying to acquire and exploit consumer data for their nefarious purposes.

Advances in Multifactor Authentication (MFA) can greatly increase both consumers' privacy and security. For this reason, we propose that the Attorney General's office recommend large-scale entities subject to CCPA – businesses subject to the law with more than \$100 million in revenue-- adopt what we term "MFA 2.0" for requests under the CCPA to access, delete or obtain in portable format personal information.

Specifically, as the Attorney General's office considers rules related to verifiable consumer requests under § 1798.185(a)(7), it should recommend the use of MFA 2.0 as technology that can help appropriately and quickly authenticate a consumer. This is especially important here because the CCPA requires turning over all "specific pieces" of personal information upon receipt of a verifiable request. This creates a significant avenue for fraudsters to obtain consumer data, including sensitive information such as government ID and financial account numbers. In this context, it is *critical* that strong authentication processes are in place. And, in order to secure personal data more generally, businesses should have effective tools in their toolbox to frustrate fraudsters' efforts.

On the consumer side, technology is progressing quickly, and MFA 2.0 offers unparalleled opportunities to provide a far greater degree of consumer authentication and data security than currently exists.

Finally, we discuss how MFA 2.0 is uniquely equipped to counteract the nascent but pervasive effect of “deepfakes.”

What is MFA 2.0?

MFA 2.0 is a system of multifactor authentication that combines at least two of: 1) something you are; 2) something you have; and 3) something you do. This third factor – something you do – replaces the factor “something you know,” which has been the dominant factor in MFA since MFA’s inception.

The ability to incorporate something you do into an MFA process represents a dramatic, generational improvement in the ability of companies to safeguard customer and employee data, and also offers possibilities to more securely authenticate a consumer in the context of his or her individual transactions.

How Can MFA 2.0 Help Enterprise Businesses Comply with CCPA and Enhance Its Cybersecurity?

As stated above, we propose that the Attorney General recommend the adoption of MFA 2.0 for enterprise-level businesses with in-state revenues over \$100M, and who use a phone line to receive verifiable consumer requests. These businesses should utilize a minimum of two, but preferably three of the authentication factors. Doing so provides a highly certain, and consequently strong, degree of authentication to the transaction.

As an example, Phoneprinting is an enterprise technology that analyzes the entire audio signal of a call, including the one-time characteristics of the call’s path. It combines this information with extractions of non-voice audio features such as the signal-to-noise ratio and dropped frames to help determine the device type, location, and carrier. As Gartner states in its 2018 Report “Don’t Let the Call Center Be Your Fraud Achilles Heel,”¹ “Phoneprinting...can identify anomalies and the unusual repetition of background noise across multiple calls” and is “often effective at detecting fraud.” By establishing a unique signature that combines authentication factors from both the caller (voiceprint) and the device (phoneprint), institutions are able to

¹ Gartner, Inc. *Don’t Let the Contact Center Be Your Fraud Achilles Heel*, Published December 18, 2018, available at <https://www.gartner.com/doc/3895904/dont-let-contact-center-fraud>

make real-time risk assessments to determine whether a caller is a fraudster, or a legitimate customer, even for first-time callers whose voice may not be in a database. This type of authentication improves efficiency, accuracy, and most importantly, the security of consumer information. Institutions can have a much higher degree of confidence that the caller is verified, rather than a fraudster who has obtained legitimate KBA information (such as a former street address or vehicle) to obtain, e.g., a consumer's checking account and routing numbers.

How Can MFA 2.0 Enhance Consumer Security and Privacy?

As hackers have become more sophisticated, knowledge-based authentication (KBA) no longer provides an adequate level of protection for consumers and institutions as a frontline MFA factor. That is because KBA focuses on static data elements, such as birth date, a former address, or a mother's maiden name. These data elements are frequently available via public information on social media platforms, real estate websites, and from services that compile public records for a fee, and often only one or two correct answers to these questions are needed to access an account.² As individuals' data increasingly becomes available on the dark web, these elements are even more readily accessible. The 2015 IRS breach was a result of precisely this point of failure in the system – hackers were able to correctly guess the knowledge-based elements, and as a result, the IRS suffered a breach of 100,000 taxpayer accounts.

Even as consumer information is appearing for sale and use on the black market – some estimates put the number of consumer records available on the black market at 1.4 *billion*³ – consumers are valuing their own data more and more. A 2016 study by the Ponemon Institute indicated that 75% of respondents stored either a moderate or significant amount of personal data on their mobile phones.⁴ Moreover, respondents valued the data on their phones at an average of \$14,000, and respondents who took steps to secure the data on their phone valued their data at \$16,268.

Surely, the amount of data consumers bring with them every day, and the value they place on that data, has only increased since 2016. And while fraudsters are becoming more sophisticated, the very devices that they seek to penetrate are the devices that have the potential to offer the greatest degree of security when they incorporate MFA 2.0.

² <https://www.itprotoday.com/identity-management-access-control/security-sense-how-do-you-do-knowledge-based-authentication-when>

³ <https://www.pymnts.com/news/security-and-risk/2018/retire-knowledge-based-authentication/>

⁴ <https://www.ponemon.org/local/upload/file/How%20much%20is%20the%20data%20on%20your%20mobile%20device%20worth%20Final%2010.pdf>

MFA 2.0's authentication goes far beyond the sophistication with which current hackers and fraudsters operate. By engaging unique, one-time authentication sequencing, efforts to forge, replicate, or guess at an authentication factor stands an exponentially lower chance of success. The ability to pair an identifier such as a highly developed voiceprint, and also the device proximity that MFA 2.0 has the potential to include, means that any individual transaction, as well as overall account security, becomes secure to a degree that the current cybersecurity ecosystem has yet to fully appreciate.

MFA 2.0 Can Support Future Public Policy Challenges

In the coming months and years, "deepfakes" – the use of synthetic audio files derived from actual voice recordings, synced with real (sometimes modified) video, will become a pressing public policy and social issue.⁵ While they are currently somewhat rudimentary, increasing sophistication with video and audio development have the potential to wreak havoc with the concept of a democracy based on facts. As this progression occurs, MFA 2.0 will be the single most effective tool to combat these efforts, as it will be able to quickly and accurately determine the authenticity, or lack thereof, of an individual's voice and device origin. Recommended adoption now will help suppress and deter deepfakes in the future.

Next Steps – CCPA and Beyond

The California Attorney General's Office is no stranger to providing guidance on how businesses can best protect themselves and their customers from data breaches. In 2016, this office, under the leadership of then-Attorney General Kamala Harris, issued a data breach report specifically recommending that businesses adopt MFA in order to provide sufficient data security. The report states:

Th[e] authentication system is failing. We don't use unique passwords for each of our accounts because it would simply be too hard to remember them all...Making matters worse, many individuals do not use strong passwords that are difficult to guess.

A stronger form of online authentication uses multiple factors...this form of authentication should be used by all organizations to help protect access to critical systems and sensitive data. Multi-factor authentication should also be more widely available for consumer-facing online accounts that contain sensitive personal information.⁶

⁵ <https://www.biometricupdate.com/201902/threat-of-deepfakes-draws-legislator-and-biometrics-industry-attention>

⁶ <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>

The obsolescence of KBA today echoes the report's warnings about weak, commonly-used passwords just three years ago. Instead of weak passwords, KBA's decreasing relevance and inherent weakness derives from easy-to-guess questions and readily attainable information that informs common questions. Attempting to improve KBA by creating more unique or harder questions means these questions will also be harder to remember, and inevitably create greater friction for a customer trying to log on to an app, or interact with a customer-service business function. Even "easy" KBA questions can be difficult to remember – a 2015 study by Google revealed that only 47% of respondents could remember what they put down as their favorite food a year earlier, but that hackers could guess that food (pizza) nearly 20% of the time.⁷

Your office has been charged, in part, to issue rules regarding consumer verification so that businesses can properly identify consumers as they exercise their rights. This presents grave issues of security and authentication. We request that the Attorney General's office issue guidance recommending the use of MFA 2.0, both in this rulemaking and in other forthcoming publications that examine issues of data privacy and security.

It is not a question of whether MFA 2.0 is effective – it is a question of how quickly it will be adopted. California can help chart a course toward the adoption of virtually instant, virtually impenetrable consumer authentication, and we urge the Attorney General to seize this opportunity.

For these reasons, we respectfully request that your verifiable request rules under § 1798.185(a)(7) recommend use of MFA 2.0 as a method to verify requests, and that subsequent cybersecurity guidance do so as well.

A handwritten signature in black ink, appearing to read "Clarissa Cerda".

Clarissa Cerda
General Counsel
Pindrop Security, Inc.

⁷ <https://www.forbes.com/sites/forbestechcouncil/2018/01/22/everybody-knows-how-knowledge-based-authentication-died/#64b13cee4eee>

Message

From: Ferenc Kovac [REDACTED]
Sent: 3/5/2019 11:37:12 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Public (my) comment/concerns
Flag: Follow up

1. Given that my personal information out there that has likely lead to my recent identity theft (some on the 'dark web', some available for free and the rest requiring payment), how and when may I legally request its removal? How will they know it is I making the request? Will I need to reveal even more personal information, which would compromise me more?
2. How do I find out what they have on their pay-to-see personal data web site, without paying?
3. Is there a list of personal information that is publicly available, and if so, can such collection/aggregation be stopped? A simple example of invasion of privacy is keeping track of my internet or my physical location or buying habits over a period of time. How will this protect us from Vigilant's LPRs and other data gathering (and sale) by outfits such as TLO and FB who do not even tell us what they have?
4. What personal information is gathered (and 'only' view-able after a rubber stamp order by the Feds (I recall the interaction with Merkel and Obama)? What right to privacy do we law-abiding-non-terrorist citizens still have, and will the CCPA have any jurisdiction? Will it be stuck in courts and eventually eliminated because of some over-riding National Security concerns?
5. Current opt outs provided are too limited - they say they will share my information with their and their (unnamed) partners - something that I am unable to opt out of. Consumer's data sales and data sharing/collection should be default, and allowed only at the request of the individual.
6. How can we be sure someone like Amazon is not tracking and making use of data their Alexa processes, even when not instructed? Ditto on other 'voice control' consumer items (cable TV remotes, etc.).
7. Verification: how will I know if they are not keeping a subscription/for pay site going, even if they said they erased it?
8. Will consumers be paying out of pocket private legal fees to file claims against offenders?
9. How will any fines the offender help the consumer - they may just view it as a cost of doing business - such as the robo-call companies are currently doing with the FCC. With the hopeful assumption that CCPA succeeds - for large, aggregated claims, such as with the huge Fed v. Wells Fargo fines, will affected consumers need to justify and produce financial loss claims for their share, or will it mostly get swallowed up into the bureaucratic black hole?

Ferenc Kovac

(you probably have my phone number ;-)

Message

From: U U [REDACTED]
Sent: 1/31/2019 11:26:14 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Public Comment: Privacy Regulations - Privacy feedback to AG

Many apartment rental companies use third parties for leasing signing process. They say they are not responsible for any data that these parties collect and share. They also say in their disclaimers that they are not responsible for any data I chose to share with these companies but the fact is that I can only submit an online application for lease operated by these third parties including credit history, employer, bank etc.

These third parties say they in turn share my data with other parties for legitimate business purpose but they do not disclose what that legitimate business purpose is.

"The Website includes certain services, including Active Building and online leasing and employment applications, that are operated by third parties. Any Personal Information you choose to submit through these services will be retained by such third parties pursuant to their own privacy policies. Links to those privacy policies are provided in Section 5 below. We encourage you to familiarize yourself with their terms."

<https://prometheusapartments.com/privacy>

I believe they are selling my information to companies that target financial products like credit card offers.

How I know

Two persons are on lease, both have same credit cards, credit rating and history but the payment of the rent comes from bank account of one person only. This was a safety step in case there is a breach only one bank account not two could be compromised.

So offers come to only the person whose bank account pays the rent.

There are many more examples.

Message

From: Gary Wright [REDACTED]
Sent: 1/17/2019 8:01:38 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Public Comments at San Marcos Session
Attachments: Categories of Personal Data Infographic.pdf

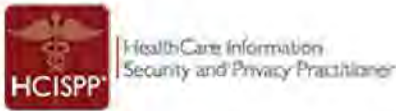
Good morning – I wanted to expand on my comments at the session you held at Cal State San Marcos on Monday this week.

1. Tie the definition of personal information to the NIST 800-122
 - a. The following list contains examples of information that may be considered PI.
 - i. Name, such as full name, maiden name, mother's maiden name, or alias
 - ii. Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number
 - iii. Address information, such as street address or email address
 - iv. Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
 - v. Telephone numbers, including mobile, business, and personal numbers
 - vi. Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)
 - vii. Information identifying personally owned property, such as vehicle registration number or title number and related information
 - viii. Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).
 - b. Promotes uniformity of definitions, especially for those companies that spread across geographical boundaries and countries.
2. Tie Privacy statute to both NIST (NIST 800-53, 800-53A, rev 5 on both – Privacy controls) and ISO (ISO 29100:2011 – Privacy Framework) standards again to promote uniformity across all laws and regulations.

3. Use the Personal Information categories that are accepted by most privacy organizations shown in the Enterprise Consulting Group diagram (attached) for PI Categories.
 - b. Prevent narrow interpretation of only those listed in 1798.80 definition and reluctance to honor the "including, but not limited to" and only considering those categories listed after the "including, but not limited to".
4. Consider GDPR regulations when setting definitions and or rules, for example days allowed to respond to consumers, as well as standardizing definitions and rules to help corporations that have consumers across several boundaries, i.e., California, US, EU, Asia, etc.
 - . Helps promote consistency across boundaries so corporations don't have to staff up to provide privacy services based on geography and geographical regulations. Could severely impact the bottom line of companies.
 - a. Doesn't make the CCPA only about California consumers. Privacy is an international concern and should have consistent standards and regulation that span across boundaries.

Thank you for considering my comments and suggestions,

Gary Wright



Consultant

Corporate Information Security (CIS) Program



CATEGORIES OF PERSONAL INFORMATION

The following are categories of information relating to an individual, whether it relates to his or her private, professional or public life. Categories are not exclusive. Information may transcend multiple categories.



INTERNAL



Knowledge and Belief

Information about what a person knows or believes religious beliefs, philosophical beliefs, thoughts, what they know and don't know, what someone thinks



Authenticating

Information used to authenticate an individual with something they know passwords, PIN, mother's maiden name



Preference

Information about an individual's preferences or interests opinions, intentions, interests, favorite foods, colors, likes, dislikes, music



EXTERNAL



Identifying

Information that uniquely or semi-uniquely identifies a specific individual name, user-name, unique identifier, government issued identification, picture, biometric data



Ethnicity

Information that describes an individual's origins and lineage race, national or ethnic origin, languages spoken, dialects, accents



Sexual

Information that describes an individual's sexual life gender identity, preferences, proclivities, fetishes, history, etc.



Behavioral

Information that describes an individual's behavior or activity, on-line or off browsing behavior, call logs, links clicked, demeanor, attitude



Demographic

Information that describes an individual's characteristics shared with others age ranges, physical traits, income brackets, geographic



Medical and Health

Information that describes an individual's health, medical conditions or health care physical and mental health, drug test results, disabilities, family or individual health history, health records, blood type, DNA code, prescriptions



Physical Characteristic

Information that describes an individual's physical characteristics height, weight, age, hair color, skin tone, tattoos, gender, piercings



HISTORICAL



Life History

Information about an individual's personal history events that happened in a person's life, either to them or just around them which might have influenced them (WWII, 9/11)



FINANCIAL



Account

Information that identifies an individual's financial account credit card number, bank account



Ownership

Information about things an individual has owned, rented, borrowed, possessed cars, houses, apartments, personal possessions



Transactional

Information about an individual's purchasing, spending or income purchases, sales, credit, income, loan records, transactions, taxes, purchases and spending habits



Credit

Information about an individual's reputation with regards to money credit records, credit worthiness, credit standing, credit capacity



SOCIAL

Professional

Information about an individual's educational or professional career job titles, salary, work history, school attended, employee files, employment history, evaluations, references, interviews, certifications, disciplinary actions



Criminal

Information about an individual's criminal activity convictions, charges, pardons



Public Life

Information about an individual's public life character, general reputation, social status, marital status, religion, political affiliations, interactions, communications meta-data



Family

Information about an individual's family and relationships family structure, siblings, offspring, marriages, divorces, relationships



Social Network

Information about an individual's friends or social connections friends, connections, acquaintances, associations, group membership



Communication

Information communicated from or to an individual telephone recordings, voice mail, email



TRACKING



Computer Device

Information about a device that an individual uses for personal use (even part-time or with others) IP address, Mac address, browser fingerprint



Contact

Information that provides a mechanism for contacting an individual email address, physical address, telephone number



Location

Information about an individual's location country, GPS coordinates, room number

Message

From: Veronica Abreu [REDACTED]
Sent: 3/7/2019 7:08:12 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Dan Swislow [REDACTED]
Subject: Public Comments on CCPA
Attachments: CCPA Public Comments on AG Rulemaking.pdf

Dear Attorney General Becerra:

Thank you for giving Square the opportunity to participate in the public comments as your office formulates regulations to further the purposes of the California Consumer Privacy Act of 2018 ("CCPA"). Square's mission is economic empowerment. We provide critical services to millions of small and medium-sized businesses ("SMBs") throughout California and the United States. We partner with SMBs to prevent risk and fraud, and to secure the data they process through Square - both of which rely on a nuanced understanding of customer and business data. Responsible uses of data are also essential for us to provide other critical services to SMBs, such as helping them process payments, run their businesses, pay and provide benefits to their employees, and get access to capital to grow. We fully support thoughtful implementation of strong privacy laws that protect consumers while allowing legitimate businesses such as Square to continue to serve their customers by preventing fraud, securing data, and providing innovative products and services that benefit consumers and SMBs alike.

We respectfully encourage Attorney General Becerra to adopt regulations that balance advancing the substantive rights CCPA grants to consumers with empowering industry to take appropriate measures to mitigate risks, whether of a fraud or security nature, as well as to provide consumers with the products and services they request and that benefit them.

To that end, we urge the AG to issue regulations that clarify the following:

Definition of "Personal Information"

Legislative intent, as reiterated at the February 20, 2019 hearing of the Assembly Committee on Privacy & Consumer Protection, was that CCPA's definition of "personal information" ("PI") (CCPA 1798.140(o) (1)) comprise all data that directly or indirectly **identifies a natural person** residing in California. Indeed, CCPA provisions such as Sec 1798.100(e) and Sec 1798.110(d)(2) would make no sense unless the definition of PI requires that the data directly or indirectly **identify** a natural person.

We urge the Attorney General to issue regulations that clearly reflect this legislative intent, to forestall non-sensible misinterpretations that broaden the intended meaning of "personal information" to include things such as the gender "female," which, in isolation, is capable of being associated with about half the human population but does not *identify* any particular individual. Regulations that clarify the legislative intent by focusing on data that identifies an individual would still protect such data on any device (and collected through devices shared by a household) while protecting innovation that benefits consumers and averting unintended erosion of the privacy of *other* individuals whose data is commingled in the same household or device.

Data "Sales" do not comprise the use of service providers for legitimate business purposes

As the plain language of Section 1798.140(t) makes clear, "Sell," "selling," "sale," or "sold," is intended to capture "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise

communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party ***for monetary or other valuable consideration.***"

As expressly stated in 1798.140(t)(2), this definition ***excludes*** - and the CCPA does not provide consumers a right to opt out of - data disclosures by a business to service providers as reasonably necessary to effectuate legitimate business purpose. We urge the Attorney General to issue regulations that clearly implement this thoughtful legislative choice, which was carefully calibrated to permit legitimate business such as Square to, for example, be able to continue to share reasonably necessary data with service providers who assist it with its fraud detection and prevention, anti-money laundering, anti-terrorist finance efforts as well as with those who help it run its technology infrastructure, payments processing, or who otherwise assist it in the provision of its products and services.

Verifying data rights requests

We urge the Attorney General to adopt regulations under Section 1798.185(a)(7) that empower businesses to make risk-based determinations of what constitutes a "verifiable consumer request," calibrated to the reality and specific context of their relationship with the consumer. As both the plain language and legislative intent of Section 1798.140(y) make clear, it is crucial that the business be able to verify that "a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf."

Without this critical requirement, someone could submit CCPA data requests to fraudulently obtain a copy of someone else's data without even having to bother hacking a company that holds it. To be *effective* verifying requests, businesses must be given the discretion to conduct risk-based authentication of consumer requests tailored to the context of their business, their relationship to the consumer, industry trends, evolving attack vectors and technologies, and security considerations. A one-size fits all rule that takes away a business's discretion to conduct risk-based authentication (including via account logins) would backfire and hurt consumers and businesses alike.

Exemptions

Lastly, we urge you to clarify that the plain language of 1798.145(a) means that the obligations imposed by CCPA shall not interfere with a business's ability to effectively comply with the law, including by complying with anti-money laundering and anti-terrorist finance rules, engaging in fraud and risk detection and prevention, and meeting data security obligations.

We thank you and your staff in advance for taking a thoughtful approach to this impactful and critically important process.

Best,

Veronica Abreu
Chief Privacy Officer, Square Inc.

Dear Attorney General Becerra:

Thank you for giving Square the opportunity to participate in the public comments as your office formulates regulations to further the purposes of the California Consumer Privacy Act of 2018 (“CCPA”). Square’s mission is economic empowerment. We provide critical services to millions of small and medium-sized businesses (“SMBs”) throughout California and the United States. We partner with SMBs to prevent risk and fraud, and to secure the data they process through Square - both of which rely on a nuanced understanding of customer and business data. Responsible uses of data are also essential for us to provide other critical services to SMBs, such as helping them process payments, run their businesses, pay and provide benefits to their employees, and get access to capital to grow. We fully support thoughtful implementation of strong privacy laws that protect consumers while allowing legitimate businesses such as Square to continue to serve their customers by preventing fraud, securing data, and providing innovative products and services that benefit consumers and SMBs alike.

We respectfully encourage Attorney General Becerra to adopt regulations that balance advancing the substantive rights CCPA grants to consumers with empowering industry to take appropriate measures to mitigate risks, whether of a fraud or security nature, as well as to provide consumers with the products and services they request and that benefit them.

To that end, we urge the AG to issue regulations that clarify the following:

Definition of “Personal Information”

Legislative intent, as reiterated at the February 20, 2019 hearing of the Assembly Committee on Privacy & Consumer Protection, was that CCPA’s definition of “personal information” (“PI”)¹ comprise all data that directly or indirectly **identifies a natural person** residing in California. Indeed, CCPA provisions such as Sec 1798.100(e)² and Sec 1798.110(d)(2)³ would make no sense unless the definition of PI requires that the data directly or indirectly **identify** a natural person.

We urge the Attorney General to issue regulations that clearly reflect this legislative intent, to forestall non-sensible misinterpretations that broaden the intended meaning of “personal information” to include things such as the gender “female,” which, in isolation, is capable of being associated with about half the human population but does not *identify* any particular individual. Regulations that clarify the legislative intent by focusing on data that identifies an

¹ CCPA 1798.140(o) (1)

² Clarifies that businesses are not required “to **reidentify** or otherwise link information that is **not** maintained in a manner that would be considered **personal information**.” (emphasis added)

³ Clarifies that businesses are not required to “**Reidentify or otherwise link** any data that, in the ordinary course of business, is **not maintained in a manner** that would be considered **personal information**.” (emphasis added)

individual would still protect such data on any device (and collected through devices shared by a household) while protecting innovation that benefits consumers and averting unintended erosion of the privacy of *other* individuals whose data is commingled in the same household or device.

Data “Sales” do not comprise the use of service providers for legitimate business purposes

As the plain language of Section 1798.140(t) makes clear, “Sell,” “selling,” “sale,” or “sold,” is intended to capture “selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party **for monetary or other valuable consideration.**”

As expressly stated in 1798.140(t)(2), this definition **excludes** - and the CCPA does not provide consumers a right to opt out of - data disclosures by a business to service providers as reasonably necessary to effectuate legitimate business purpose. We urge the Attorney General to issue regulations that clearly implement this thoughtful legislative choice, which was carefully calibrated to permit legitimate business such as Square to, for example, be able to continue to share reasonably necessary data with service providers who assist it with its fraud detection and prevention, anti-money laundering, anti-terrorist finance efforts as well as with those who help it run its technology infrastructure, payments processing, or who otherwise assist it in the provision of its products and services.

Verifying data rights requests

We urge the Attorney General to adopt regulations under Section 1798.185(a)(7) that empower businesses to make risk-based determinations of what constitutes a “verifiable consumer request,” calibrated to the reality and specific context of their relationship with the consumer. As both the plain language and legislative intent of Section 1798.140(y) make clear, it is crucial that the business be able to verify that “a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf.”

Without this critical requirement, someone could submit CCPA data requests to fraudulently obtain a copy of someone else's data without even having to bother hacking a company that holds it. To be *effective* verifying requests, businesses must be given the discretion to conduct risk-based authentication of consumer requests tailored to the context of their business, their relationship to the consumer, industry trends, evolving attack vectors and technologies, and security considerations. A one-size fits all rule that takes away a business's discretion to conduct risk-based authentication (including via account logins) would backfire and hurt consumers and businesses alike.

Exemptions

Lastly, we urge you to clarify that the plain language of 1798.145(a) means that the obligations imposed by CCPA shall not interfere with a business's ability to effectively comply with the law, including by complying with anti-money laundering and anti-terrorist finance rules, engaging in fraud and risk detection and prevention, and meeting data security obligations.

We thank you and your staff in advance for taking a thoughtful approach to this impactful and critically important process.

Best,

Veronica Abreu
Chief Privacy Officer, Square Inc.

Message

From: Drew Liebert [REDACTED]
Sent: 3/8/2019 3:19:12 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Anthony Lew [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=24934231988147abb6982536642d654f-Anthony Lew]
Subject: Purism Comments About CCPA Regulations Development and Implementation

Dear Attorney General Becerra:

Thank you for the opportunity to briefly share with you my thoughts on the imperative for developing strong and effective privacy regulations implementing the CCPA as you fulfill your critically-important privacy protection efforts on behalf of all Californians.

I am the president and CEO of Purism, a growing technology privacy company I started five years ago founded on the simple but profound notion that technology and privacy-protection on the Internet are not just compatible and profitable -- but are also a moral imperative. I am an unusual tech company commenter, for I am seeking much stronger consumer privacy protections here in California and around the world, not weaker ones.

I believe the default approach in California should be the right to optin, rather than requiring all of us to have to inconveniently optout, of the exploitation and profiteering from our most personal information across all software, every service, and every site we use. I also strongly support your efforts to hold companies, including mine, fully accountable in court if we violate a person's privacy rights - rights which you have noted are guaranteed in our state Constitution.

Purism is already manufacturing computer hardware and offering other technology services in California, assembling privacy-protecting (and AB 375-compliant) laptops in Carlsbad, including the operating system, applications, and bundled services - all services specifically designed not to track you -- period. The company is growing triple-digits year over year. And notwithstanding all the nay-saying by some of the country's biggest tech companies, I believe it is crystal clear that future innovation and job creation around "privacy by design" is actually the bright and inevitable economic and moral future for the tech sector on which California and the nation need to lead.

I suspect the three adjacent words I used in the opening paragraph of my letter have not come up often in comments from most other tech companies you have received, namely, "technology privacy company." That is because the major technology companies have arrogantly profited from their users' data as the very foundation of their cynical business models. Indeed, as you know, the business models of almost all the major tech companies continue to be privacy-exploiting rather than privacy-protecting.

User privacy protection however is at the very heart of the business model of my social purpose company, Purism. I started Purism when I came to realize that my two daughters, like all children, need easy-to-use products and services that protect them, rather than exploit them. As a technologist, I understand painfully well how much the technology sector can exploit my kids and all of our children with ease - and are doing so every day. For example, as you know well, most smartphones today track your exact location and everything done on your device, every millisecond of every day, and record that personal data permanently for retrieval and potential sale anytime, never purging every search, purchase, chat, photo, video, and article you read.

This unregulated exploitative business model used by most tech companies today ensures everything you do in the digital world leaves

excruciating details about you permanently - all without your knowledge. My company flips this current exploitive approach on its head. And it's working: Consumer demand for privacy is real and happening - and it's high time for it to be the default: privacy by design. And though they often suggest otherwise, this is an approach all tech companies can implement if they are truly committed to user privacy, beyond just marketing slogans.

In short, I believe it's long past time for California's extraordinary tech industry to stop harvesting and "sharing" our most personal private data without our meaningful consent and knowledge. Your upcoming regulations, in implementing this clear intent behind AB 375, have the power - indeed, I submit the responsibility -- to make this privacy protection a reality.

In the meantime, we are hearing some business and tech communities suggesting California's new privacy law is going to cause extraordinary business hardship and confusion. These are of course the same arguments that were made by many of these same companies regarding Europe's GDPR - but since the GDPR went into effect, these companies have prospered, and in most cases have grown enormous profits. That is real evidence that California's new privacy law is not going to destroy Internet commerce as we know it, notwithstanding claims that the sky will fall here too.

I believe that AB 375 (or stronger) protections - just like those in the GDPR - are not going to be hard to implement. The key is whether technology companies, including my own, are willing to begin to honor our customer's privacy rights by designing, or if need be re-designing, our services to be privacy-protecting by default, rather than privacy-exploiting by default.

Is this possible? Absolutely. Purism is just one example proving this every day, because it believes privacy is a right, and one's every location and every communication and every web page and every search should not be stored permanently -- and exploited forever -- simply to be able to access needed services online. We design our products to reflect that belief - just as the big tech companies could do in order to comply with AB 375, and, hopefully, your upcoming regulations implementing this landmark new privacy law.

Please contact me if you have any questions at all about my comments or would like any additional information. You can view Purism's current products, and our company philosophy, at https://urldefense.proofpoint.com/v2/url?u=http-3A__www.Purism.com&d=DwIDAQ&c=uASjV29gZuJt5_5J5CPRuQ&r=kXcUIWCJFJC3Y7A6WP15oNx0wEUzL_7Mxj0spe9bxxI&m=cmDwIYtGGIaIm0QQ-bLb_EszxH05VtJffD-bQ_C5D5c&s=EGlADT6YkMuIgnRxyXKqcIrqgA7SQAt-_JQGQh974bU&e= and I'd be delighted to demonstrate our products anytime to you or your staff.

Todd Weaver
CEO, Purism

Message

From: Determann, Lothar [REDACTED]
Sent: 1/11/2019 9:53:21 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: RE: Attorney General Becerra to Continue Public Forums on California Consumer Privacy Act as Part of Rulemaking Process

Thank you, much appreciated. Here are my notes from the hearing in San Francisco:
<https://iapp.org/news/a/californias-ccpa-forums-are-underway-heres-what-happened-at-the-first-one/>

Please let me know if I can assist further.

Lothar

This message may contain confidential and privileged information. If it has been sent to you in error, please reply to advise the sender of the error and then immediately delete this message. Please visit www.bakermckenzie.com/disclaimers for other important information concerning this message.

From: Privacy Regulations [mailto:PrivacyRegulations@doj.ca.gov]
Sent: Friday, January 11, 2019 5:47 PM
To: Privacy Regulations
Subject: [EXTERNAL] Attorney General Becerra to Continue Public Forums on California Consumer Privacy Act as Part of Rulemaking Process

Good afternoon,

On January 8, 2019, the California Department of Justice (DOJ) held the first CCPA Public Forum in San Francisco. For those who were in attendance, thank you for your participation.

As the rulemaking process continues, the Department of Justice will hold five additional statewide forums to gather comments from stakeholders.

CCPA PUBLIC FORUMS

January 14, 2019 10 AM - 1 PM
California State University, San Marcos
333 S. Twin Oaks Valley Road
San Marcos, CA 92096

January 24, 2019 10 AM - 1 PM
Cesar Chavez Community Center
2060 University Avenue
Riverside, CA 92507

January 25, 2019 10 AM - 1 PM
Ronald Reagan Building
300 S. Spring Street
Los Angeles, CA 90013

February 5, 2019 10 AM - 1 PM
California State Building
1500 Capitol Avenue
Sacramento, CA 95814

February 13, 2019 10 AM - 1 PM
California State Building
2550 Mariposa Mall, Room 1036
Fresno, CA 93721

The DOJ invites all interested persons and parties to submit comments regarding the CCPA regulations at any of the statewide forums, via mail or email.

To email or mail please follow the instructions below:

- Email: PrivacyRegulations@doj.ca.gov
- Mail: CA Department of Justice

ATTN: Privacy Regulations Coordinator

300 S. Spring St., Los Angeles, CA 90013

Please feel free to share this information with your relevant contacts. I have attached a PDF flyer for your convenience.

For additional information about the CCPA, please visit www.oag.ca.gov/privacy/ccpa.

Thank you.

CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.

Message

From: Evan Engstrom [REDACTED]
Sent: 3/8/2019 2:47:13 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Re: Implementing Regulations for the California Consumer Privacy Act
Attachments: Engine - CCPA comments.pdf

Dear Privacy Regulations Coordinator:

Attached please find the comments of Engine Advocacy regarding the implementing regulations for the California Consumer Privacy Act.

--
Evan Engstrom
Executive Director

[Engine](#)
[REDACTED]



Engine
44 Tehama St.
San Francisco, CA 94105

March 8, 2019

The Honorable Xavier Becerra
Attorney General
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

Re: Implementing Regulations for the California Consumer Privacy Act

Dear Mr. Becerra:

Engine submits the following comments in response to the Justice Department's request for comments regarding the Department's rulemaking process in the wake of the 2018 passage of the California Consumer Privacy Act (CCPA). We appreciate the opportunity to comment.

I. Introduction

Engine is a non-profit technology policy, research, and advocacy organization that bridges the gap between policymakers and startups. Based in San Francisco, California, and Washington, D.C., Engine works with a nationwide network of startups to understand how ongoing policy debates affect new and small high-growth technology companies and how to best advocate on behalf of the ever-changing and growing startup ecosystem in the U.S. The thriving U.S. startup ecosystem is responsible for some of the most innovative products and services as well as the vast majority of net job growth in the U.S. The center of that activity is undeniably in California. Creating regulatory burdens in the name of protecting users' privacy without fully understanding the actual privacy benefits and the very real threats to startups risks unnecessarily crippling one of the most important economic sectors of our state and country.

II. Regulations have a disproportionate effect on startups, which are the companies best-positioned to innovate and challenge incumbents.

Engine supports providing consumers with increased transparency and control over their data. In fact, startups in this state, as well as the rest of the U.S., depend on maintaining consumers' trust in the Internet.

Most of the conversations surrounding consumer privacy in recent years have focused on the headline-grabbing missteps of some of the world's largest Internet companies. The ballot initiative that led to the passage of CCPA was undoubtedly inspired by¹—and gained momentum after²—some understandably controversial data collection, use, and sharing practices by Silicon Valley giants came to light. While we're long overdue for a serious policy conversation about protections for consumer data, regulating with only the largest players in mind will enshrine their market power by hurting smaller companies.

Startups have the most to lose in today's policy debate about consumer privacy and in the forthcoming implementation of the CCPA. If consumers lose trust in the Internet ecosystem, it's the products and services created by startups—which typically don't have long-standing reputations or relationships with consumers—that will be abandoned first. But if policymakers create complex and burdensome regulations, startups won't be able to afford to comply since they don't have large budgets for legal resources. Ironically, writing policies based on fears about the world's largest Internet companies' data practices could ensure that only those large Internet companies continue to exist.

It remains to be seen how CCPA compliance costs will impact startups. In discussions with our statewide network of companies, it's clear that many have struggled to think about how to comply with the law since the law itself remains unsettled.

There is an illustrative example of how costly and burdensome privacy rules that can shut small businesses out of the market: the newly-implemented General Data Protection Regulation (GDPR) in the European Union. Less than a year since the implementation of GDPR last May, companies have started speaking publicly about the compliance costs they faced³ in terms of dollars and person-hours and the choice to avoid these rules by leaving the European Union market.⁴ Smaller companies are at a disadvantage in post-GDPR Europe. One study of the online advertising market found that post-GDPR, small ad tracking firms were most severely and negatively impacted, while Facebook suffered a small loss and Google actually realized a small increase in market share.⁵ As California implements CCPA, policymakers should keep in mind the kind of disproportionate impact that regulations can have on startups.

- III. Startups need a balanced approach to the definition of personal information, which should explicitly exclude de-identified and aggregated data.

¹ <https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html>

² <https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law>

³ <https://www.mediapost.com/publications/article/309342/the-price-of-compliance-study-uncovers-gdpr-costs.html>

⁴ <https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html>

⁵ <https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr>

Startups rely on data that carries little or no risk of privacy harms—especially de-identified and aggregated data—every day to innovate and improve their offerings to consumers. Engine is concerned that the current definition of personal information in CCPA is overly broad and does not explicitly exclude de-identified and aggregated data, which will consequently make it difficult for startups to comply with the obligations in the law that relate to the definition of personal information. CCPA rulemaking should clarify the law by explicitly excluding aggregated and de-identified data, as it's defined by the law (1798.140(h)), from the definition of personal information. More broadly, as the Department continues to consider future CCPA-related rulemakings such as updating the definition of personal information “to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns,” Engine hopes the Department will take a balanced approach. It should avoid adding new categories of information that startups rely on but which do not pose the threat of substantial privacy harms for consumers.

- IV. Startups need clarity on methods for submitting verifiable requests for data that don't create opportunities for fraud or requirements for additional data collection.

As written, CCPA could put companies in the complicated position of either having to collect more personal information or run the risk of unauthorized disclosure of consumer data in an effort to comply with the law. CCPA requires companies to “promptly take steps to determine whether the request is a verifiable request,” and the time to complete those steps cannot add to the 45 days a company has to respond to a verifiable request. While the law (1798.180(a)(7)) includes “a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account” as a verifiable request under the law, it also prohibits a company from “requir[ing] the consumer to create an account with the business in order to make a verifiable request” (1798.130(a)(2)).

If a consumer has a relationship with a company, submitting a verifiable request through the consumer's password-protected account with the company is arguably the most pro-privacy way to process consumer requests for their own data. If companies are kept from using established relationships with consumers to receive and evaluate requests, they will have to either collect additional, likely sensitive, information—such as photo or government-issued identification—or run the risk of disclosing information to a bad actor posing as a particular consumer, which triggers other risks and legal penalties. The Department should craft rules regarding verifiable requests to minimize the administrative burden on companies, the need to collect additional information, and the risk of fraudulent access to consumer data.

- V. The design and procedure of the opt-out function should include flexibility reflect the various ways startups interact with consumers.

Startups interact with users in a variety of ways. The design of everything from a website to an app to a connected device varies wildly across the technology industry and startup ecosystem. The rules regarding “a recognizable and uniform opt-out logo or button” should take those

variances into account. Ideally, the Department would seek input from a diverse set of technology industry and startup ecosystem members who can provide expertise on user interfaces so that the uniform opt-out logo or button can be developed in way that clearly communicates its purpose and consequences across various interfaces and contexts.

Engine supports the Department using its rulemaking process to add some flexibility to a company's obligations once a consumer opts-out of the sale of his or her information and new burdens and obligations are triggered. Given the realities that startups face—and the realities of the data architectures they rely on—it is not practical to expect complete and immediate compliance with an opt-out request once it has been submitted by a consumer. Engine also supports the Department adding flexibility to choices consumers are granted when they want to opt-out of the sale of their personal information. The current definition of “sale” in the law (1798.140(t)(1))—specifically the inclusion of “making available...or otherwise communicating...[to] a third party for monetary or other valuable consideration”—is so broad that it will likely sweep in data sharing that could benefit consumers. The opt-out process could be constructed so consumers can opt-out of types of sales to entities they find troubling, such as data brokers, without opting out of all data sharing covered under the new law.

- VI. CCPA should retain a 30-day cure period to ensure startups can improve the security of users without immediate fear of costly statutory damages.

Currently CCPA (1798.150(b)(1)) gives businesses a 30-day window to address consumer complaints about alleged unauthorized access and exfiltrations, thefts or disclosures in violation of the law before consumers can bring a case for statutory damages. This provision allows good actors to receive notice so they can respond to security concerns before facing statutory damages. Those statutory damages can be cripplingly damaging under the law, which sets them at between \$100 and \$750 per consumer per incident. Policymakers have suggested removing this 30-day cure period, but we urge that the provision stay in the law. Allowing companies and consumers to communicate about security concerns without immediate fear of legal actions resulting in costly statutory damages will encourage developments that improve security for users.

- VII. CCPA rulemaking should seek to minimize compliance burdens for the diverse business models represented in California's startup ecosystem.

The startup ecosystem in California contains companies of all sizes offering products and services that depend on wildly different business models. Each company faces different regulatory and legal obligations at the state and federal level, and there is no one-size-fits-all compliance strategy. The compliance issues faced by an app that collects biometric health-related data from its users are very different than the compliance issues faced by an Internet platform that allows individuals to sell physical goods online or the compliance issues faced by a website producing children's programming. Engine appreciates the concerted efforts the Department is making in this rulemaking process to harmonize CCPA's obligations with

existing obligations under state and federal law and add exceptions to CCPA when necessary to resolve any conflicts.

VIII. Conclusion

While the trope of a young startup CEO coding an ingenious app out of a garage or dorm room with little regard for its users' privacy has pervaded popular culture, California's thriving startup ecosystem is full of companies working in good faith to protect the privacy and security of their users. Startups support giving users better and more informed control over their data. We support the overall goals of CCPA, but we hope policymakers continue to refine and clarify the law—including through the Department's rulemaking process—to ensure California's startups can innovate and compete.

Message

From: Ariel Silverstone [REDACTED]
Sent: 3/8/2019 10:53:50 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: RE: Submit CCPA Preliminary Comments by Friday, March 8th

Hello Team and nice meeting some of you in Stanford.

Here are my suggestions:

1. Require that each law-covered entity appoint a DPO, in writing.
2. Appoint a government + industry privacy focused advisory board for the purpose of CCPA and upcoming rules. Examples: [Future-of-Privacy Forum](#), [the United Nations](#), and from [the City of Oakland](#).
3. Clarify the requirement of, and the description for *Transparency*. Doing so will help not only consumers, but businesses too. As an example, [here](#) is a pdf from A29WP (Papers of the Article 29 Working Party: Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679: WP 2602/2003'. This can be also seen at GDPR, Art. III(1)(a)(12).
4. Prohibit the collection of device [UUID](#). The only purpose outside of law enforcement and the actual connectivity of devices, is to combine vast volumes of data from multiple sources, of a specific data subject.
5. I suggest that the verification-before-DSAR-request compliance will be similar to GDPR, Rec. 64. I also would recommend that the verification requirements shall not be made more difficult than the process used to collect the data itself: if an email address (or an IP address) were used to identify the data subject at the time of collection, make verification before compliance with a request also be email address (or an IP address).
6. The definitions of data categories should be made clearer. For example: PII, SPI, PHI. I also suggest synchronicity with the definitions in [ISO 291xx](#) and with ISO [27xxx](#) when appropriate.
7. The potential 'conflict' regarding HIPAA and similar laws should be clarified. For example, if 'first-name last-name' is part of a HIPAA record, I believe the intent of the legislature was not to exclude these fields from the CCPA protection, only to avoid a conflict with the actual PHI. Also, based upon comments made, I note that some organizations are 'declaring' themselves out of CCPA scope because they are a healthcare-related organization. I suggest clarifying that category of businesses' responsibilities.
8. I have noted a few questions regarding GPS. For example, could we clarify what happens when a device (phone or car), which has GPS capabilities, of a California resident, enters (or leaves) the State boundaries.
9. Please clarify the line between Service Providers, 3rd parties and data brokers. Many Ad-tech companies are going to claim they are if the least onerous category.
10. Please clarify whether (and I suggest 'yes') derived and assumed data regarding a data subject is included in the disclosure, sharing, selling and removal requirements of the data. If not, we are likely to find easily re-identifiable data everywhere.
11. I suggest that a private right/cause of action be allowed. Simply put: since cost-of-compliance will be higher then the penalty of up to \$7,500 per incident, if we really want businesses to take notice we should rephrase that as \$7,500 per record and per customer.
12. Please seriously consider the removal of the incentive-trade section. Keeping it will create two classes of citizens and will negatively effect our weakest (read elderly and lower economic group) residents.
13. I would recommend an addition whereby companies should not be allowed to share data with other entities in areas which are hostile to privacy. Examples may include in China, in Russia, etc.

Happy to discuss, and thank you again for asking.

Ariel Silverstone, MSc, CISSP, CIPP/IT, CIPM

External Data Protection Officer



Data Protectors, LLC. and Data Protectors Sp. z o. o. Sp. k. (KRS 0000723878)

Registered Data Protection Officer

Germany: Datenschutzbeauftragter (DSB) GDD A5248

France: Correspondants Informatique et Libertés (CIL)

Poland: Inspektor Ochrony Danych (IOD)



From: Privacy Regulations

Sent: Wednesday, March 6, 2019 6:58 PM

Subject: Submit CCPA Preliminary Comments by Friday, March 8th

Good evening,

On June 28, 2018, Governor Brown signed Assembly Bill 375, now known as the California Consumer Privacy Act of 2018 (CCPA). The CCPA grants consumers new rights with respect to the collection and use of their personal information.

The CCPA, which will go into effect on January 1, 2020, authorizes the Attorney General to promulgate regulations that will establish procedures to facilitate consumers' rights. The California Department of Justice (DOJ) is currently collecting feedback from stakeholders early in the rulemaking process.

The DOJ invites all interested persons and parties to submit comments regarding the CCPA regulations via mail or email. Written comments should be submitted by **Friday, March 8th, 2019** for consideration in the preliminary rulemaking stage.

To email or mail comments, follow the instructions below:

- Email: PrivacyRegulations@doj.ca.gov
- Mail: CA Department of Justice

ATTN: Privacy Regulations Coordinator

300 S. Spring St., Los Angeles, CA 90013

Thank you.

You are receiving this email because you've signed up to receive notifications on the California Consumer Privacy Act (CCPA) rulemaking process at: <https://oag.ca.gov/privacy/ccpa/subscribe>. If you'd like to be removed from this mailing list, please email: PrivacyRegulations@doj.ca.gov.

CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.

Message

From: [REDACTED]
Sent: 3/8/2019 4:42:59 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: [REDACTED]
Subject: Refinitiv Comment Letter
Attachments: Refinitiv CCPA Comment Letter.pdf

Please find attached comment letter from Refinitiv regarding the CCPA regulations.

Feel free to contact me with any questions or concerns.

Thank you,

Chip

Chip Thresher

Head of Government Affairs, Americas



REFINITIV™
DATA IS JUST
THE BEGINNING 

Sensitivity: Confidential

CCPA00000999

This e-mail is for the sole use of the intended recipient and contains information that may be privileged and/or confidential. If you are not an intended recipient, please notify the sender by return e-mail and delete this e-mail and any attachments. Certain required legal entity disclosures can be accessed on our [website](#).

The Honorable Xavier Becerra
Attorney General, State of California
1300 I Street
Sacramento, CA 95814

Via Email to: PrivacyRegulations@doj.ca.gov

Dear Attorney General Becerra,

Refinitiv writes to provide comments regarding the California Consumer Privacy Act of 2018 (CCPA) while the California Department of Justice is collecting feedback from stakeholders during their preliminary rulemaking process.

Refinitiv is one of the world's largest providers of financial markets data and infrastructure, serving over 40,000 institutions in over 190 countries. We provide leading data and insights, trading platforms, and open data and technology platforms that connect a thriving global financial markets community - driving performance in trading, investment, wealth management, regulatory compliance, market data management, enterprise risk and fighting financial crime.

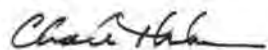
Our primary concern with the CCPA is regarding clarity around activities performed to fight financial crime. To combat financial crime, private sector corporations, financial institutions, governments, law enforcement agencies and regulators often need to screen both customers and suppliers. In many cases, as with banks, these checks on organizations are mandatory. Such activities represent best practices and are in line with international objectives for corporate governance and efforts to fight crime, terrorism, slavery, bribery and corruption around the world, including standards set forth in the UN Global Compact. These activities also complement policy priorities stated directly by the California Department of Justice, including fighting human trafficking, terrorism, and money-laundering.

Activities such as checks on customers and suppliers to prevent money laundering, terrorist financing and fraud often necessitate the processing of personal information, as defined under §1798.140 of the CCPA. For these activities, the personal information processed is aggregated largely from publicly available sources and often supplied by data providers like Refinitiv, which maintain databases and provide services to support these efforts. Generally, Refinitiv and similar entities have no direct relationship with the entity or person (e.g., "consumer") being screened, yet such activities serve a clear public interest, by helping to identify individuals and organizations that are engaged in illegal or suspicious activities. Any rulemaking should make clear that the CCPA shall not apply to these types of activities in which Refinitiv and organizations like it are engaged. Refinitiv should be permitted to process personal information for these purposes and not be required to honor a consumer's request to delete their personal information, or opt out of Refinitiv's sharing of such personal information for these purposes. Any interpretation of the CCPA that would allow a potential bad actor to manipulate the system runs contrary to law and the work of the California Department of Justice.

Refinitiv is proud to play its part in helping our customers in banking and finance and other sectors to both fulfill their legal obligations and help in the fight against financial crime and modern slavery. We hope the Attorney General's office will consider these important public interest goals when using its statutory authority to clarify this important issue, along with other issues, including third-party responsibilities, the use of publicly available information, and the establishment of exemptions to comply with state and federal law, under the Attorney General's rulemaking authority specified in §1798.185 of the CCPA.

Refinitiv would be pleased to discuss our comments at greater length with the Office of the Attorney General. Please feel free to contact Chip Thresher at [REDACTED] or [REDACTED] with any questions about this comment.

Respectfully submitted,



Chip Thresher
Head of Government Affairs, Americas
Refinitiv

Message

From: Sugarman, Peggy (HRD) [REDACTED]
Sent: 3/8/2019 2:23:12 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Regulatory Request from the City & County of San Francisco
Attachments: CCSF Response to DOJ.CCPA.3.8.2019.pdf

Please see attached comments from the City & County of San Francisco to the pre-rulemaking notice of solicitation for public comment on the California Consumer Privacy Act of 2018.



Connecting People with Purpose

Peggy Sugarman, Workers' Compensation Director

Department of Human Resources

One South Van Ness Ave., 4th Floor

San Francisco, CA 94103

[REDACTED]
Website: www.sfdhr.org

City and County of San Francisco
Micki Callahan
Human Resources Director



Department of Human Resources
Connecting People with Purpose
www.sfdhr.org

March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

VIA EMAIL

RE: Regulations to Exempt the California Workers' Compensation System from the California Consumer Privacy Act

Dear Privacy Regulations Coordinator,

The City & County of San Francisco is a self-insured, primarily self-administered employer for Workers' Compensation purposes. We receive approximately 2800 new claims per year, approximately 25% of which are handled by a contracted third-party administrator. Our benefit delivery program depends heavily on the safe transfer of private information, particularly medical information, to hospitals, physicians, medical bill review organizations, utilization review organizations, investigation firms, document retrieval companies, banks, and other service providers. This information transfer is essential to the proper management of workers' compensation claims.

While the City is supportive of the intent of the CCPA to safeguard consumer privacy, we are concerned that the law has unintended consequences for the workers' compensation industry as outlined in detail by the March 8, 2019 letter from the Risk Insurance Management Society (RIMS) – California Delegation. Acknowledging that public agencies are exempt from the requirements of the CCPA, the businesses that support our program are not.

For example, Civil Code § 1798.115(a) of the CCPA states that the consumer has a right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer (1) the categories of personal information that the business collected about the consumer, (2) the categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold, and (3) the categories of personal information that the business disclosed about the consumer for a business purpose.

Section 1798.115(a) would likely apply to nearly all workers' compensation claims transactions. As noted above, medical records are sent to a medical provider network, medical records are sent to a utilization review organization, and medical records are sent to an independent review organization contracted by the State for Independent Medical Review. "Personal information" would clearly include payment information sent to a payment processing center falling within the definition of "service provider." A vocational evaluator would clearly need to know "professional or employment-related information" that is included within the definition of "personal information" in Civil Code Sec. 1798.140(o)(1)(I).

During the routine administration of a workers' compensation claim, especially a claim involving indemnity benefits, considerable "personal information," as defined in Civil Code Sec. 1798.140(o), must be collected so that the claim can be processed and the injured worker can be treated and compensated. For physicians and other service providers, an injured worker's personal information is collected during the payment and remittance process.

Extensive laws already exist to protect the privacy of injured workers¹. Disruption of the flow of information to these necessary entities in order to provide state-mandated medical treatment and other services would be catastrophic.

We join with the RIMS – California Delegation in our request that you, as the regulatory body required to adopt regulations to further the purposes of the CCPA, adopt regulations that exempts all aspects of the workers' compensation system necessary to deliver timely benefits as mandated by the State Division of Workers' Compensation from the requirements of the CCPA.

Thank you for your consideration,

A handwritten signature in dark ink, appearing to read 'Peggy W. Sugarman', with a long horizontal flourish extending to the right.

Peggy W. Sugarman, Workers' Compensation Director
City & County of San Francisco

Cc: Micki Callahan, Human Resources Director
City & County of San Francisco

¹ See Labor Code sections 138.7, 3762(c), 4603.4(b), 4610.5(m)

Message

From: Sheila Stine [REDACTED]
Sent: 3/6/2019 6:17:11 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Request for Rulemaking
Attachments: Request for rulemaking.pdf
Flag: Follow up

Please see attached correspondence requesting rulemaking on CCPA.

Thank you,

Sheila Stine, JD

Chief Legal Counsel

www.eMDs.com

[REDACTED]
10901 Stonelake Blvd., Suite 200

Austin, TX 78759

CONFIDENTIAL

The information contained in this electronic message is confidential. It may also be subject to the attorney-client and/or work product privileges. This information is intended solely for the exclusive use of the individual or entity named above. If you are not the intended recipient, you are notified that the sender does not waive any privileges accorded to this information and that any use, disclosure, dissemination, distribution, copying or the taking of any action because of this information is strictly prohibited. If you have received this information in error, please immediately notify the sender by telephone or electronic mail to arrange for the return of the information.

***** This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error please notify the system manager. This footnote also confirms that this email message has

CCPA00001005

been checked for viruses with Microsoft Exchange Online Protection . In addition, eMDs, Inc. strongly discourages sending any form of confidential patient information as defined by HIPAA in the form of text, screen shots, or other formats via email messages. *****



March 6, 2019

BY EMAIL: privacyregulations@doj.ca.gov

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

Re: California Consumer Privacy Act Rulemaking

Dear Sir or Madam:

eMDs, Inc. and Aprima Medical Software and eMDs company combine leading technologies with tailored services to remove operational burden and empower healthcare providers to maximize the impact of their care. Founded by physicians, eMDs brings decades of expertise and understanding to our integrated electronic health records products, practice management software, revenue cycle management solutions, and credentialing services for medical practices and enterprises. eMDs and Aprima's extensive experience allows us to craft proven, transformative, solutions that meet the unique needs of healthcare organizations, enabling unmatched productivity and a superior experience for patients and practitioners alike.

As organizations entrusted with patient health records, we strongly support the objectives of the California Consumer Privacy Act (CCPA) and believe privacy deserves effective protection in the marketplace. We, however, have notable concerns around the likely negative impact on both its business and California consumers from the lack of clarity caused by the use of certain language in the CCPA.

We believe the law could be clarified through rulemaking to provide improved consumer protection and guidance to Businesses in two areas: (1) the application of the CCPA to employee data; and (2) the scope of the definition of "personal information."

I. Employee Data

**Expert Solutions.
Stronger Partners.
Healthier Patients.**

We request the Attorney General clarify that a "consumer" does not include an employee of the Business.

Section 1798.140(g) defines a "consumer" as "a natural person who is a California resident." Similarly, the provisions of the CCPA are triggered by the collection of a consumer's "personal information." To that end, section 1798(o)(1) defines "personal information" as "Personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Further, personal information includes "professional or employment-related information" if it "identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household." Section 1798.140(o)(1)(I). Accordingly, as hastily drafted, the CCPA could reasonably be read to include among the protected "consumers," employees of an organization, and that the "personal information" collected could include all the information gathered during their employment, including their entire employee file. We do not believe that this was the intent of the legislature.

As a starting point, there is nothing in the legislative history reflecting an intent to apply the CCPA to employee data. Indeed, the name of the law itself makes clear that its intent is to protect the privacy of individuals who fall under the common understanding of a consumer, i.e., an individual who buys products or services for personal, family or household purposes.

In addition, various provisions in the CCPA simply do not fit employment relationships and demonstrate that employees were not intended to be embraced by the definition of consumer:

- Section 1798.135 mandates that Businesses satisfy their core notice obligations by posting the notice on their public-facing website, without exception. This would be an inappropriate way to provide notice to employees, as employee notices usually take the form of provisions in an employee handbook, sharing information directly with the workforce, or posting notices in common areas such as break rooms.
- Section 1798.125, the anti-discrimination provision, prohibits the denial of goods or services to a consumer or the charging of different prices or rates for goods or services in response to a consumer's exercise of CCPA rights. The provision does not address workplace-related activities based on the exercise of CCPA rights.
- Section 1798.100 confers on consumers the right to request that a Business disclose all specific pieces of personal information that the Business has collected.

If this provision applied in the employment context, an employee could demand access both to a Business's sensitive or confidential information, such as internal email communications that merely reference the name of the employee or confidential sexual harassment complaints.

- Section 1798.105 confers on consumers the right to request that the Business delete their personal information. That right is incompatible with common workplace human resources practices. For example, such deletion would permit an employee to request deletion of disciplinary records (e.g. records of workplace harassment) that are outside of the statutorily prescribed retention period but potentially relevant to the workplace environment.

In these ways, the CCPA presents a sub-optimal framework for addressing employee data and was clearly not intended to apply in the employment context. Accordingly, we request that the Attorney General exercise his broad authority to issue regulations "to further the purposes of" the CCPA to clarify that a "consumer" as defined in section 1798.140(g) does not include an employee of the Business. Alternatively, to the extent that the Attorney General believes that this necessary clarification cannot be made through this rulemaking process, we urge the Attorney General to request that the legislature: (i) amend section 1798.140(g) of the CCPA to exempt employees from the definition of consumer and (2) amend section 1798(o)(1) to eliminate "professional or employment-related information."

II. Business Contact Information

We request the Attorney General clarify that the definition of "personal information" set forth in section 1798.140(o) does not include the name or business contact information provided by third-party employees or contractors in the regular course of business.

Vendor and service provider contracts are a part of everyday business practice for many Businesses. As part of those business interactions, employees and contractors of the third-party often provide contact information either on forms or as part of routine normal email correspondence. That contact information typically includes the contact's name, business telephone number, cell phone number, business email address, and business address. Based on a plain reading of the CCPA, it is unclear whether this type of business information is encompassed by the definition of personal information.

Ordinarily, an employee or contractor who provides their name and business contact information on behalf of a third-party service provider does not act as a "consumer" in the traditional sense of the word, i.e. as an individual who buys products or services for personal, family or household purposes. Instead, the

individual acts and provides information in solely in his or her capacity as a corporate representative. In effect, while the name and contact information are linked to a particular individual, that information is not truly "personal" to the individual, it is the information of the third-party company.

Nothing in the legislative history of the CCPA reflects an intent by the legislature to extend CCPA protections to business contact information. By contrast, reflecting this reality and its clear intent, the legislature amended section 1798.140(o) to limit personal information to that information that "identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household." Accordingly, we request that the Attorney General exercise his authority to further the purposes of the CCPA by issuing a rule clarifying that the definition of "personal information" set forth in section 1798.140(o) does not include the name or business contact information provided by third-party employees or contractors in the regular course of business.

Thank you for providing us with the opportunity to provide these comments at this stage of the rulemaking process. Should you have any questions or wish to discuss our requested clarifications, please do not hesitate to contact me.

Sincerely,



Sheila Stine
Chief Legal Counsel
eMDs, Inc.
Aprima Medical Software

Message

From: Shapiro, Mike [REDACTED]
Sent: 3/8/2019 4:30:47 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Response to Request for Comments for California Consumer Privacy Act
Attachments: County of Santa Clara Privacy Office - CCPA Response to Request for Comments (Signed).pdf

California Department of Justice, Privacy Regulations Coordinator,

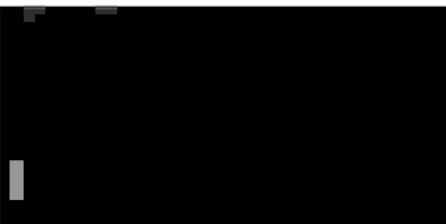
The attachment to this email (a copy is provided below) includes the County of Santa Clara Privacy Office's response to the California Attorney General's request for comments for the California Consumer Privacy Act (CCPA). If you have any questions or would like additional information about our comments, please let us know. We thank you for your time and consideration with this important task in protecting consumer privacy for Californians.

Thanks,

Mike Shapiro

Chief Privacy Officer

County of Santa Clara



NOTICE:

This e-mail message and/or its attachments may contain information that is confidential or restricted. It is intended only for the individuals named as recipients in the message. If you are NOT an authorized recipient, you are prohibited from using, delivering, distributing, printing, copying, or disclosing the message or content to others and must delete the message from your computer. If you have received this message in error, please notify the sender by return e-mail.

County of Santa Clara

Privacy Office



County of Santa Clara

Privacy Office

1555 Berger Dr., Building 2, 3rd Floor

San Jose, CA. 95112

DATE: March 8, 2019

TO: California Department of Justice

Privacy Regulations Coordinator

300 S. Spring St.

Los Angeles, CA. 90013

FROM: Michael L. Shapiro

Chief Privacy Officer

County of Santa Clara

SUBJECT: Response to Request for Comments for California Consumer Privacy Act

Dear Privacy Regulations Coordinator,

The passage of the California Consumer Privacy Act of 2018 (CCPA) marks a historic moment in privacy rights for California Consumers. Although the right of local District Attorneys and select city attorneys was removed from the legislation as the ballot initiative became law, our County of Santa Clara Privacy Office looks forward to partnering with your office in the future. We share the charter to protect the privacy rights of our respective and overlapping constituencies.

With regard to our input during the public comment period for the Attorney General's rulemaking procedures, we support the re-introduction of the private right of action as detailed in California Senator Hannah-Beth Jackson's SB-561. We believe the law must provide practical avenues for enforcement. The law, as it stands, only allows for a private right of action in the context of the specific circumstances of a data breach described in Section 1798.150. To share the burden of enforcement, the CCPA should be amended to explicitly allow consumers a private right of action for any violations of the law's provisions.

Also, we are concerned with the provisions for requests of household data and agree that an individual should not be able to request the information for other individuals within the household. Only data that is assignable to a household such as household income and utility usage should be available to all members of a household. Verifiable household identification will be troublesome for industry to implement technologically, and we believe maintaining privacy of individuals inside the household should be of primary importance as this technology and enforcement area evolves.

Additionally, the options for businesses to opt-out of a deletion request contain loopholes of concern to our office. Specifically, in section 1798.105, d, (6), the law allows a deletion request to be ignored if the data will be used to engage in public or peer reviewed scientific historical or statistical research in the public interest and the deletion request is likely to render impossible or seriously impair the achievement of such research. One of our concerns is that while the first consumer deletion request could not reasonably be declared to "render impossible the research", perhaps the 500th request may "render impossible the research". Therefore, the rights of the first consumer to delete her/his data is theoretically greater than the rights of the 500th consumer to make such a request, depending on the researcher's definitions of statistical significance, desired samples sizes, research design, etc. This clause presents a logical challenge for enforcement such that to provide equity to all consumers, the Attorney General must either allow all data collected for scientific research purposes to remain exempt from a deletion request or none of it. We believe the right to privacy and equal protection under the law should be balanced with research interests. As such, for identifiable records used in research, a consumer's verifiable request should be honored. For anonymized or aggregated records used in research, it would be at a business's discretion whether or not they can or would honor a verifiable consumer request.

A similar loophole exists in the deletion request section in 1798.105, d, (8) which allows a business to ignore a deletion request to “comply with a legal obligation”. This is a broad exception that could be applied to any number of scenarios that do not align with the spirit of the law. For example, if Social Media Company A has a legal contract with Advertising Company B, they could deny a consumer’s request to delete purely because of an existing commercial contract. This loophole renders parts of the section ineffective because all data sharing agreements could be considered “legal obligations” and therefore exempt from deletion requests. We recommend that “legal obligation” should be defined more specifically within General Guidance provided for businesses seeking to comply with the CCPA. Sample language could include:

Businesses may deny a consumer request to delete personal information in order to comply with a “legal obligation”. A “legal obligation” in this context means a court order, warrant, or federal/state/local law and does not include contracts or agreements.

Regarding verifiable consumer requests, we believe that the verification method should be proportional to the original identification of the consumer. For example, if a user ID and password are the original means by which a consumer creates an account, then possession of those two fields by a consumer should qualify as a verifiable consumer request. On the other hand, the Attorney General should discourage routine verification through government-issued identification, such as drivers licenses or passports in order to reduce the potential for collection of additional personal information and the burden of such collection on businesses. Such documents are often disproportionate to the method used by the consumer to create an account. Verification should also be context-specific and aligned with consumer expectations. This means that in general, as the sensitivity of information increases, the level of authentication required to qualify as a verifiable consumer request can also increase. In addition, businesses should allow consumers to make requests using the same mode under which information was originally collected or accounts were created. For example, if the business originally collected information over the phone from the consumer, there should be a phone number for consumers to call to ask about categories of data collected and specific data elements known to the business about the consumer.

In section 1798.140, the definition of business includes companies that annually buy, sell, or share the personal information of 50,000 or more consumers, households, or devices. This has given rise from many industry representatives stating that small businesses that simply maintain a website or mailing list will fall under the law. To address these complaints, the Attorney General should explicitly state that IP address alone, and used only for website experience and functionality, will not trigger the CCPA. However, if a business maintains a mailing list that couples email address with name, the 50,000 consumers, households, or devices threshold should still apply.

Thank you for your time and consideration in reviewing our comments. If you would like to discuss these further, we would be happy to meet or have a conversation as you proceed in developing regulations for the CCPA.

Sincerely,

A handwritten signature in blue ink that reads "Michael L. Shapiro". The signature is written in a cursive, flowing style.

Michael L. Shapiro

Chief Privacy Officer

County of Santa Clara

County of Santa Clara

Privacy Office

County of Santa Clara
Privacy Office
1555 Berger Dr., Building 2, 3rd Floor
San Jose, CA. 95112



DATE: March 8, 2019

TO: California Department of Justice
Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA. 90013

FROM: Michael L. Shapiro
Chief Privacy Officer
County of Santa Clara

SUBJECT: Response to Request for Comments for California Consumer Privacy Act

Dear Privacy Regulations Coordinator,

The passage of the California Consumer Privacy Act of 2018 (CCPA) marks a historic moment in privacy rights for California Consumers. Although the right of local District Attorneys and select city attorneys was removed from the legislation as the ballot initiative became law, our County of Santa Clara Privacy Office looks forward to partnering with your office in the future. We share the charter to protect the privacy rights of our respective and overlapping constituencies.

With regard to our input during the public comment period for the Attorney General's rulemaking procedures, we support the re-introduction of the private right of action as detailed in California Senator Hannah-Beth Jackson's SB-561. We believe the law must provide practical avenues for enforcement. The law, as it stands, only allows for a private right of action in the context of the specific circumstances of a data breach described in Section 1798.150. To share the burden of enforcement, the CCPA should be amended to explicitly allow consumers a private right of action for any violations of the law's provisions.

Also, we are concerned with the provisions for requests of household data and agree that an individual should not be able to request the information for other individuals within the household. Only data that is assignable to a household such as household income and utility usage should be available to all members of a household. Verifiable household identification will be troublesome for industry to implement technologically, and we believe maintaining privacy of individuals inside the household should be of primary importance as this technology and enforcement area evolves.

Additionally, the options for businesses to opt-out of a deletion request contain loopholes of concern to our office. Specifically, in section 1798.105, d, (6), the law allows a deletion request to be ignored if the data will be used to engage in public or peer reviewed scientific historical or statistical research in the public interest and the deletion request is likely to render impossible or seriously impair the achievement of such research. One of our concerns is that while the first consumer deletion request could not reasonably be declared to “render impossible the research”, perhaps the 500th request may “render impossible the research”. Therefore, the rights of the first consumer to delete her/his data is theoretically greater than the rights of the 500th consumer to make such a request, depending on the researcher’s definitions of statistical significance, desired samples sizes, research design, etc. This clause presents a logical challenge for enforcement such that to provide equity to all consumers, the Attorney General must either allow all data collected for scientific research purposes to remain exempt from a deletion request or none of it. We believe the right to privacy and equal protection under the law should be balanced with research interests. As such, for identifiable records used in research, a consumer’s verifiable request should be honored. For anonymized or aggregated records used in research, it would be at a business’s discretion whether or not they can or would honor a verifiable consumer request.

A similar loophole exists in the deletion request section in 1798.105, d, (8) which allows a business to ignore a deletion request to “comply with a legal obligation”. This is a broad exception that could be applied to any number of scenarios that do not align with the spirit of the law. For example, if Social Media Company A has a legal contract with Advertising Company B, they could deny a consumer’s request to delete purely because of an existing commercial contract. This loophole renders parts of the section ineffective because all data sharing agreements could be considered “legal obligations” and therefore exempt from deletion requests. We recommend that “legal obligation” should be defined more specifically within General Guidance provided for businesses seeking to comply with the CCPA. Sample language could include:

Businesses may deny a consumer request to delete personal information in order to comply with a “legal obligation”. A “legal obligation” in this context means a court order, warrant, or federal/state/local law and does not include contracts or agreements.

Regarding verifiable consumer requests, we believe that the verification method should be proportional to the original identification of the consumer. For example, if a user ID and password are the original means by which a consumer creates an account, then possession of those two fields by a consumer should qualify as a verifiable consumer request. On the other hand, the Attorney General should discourage routine verification through government-issued identification, such as drivers licenses or passports in order to reduce the potential for collection of additional personal information and the burden of such collection on businesses. Such documents are often disproportionate to the method used by the consumer to create an account. Verification should also be context-specific and aligned with consumer expectations. This means that in general, as the sensitivity of information increases, the level of authentication required to qualify as a verifiable consumer request can also increase. In addition, businesses should allow consumers to make requests using the same mode under which information was originally collected or accounts were created. For example, if the business originally collected information over the phone from the consumer, there should be a phone number for consumers to call to ask about categories of data collected and specific data elements known to the business about the consumer.

In section 1798.140, the definition of business includes companies that annually buy, sell, or share the personal information of 50,000 or more consumers, households, or devices. This has given rise from many industry representatives stating that small businesses that simply maintain a website or mailing list will fall under the law. To address these complaints, the Attorney General should explicitly state that IP address alone, and used only for website experience and functionality, will not trigger the CCPA. However, if a business maintains a mailing list that couples email address with name, the 50,000 consumers, households, or devices threshold should still apply.

Thank you for your time and consideration in reviewing our comments. If you would like to discuss these further, we would be happy to meet or have a conversation as you proceed in developing regulations for the CCPA.

Sincerely,



Michael L. Shapiro
Chief Privacy Officer
County of Santa Clara

Message

From: Jason Litchney [REDACTED]
Sent: 3/8/2019 2:44:29 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Jan Stieger [REDACTED]; David Reid [REDACTED]
Subject: RMAI Comments Regarding the CA Consumer Protection Act of 2018
Attachments: RMAI Comments Regarding the California Consumer Protection Act of 2018.pdf

Please see attached RMAI comments regarding the CA Consumer Protection act of 2018.

Regards,

Jason Litchney

Director of Marketing & PR

Receivables Management Association International



rmaintl.org

1050 Fulton Avenue, Suite 120

Sacramento, CA 95825



NOTICE: RMAI email addresses are issued to employees for the purpose of conducting official business of the corporation. Any correspondence inconsistent with the positions, policies, and procedures of RMAI are the personal opinions and views of those individuals for which RMAI does not accept liability.

March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Sent via email: privacyregulations@doj.ca.gov

Re: RMAI Comments Regarding the California Consumer Protection Act of 2018

Dear Privacy Regulations Coordinator:

The Receivables Management Association International ("RMAI") appreciates this opportunity to submit the following pre-rulemaking comments regarding the California Consumer Protection Act of 2018 ("CCPA").

I. BACKGROUND

RMAI is the nonprofit trade association that represents more than 500 companies that purchase or support the purchase of performing and non-performing receivables on the secondary market. The existence of the secondary market is critical to the functioning of the primary market in which credit originators extend credit to consumers. An efficient secondary market lowers the cost of credit extended to consumers and increases the availability and diversity of such credit.

RMAI is an international leader in promoting strong and ethical business practices within the receivables management industry. RMAI requires all of its member companies who are purchasing receivables on the secondary market to become certified through RMAI's Receivables Management Certification Program ("RMCP")¹ as a requisite for membership. The RMCP is a comprehensive and uniform source of industry standards that has been recognized by the collection industry's federal regulator, the Consumer Financial Protection Bureau, as "best practices."²

¹ RMAI, *RMAI Receivables Management Certification Program*, <https://rmaintl.org/certification> (last accessed March 2, 2019).

² Consumer Financial Protection Bureau, *Small Business Review Panel for Debt Collector and Debt Buyer Rulemaking, Outline of Proposals Under Consideration*, July 28, 2016, p. 38, http://files.consumerfinance.gov/f/documents/20160727_cfpb_Outline_of_proposals.pdf (last accessed March 2, 2019).

In addition to requiring that certified companies comply with local, state and federal laws and regulations concerning collection activity,³ the RMCP goes above and beyond the requirements of local, state and federal laws and regulations by requiring its member companies to comply with additional requirements not addressed by existing laws and regulations. The debt buying companies certified by the RMCP hold approximately 80 percent of all purchased receivables in the country, by RMAI's estimates.

RMCP certified companies are subject to vigorous and recurring independent third-party audits to demonstrate to RMAI their compliance with the RMAI Certification Program. This audit includes an onsite inspection of the certified companies to validate full integration of RMCP standards into the company's operations. Following a company's initial certification, review audits continue to be conducted every two to three years.

RMAI's Certification Program was recognized by a resolution of the Michigan State Senate as "exceed[ing] state and federal laws and regulations through a series of stringent requirements that stress responsible consumer protection through increased transparency and operational controls . . ."⁴

At the state level, since 2013, RMAI has worked with legislators and regulators in California, Connecticut, Colorado, Maine, Maryland, Minnesota, New York, Oregon, Washington and West Virginia toward the enactment of enhanced laws and regulations regarding the collection of purchased consumer debts.

II. RMAI COMMENTS ON THE CCPA

RMAI applauds California's enactment of the CCPA, providing consumers greater rights with respect to the collection, processing, sale and disclosure of their personal information. While the CCPA will likely undergo additional amendments before its effective date, RMAI appreciates this opportunity to provide the Department of Justice with pre-rulemaking comments on several definitions it believes would benefit from clarification.

A. Section 1798.140(t) – Definition of "Sell," "selling," "sale," or "sold."

³ The federal laws to which member companies are subject include but are not limited to the Fair Debt Collection Practices Act, Fair Credit Reporting Act, Gramm-Leach-Bliley Act, Electronic Funds Transfer Act, Telephone Consumer Protection Act, and the Health Insurance Portability and Accountability Act.

⁴ Michigan Senate Resolution 33, adopted March 26, 2015.

[https://www.legislature.mi.gov/\(S\(c0f55hrzl15jmuaxb4uv0gf\)\)/mileg.aspx?page=getobject&objectname=2015-SR-0033&query=on](https://www.legislature.mi.gov/(S(c0f55hrzl15jmuaxb4uv0gf))/mileg.aspx?page=getobject&objectname=2015-SR-0033&query=on) (last accessed March 2, 2019).

It should be clarified that the definition of these terms applies only when the primary object of the “sale,” i.e., the thing of value for which “monetary or other valuable consideration” is received, is the personal information itself.

This clarification would address the common situation in which a consumer’s contractual obligation is sold, typically as part of a portfolio, and it is the value of the obligation rather than the consumer’s associated personal information that is the object of the sale.

This concern was raised at the Sacramento and Riverside Public Hearings:

Many financial institutions regularly sell portfolios within their business. So for example, a credit card portfolio or a loan portfolio, another example would be like a delinquent account portfolio. In those cases the personal information associated with those accounts is transferred with the commercial sale of that portfolio. The terms of that customers’ contract don’t change. It would really be helpful if the regulations would clarify that selling those types of portfolios -- portfolios of that nature and transferring the corresponding personal information to some commercial purchasers excluded from the definition of sale. These types of commercial sales are common in the financial industry, and they don’t impact the customers directly.⁵

As written, the act does not apply to personal information collected, sold, processed, or disclosed pursuant to GLBA. Many financial institutions regularly sell portfolios within their businesses, and in doing so, consumer personal information is transferred with the commercial sale of the portfolio. Although the individual transactions that are part of the portfolio are protected by GLBA, the sale of the portfolio itself, such as a credit card portfolio or a delinquent account portfolio, does not appear to technically fall within this exclusion. It would be helpful if the regulations excluded from the definition of sale the selling of these types of portfolios and transferring of corresponding personal information to the commercial purchaser.⁶

⁵ Transcript, *Public Hearing on the California Consumer Privacy Act (CCPA)*, Riverside, CA, January 24, 2019, p. 9. <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-riverside-012419.pdf>? (last accessed March 3, 2019).

⁶ Transcript, *Public Hearing on the California Consumer Privacy Act (CCPA)*, Sacramento, CA, February 5, 2019, p. 52. <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-sac-020519.pdf>? (last accessed March 3, 2019).

The CCPA defines sale to include any data transfer for monetary or other valuable consideration. It's not clear whether the monetary consideration must be received for the purchase of personal data as opposed to some other business arrangement where the data is not the subject of the exchange.⁷

The receivables secondary marketplace is where ownership of performing and nonperforming receivables (i.e. the asset) are purchased by companies that were not a party to the originating transaction. A common example "is when a bank sells the ownership of its defaulted credit card receivables to a debt buying company. As a result of the sale, the ownership of the receivables and all legal rights associated with that asset are now held by a company not a party to the original transaction."⁸

The secondary marketplace benefits original creditors by allowing them to monetize performing and nonperforming receivables, thereby allowing for business growth and the extension of new lines of credit. Consumers likewise benefit because the "receivables secondary market provides consumers who have defaulted on a debt the single most expedient, efficient, and cost-effective way to improve their credit rating," providing the greatest opportunity during the life of the debt to settle the account for the lowest amount.⁹

If a consumer's right to opt-out of the sale of their personal information under the CCPA is wrongly interpreted to disallow the transference of the consumer's personal information associated with the sale of their legal obligation, their de-identified legal obligation would be virtually unenforceable. This would disable the receivables secondary marketplace and potentially lead to the abandonment of portfolios. "This outcome would leave the consumer with no solution to resolve the contractual obligation on the account, make payments, repair their credit rating, dispute the debt, bring legal action, or even to protect their confidential information from falling into the wrong hands."¹⁰

For these reasons, RMAI respectfully requests clarification that a "sale" of personal information does not occur when it is the obligation with which it is associated that is the asset for which "monetary or other valuable consideration" is received.

⁷ *Id.* at p. 30.

⁸ RMAI, *The Value of Resale on the Receivables Secondary Market*, April 2016, p. 3.
https://rmaintl.org/wp-content/uploads/2017/04/RMA_White_Paper_Value_of_Resale.pdf (last accessed March 3, 2019).

⁹ *Id.* at pp. 6-78.

¹⁰ *Id.* at 9.

B. Section 1798.140(c) – Definition of “Business.”

To meet the definition of a “business” under the CCPA, an entity must be one that “does business in the State of California” *and then* meets one of the three specified thresholds. In other words, it is a prerequisite that the entity be doing business in California. If that prerequisite is not met, it is irrelevant whether the entity also meets one or more of the thresholds.

Unfortunately, there is no definition provided for “does business in the State of California.” This lack of clarity leaves foreign corporations without guidance as to whether their level of activity in California constitutes “doing business” in the state.

Fortunately, California has several statutes that deal directly with this question. Cal. Rev. & Tax Code § 23101 provides a specific definition for “doing business” with respect to potential franchise tax liability, and Cal. Corp. Code § 191 defines what it means to be “transacting intrastate business” for purposes of requiring a certificate of qualification.

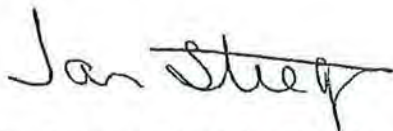
For these reasons, RMAI respectfully requests clarification on the meaning of “does business in the State of California.”

III. CONCLUSION

RMAI thanks the California Department of Justice for its consideration of these comments and looks forward to the Department's future rulemaking.

Please let us know if you have questions or if we can be of any assistance.

Sincerely,



Jan Stieger, Executive Director
Receivables Management Association International

Message

From: Sara Kloek [REDACTED]
Sent: 12/26/2018 8:30:18 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Christopher Mohr [REDACTED]
Subject: SIIA letter on CCPA
Attachments: SIIA Letter to CA AG Becerra.pdf
Flag: Follow up

To whom it may concern,

You will find a letter attached from the Software & Information Industry Association regarding operational concerns in the education space related to the recently passed California Consumer Privacy Act.

Thank you,

Sara Kloek

Director of Education Policy

SIIA

The Honorable Xavier Becerra
Attorney General, State of California
1300 I Street
Sacramento, CA 95814

Via Email to: Eleanor Blume [REDACTED] and privacyregulations@doj.ca.gov

Dear Attorney General Becerra,

On behalf of the Software and Information Industry Association (SIIA), I write in regard to the conflicts between the Family Educational Rights and Privacy Act (FERPA), the Student Online Personal Information Protection Act (SOPIPA), section 49073.1 of California's Education Code (AB 1584), and the California Consumer Privacy Act (CCPA). Nearly 200 of our members are working with schools in California to develop and deliver software applications, digital instructional content, online learning services, and related technologies. Many of these technologies use student information to help educators improve student outcomes.

Our members serve schools in a number of ways. Some provide online curriculum, some provide administrative tools such as cloud-based grade books and student information systems, and others provide hardware that help students connect to a diverse collection of educational materials.

SIIA appreciates the work California legislators, regulators, schools, and companies have done to protect student privacy and request clarification on the intersection of these laws. We are writing because the recently enacted CCPA creates conflicts with existing student privacy laws in ways that the legislature could not possibly have intended. This letter is intended to identify the conflicts between the CCPA and existing law, and to propose language that resolves potential confusion.

Student Privacy is Regulated by California Law and Federal Statutes

California, starting with student privacy legislation in 2014 and, more recently, comprehensive consumer privacy legislation, has been a leader in privacy. Unfortunately, the CCPA has created conflicts with existing student privacy legislation resulting in a lack of clarity for schools, parents, and education technology companies. (This letter will use "edtech companies" or "edtech" throughout instead of using the terms used in the specific laws such as third parties, online educational services, businesses, and operators.). When working at the direction of schools – public and private; K-12 and post-secondary – our companies are under strict and overlapping legal obligations to protect student privacy.

First, the federal Family Educational Rights and Privacy Act (FERPA), restricts how schools may share student education records and student personally identifiable information as a condition of receiving

federal funds.¹ FERPA therefore governs most public K-12 schools, some private K-12 schools, and most public and private institutions of higher education. Substantively, FERPA generally requires affirmative parental consent before any release of a student's personal information, and provides parents with the right to inspect educational records, and challenge inaccuracies in those records in appropriate circumstances.²

Narrow exceptions to the consent requirement exist that enable key educational functions. For example, FERPA's "school official exception" allows schools to outsource institutional services or functions to contractors (e.g., bus drivers), volunteers, or other third parties but only if those actors perform a function that would otherwise be done by school employees. In addition, the school must *directly* control such an actor's use and maintenance of education records, and the school is responsible to ensure that such an actor only uses personally identifiable information for narrow and school-related purposes for which the information was disclosed.³ Finally, if the school is using the school official exception to disclose information without consent, it must tell parents about the fact that the school is using the exception.⁴ Consequences for both an ed tech company and the school of any privacy violation are severe: If a vendor violates the non-disclosure requirements of FERPA, the school cannot provide access to personal information for at least five years.⁵

California has enacted two separate statutes that supplement FERPA's protection. First, AB 1584 enhances FERPA's protection by requiring schools (or "local educational agencies," in the parlance of the statute) to include privacy-protective provisions in their agreements with ed tech companies. More specifically, AB 1584 mandates that contracts between schools and edtech companies bar edtech companies from using student records for purposes other than those permitted by that contract. Among other things, the contract must include a "certification that a pupil's records shall not be retained or available upon completion of the terms of the contract and a description of how that

¹ 20 U.S.C. § 1232g; 34 CFR Part 99

² See 20 U.S.C. § 1232(g).

³ 34 CFR Part 99.31 (a) (1)(i)

⁴ 34 CFR Part 99.31 (a)(1)(ii)

⁵ 20 U.S. Code § 1232g (b) (4) (B). The Department of Education has supplemented FERPA's statutory and regulatory provisions with guidance on using edtech in the classroom that clarifies best practices on how schools should effectively exercise direct control over the use and maintenance of education records and related PII by ed tech companies. These practices include suggestions for data deletion and destruction, a process to facilitate parental access to the information through the school, and requirements to use personal information only for purposes outlined in the agreement with the school. See https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf; https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TOS_Guidance_Mar2016.pdf

certification will be enforced” and an explicit prohibition on using student information (“pupil records”) to engage in targeted advertising.⁶

While AB 1584 and FERPA regulate schools, SOPIPA directly regulates educational technology companies. SOPIPA prohibits edtech (or anyone else) from knowingly engaging in targeted advertising to students or parents, using covered information to amass a profile about a K-12 student, selling student information, or disclosing covered information.⁷ It also requires companies to maintain reasonable security procedures and practices, and delete information if requested by a school or district.⁸

Read together, SOPIPA, AB 1584, and FERPA’s requirements recognize the unique relationship between an edtech company and a school and establish guardrails for the use of student data that are both protective of student privacy and tailored to the educational context. Both AB 1584⁹ and FERPA¹⁰ include provisions that require the school or the contract between a school and a vendor to set procedures for the parent or student to request access to student records. SOPIPA prohibits the sale of covered information, and the creation of profiles. We do not believe that the legislature intended the CCPA to interfere with the operation of these statutes. But unfortunately, that is exactly what the CCPA does.

The CCPA Creates Conflicting Compliance Obligations and Direct Operational Concerns for Companies Operating in Education.

The CCPA establishes the rights of California residents to access, deletion, and porting of personal data from certain “businesses.” Included in the definition of “personal information” is “education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act.”¹¹ As many edtech companies will meet the definition of “business,” edtech companies have ensuing obligations including transparency,¹² opt-out,¹³ and deletion on request.¹⁴

When they are acting in the educational sector, CCPA places edtech companies in the impossible position of choosing between compliance with two different statutory regimes: one designed specifically for the education sector, and one applicable to consumers generally. For example, FERPA

⁶ Cal. Ed. Code § 49073.1 (b)

⁷ Cal. B.&P. Code § 22584 (b).

⁸ Cal. B.&P. Code § 22584 (b) (4)(E)

⁹ Cal. Ed. Code § 49073.1.

¹⁰ 34 CFR 99.10

¹¹ Cal. Civ. Code § 1798.198(a)

¹² Cal. Civ. Code § 1798.110 (a)

¹³ Cal. Civ. Code § 1798.120 (a)

¹⁴ Cal. Civ. Code § 1798.105

gives parents and eligible students the right to inspect and amend educational records maintained by the school. FERPA, does not, however, give parents and eligible students the right to request deletion of their student's education record. The CCPA gives consumers the right to request deletion of personal information from a business. It is not clear, however, how an edtech company that is maintaining education records under a contract with a school district must respond if a student contacts the company to request deletion of their information. Should a company uphold the terms of their contract with a school which conforms to FERPA, AB 1584, and SOPIPA requirements? Or should the company adhere to the requirements of CCPA and delete the information without the school knowledge?

Similarly, SOPIPA requires deletion of covered information "if *the school or district* requests deletion of data under the control of the school or district."¹⁵ And AB 1584 expressly provides that contracts with edtech companies ensure that all pupil records "continue to be the property of and under control of the local educational agency."¹⁶ It also mandates that the contracts describe a means for pupils to retain control of "pupil-generated content," except for standardized assessments where pupil access would jeopardize the utility of those tools.¹⁷

FERPA, SOPIPA, and AB 1548 represent strong and context-specific privacy rules that recognize that in the educational sector, edtech companies will very often have no direct legal relationship with the person that the CCPA treats as the "consumer." Nonetheless, all of this information, as well as the edtech companies operating in this space, are subject to the CCPA's obligations. SIIA members are also concerned about the CCPA's application to the security of standardized assessment tools—not just in K-12 educational assessments, but also in higher education, healthcare, professional certification, government licensure, and academic admission.

We respectfully request that these operational issues for edtech companies and schools are clarified before the effective date of the CCPA. In the Appendix to this letter, SIIA details a number of proposed amendments to the law that would address these concerns. We respectfully request a meeting with you or your staff to discuss these issues. In the interim, please do not hesitate to contact Chris Mohr at [REDACTED] and Sara Kloeck at [REDACTED] if we may be of assistance.

Sincerely,



Ken Wasch
President & CEO
Software & Information Industry Association

¹⁵ Cal. B & P Code 22584 (d)(2) (emphasis supplied).

¹⁶ Cal. Ed. Code 49073.1. (c)(4).

¹⁷ *Id.* (d)(4)

APPENDIX: AMENDMENTS

The protections afforded to California residents, such as access and deletion, through the CCPA are already included in the frameworks of federal and state student privacy laws. The amendments that follow are based on the specific operational problems that the CCPA poses in the educational sector:

- Edtech companies act as service providers to the schools and do not have a direct relationship with the student or the parent. The CCPA does not take account of this reality. A company must provide service to a “business” in order to qualify as a service provider under the bill, and schools, not-for-profits, or other governmental entities do not meet the statute’s definition of “business.”
- AB 1584 imposes specific requirements to protect pupil personal information in contracts between a school and an edtech company. An edtech company should not have to choose between violating legally valid contract clauses required by AB 1584 and CCPA compliance.
- The definition of “personal information” could be read to apply to information acquired by edtech companies not just in the kinds of standardized tests used in grade schools, but also in other fields, such as those that use standardized tests for professional certification and testing.

1. Clarify Definition of Service Provider

This amendment would clarify that companies acting on behalf of another entity (such as a government entity) qualify as a service provider so long as their activity consists of providing services under a contract that meets the requirements outlined by the bill. It is also intended to ensure that the service provider does not face liability when it acts as for a business either with respect to deletion, opt-out, or notice so long as it is acting as the instrument of a business. The amendment also deletes redundant language regarding “retaining and using.” That deletion is not intended to change the statute’s effect.

1798.140.

(v) “Service provider” means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects or processes information on behalf of ~~a business and to which the business discloses a consumer’s personal information for a business purpose~~ another entity, including a for-profit or nonprofit, or federal, state or local governmental entity, pursuant to a written contract with such an entity, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title.

~~required by law, or specified by such entity, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business. A service provider shall not be deemed a "business" under this title to the extent that the collection, processing sale or use of personal information by the service provider is done only: (1) as a service provider for and on behalf of another entity; and (2) for the purposes of performing the services specified in the contract with such entity or otherwise permitted by this title, required by law, or directed by such entity.~~

2. Clarify that a business need not breach its contracts to comply with the CCPA

This amendment would clarify that companies performing their duties under a written contract qualify for the exemption under 1798.105.

1798.105

(d)(8) "legal obligation, including a contractual obligation."

3. Clarify that standardized assessments and responses do not need to be disclosed where validity and reliability would be compromised

Assessments are critical in assessing learning in the education area, diagnosing medical issues in the health area, and evaluating competency in a number of other areas. Demonstrating competence ensures many public benefits –including health and safety – by proving that individuals who must be licensed or certified to practice a trade or profession in a State have objectively shown they have the necessary knowledge and skills to competently perform their jobs. In other circumstances, such demonstration of competence can be an important consideration in admission to secondary school, college or graduate school, or the satisfaction of academic requirements or meeting the standards for a certification required by employers in any number of fields. Access to a standardized assessment and answers outside of the testing environment can materially affect the integrity of the assessment process. To those for whom they are conducted, as well as for the countless others who rely upon their integrity in many different ways, these tests are matters of consequence. It can cost thousands of dollars to develop a single valid test question and answer. It is vital to not mandate disclosure where the validity and reliability of the assessment would be impaired.

AB 1584 recognizes this fact by excluding certain assessments from the definition of "pupil-generated content" that would otherwise be required to be given to the student, and the "reliability and validity" language in the suggestion below is drawn from that statute. Compare Cal. Ed. Code 49073.1 (d)(4) (definition of pupil generated content).

A new 1798.145(g) (renumber subsequent sections accordingly):

This title does not require a business to disclose a standardized assessment or a consumer's

specific responses to the assessment where consumer access, possession or control would jeopardize the validity and reliability of that assessment.

4. **Delete 1798.140(o)(1)(J) (educational information in the definition of personal information) and renumber accordingly**

As mentioned above, existing law pervasively regulates the acquisition and use of information in the education space. While this change in and of itself would not undo the conflicts with other laws due to the breadth of the CCPA's definition of "personal information", when read against the other changes to the statute it will help clarify the legislature's intent not to interfere with the ordinary operations of schools.

Message

From: Sara Klock [REDACTED]
Sent: 3/8/2019 2:30:53 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: SIIA letter on education and CCPA
Attachments: SIIA Letter to Becerra March 8 2019.pdf

Please see the attached letter from the Software & Information Industry Association.

Thanks and have a great Friday,

Sara

Sara Klock

Director of Education Policy, Programs, and Student Privacy

SIIA - The Software & Information Industry Association
1090 Vermont Ave NW, Sixth Floor, Washington, DC 20005
[REDACTED]

siiia.net/policy

March 8, 2019

The Honorable Xavier Becerra
Attorney General, State of California
1300 I Street
Sacramento, CA 95814

Dear Attorney General Becerra,

We are writing to follow up on our [original comments](#) submitted to your office on 12/26/2018 and the public comment made on 2/5/2019 at the Sacramento public forum. Deputy Attorney General Lisa Kim requested we write in to outline why our concerns are not addressed by 1798.145 in the California Consumer Privacy Act (CCPA).

Section 1798.145 of the CCPA states that “the obligations imposed on businesses by this title shall not restrict a business’s ability to comply with federal, state, or local laws.” Section 1798.145 does not address the contractual relationship, restrictions, and requirements in a service provider arrangement. The CCPA fails to consider the relationship involving a vendor servicing a contract to a school, state, or local government. It is unclear if this relationship would fall within the CCPA’s definition of “service provider” or if it is outside of the scope of the law. State and federal laws such as California’s Student Online Personal Information Protection Act (SOPIPA) and the federal Family Educational Rights and Privacy Act (FERPA) already heavily regulate the use of educational technology companies. There is a strong potential for confusion and conflict with contracts established between an educational technology vendor and the school or state/local government agencies, as well as the legitimate educational interests and the direct control that schools and state/local government agencies are to have over student records by law. A vendor deleting data or responding to an information or access request under the CCPA could violate contractual obligations imposed on a business that is collecting and processing personal information under the direction and control of a school, state/local governmental agency or other entity in strict compliance with existing laws. The school has certain statutory duties to maintain data. That is why deletion requests should be handled through and by the school, as provided by SOPIPA. And the school may have a legitimate interest in having an educator handle a request for access to education records instead of a vendor because it would be helpful to provide additional details and explanation by an educator that a vendor may not be able to provide.

Section 1798.185 authorizes the Attorney General to establish “any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights...” The clear conflict between CCPA and the student privacy

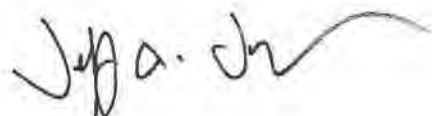
framework established by laws like SOPIPA, AB 1584, and FERPA would warrant an exception. If a company is subject to and in compliance with SOPIPA, AB 1584, or FERPA, the company should be exempt from compliance with CCPA. To be clear, the educational technology industry is not asking for exceptions when there is a direct relationship between the business and the consumer. In that instance, the company would need to follow the requirements of the CCPA.

We are also concerned about having to provide a copy of responses to test questions and related information under the CCPA and believe that an exception is needed to protect trade secret and copyrights in tests and the integrity of academic, certification, and licensure testing programs (including those which may be established pursuant to law). Having to provide information about, and a copy of, test responses by an individual could provide clues about the content of a test and compromise the utility, value, integrity, and validity of the test. It raises the prospect of giving an unfair advantage for some test takers who are able to receive information about the test and jeopardizing legitimate use of test results as measures of knowledge, skills, competence, or academic achievement. Release of information that provides clues about test questions could necessitate developing new test questions, which is a lengthy and costly process.

SIIA included suggested alternative statutory language in the original comment letter – and we suggest including an exception in order to protect intellectual property and trade secret rights and the security and integrity of tests consistent with AB1584 (Buchanan). We also note that there is an express GDPR [exception](#) under the UK Data Protection Act (2018) for test responses.

Please do not hesitate to contact Sara Kloek at skloek@siia.net if we may be of assistance.

Sincerely,



Jeff Joseph
President & CEO
Software and Information Industry Association

Message

From: James Harrison [REDACTED]
Sent: 3/8/2019 10:31:11 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Submission by Californians for Consumer Privacy
Attachments: 3.8.19 CCP Letter to AG re Proposed Regulations (00374326xAE03).pdf

Attached please find a submission on behalf of Californians for Consumer Privacy. Thank you for your consideration of CCP's comments and proposed regulations.

James C. Harrison

Remcho, Johansen & Purcell, LLP

1901 Harrison Street, Suite 1550

Oakland, CA 94612


[REDACTED]
[REDACTED]
[REDACTED]

CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.




Remcho Johansen & Purcell LLP

1901 Harrison Street
Suite 1550
Oakland CA 94612


www.rjp.com

March 7, 2019

James C. Harrison


Privacy Regulations Coordinator
Department of Justice
300 S. Spring Street
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

Re: Comments and Proposed Regulations Regarding the California Consumer Privacy Act

Dear Privacy Regulations Coordinator:

On behalf of Californians for Consumer Privacy, the sponsor of the California Consumer Privacy Act of 2018 (the "CCPA"), we would like to thank the Attorney General's Office for its dedication to protecting consumer privacy, holding businesses accountable for violating consumers' privacy rights, and implementing the CCPA. We respectfully submit the following comments and proposed draft regulations for your consideration.¹

In considering proposed regulations, we urge the Attorney General to ensure that:

- (1) Californians can learn what personal information a business collects about them and how they use it in a safe and secure manner;
- (2) Californians can easily exercise the right to say no to the sale of their personal information;
- (3) Californians can exercise the right to instruct a business to delete their personal information in a safe and secure manner; and
- (4) businesses are barred from penalizing consumers who exercise their rights under the CCPA.

Consistent with these rights, we believe the top four priorities for the Attorney General's rulemaking should be to: (1) make it clear and easy for consumers to opt out of the sale of their personal information; (2) ensure that consumers may obtain access to their personal information, or delete the information the business has collected from them, by submitting a verifiable consumer request that can be authenticated by businesses, such as through the use of a password-protected account for consumers

¹ We have previously submitted copies of these same regulations by email.

who maintain an account with the business, dual factor authentication, challenge-response authentication, or other similar means of verifying that the consumer who is making the request is the consumer about whom the request is made; (3) ensure that any financial incentives offered by businesses for the sale of consumers' personal information do not create a pay-for-privacy system by tying participation in discount and loyalty programs to the average value of consumers' data to the business; and (4) clarify the scope and application of the business purpose exception, including by requiring a service provider to "silo" personal information it receives from a business about a consumer from personal information it receives about the same consumer from another person or from its own interactions with that consumer. Attached are proposed regulations that address each of these priorities.

We would also like to take this opportunity to address several comments made about the CCPA at the Attorney General's privacy forums and in recent legislative hearings.

First, several commenters have suggested that pseudonymized information was unintentionally excluded from the exception for aggregate and deidentified information; in fact, we intentionally drafted the law to omit pseudonymized information from the exception for aggregate and deidentified information, because, by definition, it can be related back to a specific consumer and therefore does not afford consumers' sufficient protection.

Second, several commenters have raised questions about the potential liability of third parties under section 1798.115(d); once again, this provision was intentionally crafted to ensure that the default state was that third parties could not sell consumers' personal information unless they verified that the business from which they received the data provided consumers with express notice and the opportunity to opt out.

Third, some speakers have suggested that the CCPA does not offer businesses a safe harbor from liability for data breaches. This is simply false. In fact, the CCPA affords businesses three means by which they can protect themselves against liability for a data breach: (a) a business can encrypt consumers' personal information, a best practice for businesses that hold consumers' personal information; (b) a business can redact consumers' personal information so that it cannot be used to identify an individual consumer; and (c) a business can protect itself against liability by implementing and maintaining reasonable security procedures and practices appropriate to the nature of the information the business maintains. Cal. Civ. Code § 1798.150(a).

Fourth, some speakers have suggested that CCPA erred in not creating a separate, more sensitive category of personal information, as the European GDPR does. In fact, the authors of CCPA intended that personal information be broadly defined, rather than segmenting it into “sensitive” and “less sensitive” categories specifically because information is “less sensitive” to one consumer may be “sensitive” to another. For example, geolocation data may not be sensitive to a consumer who lives in a retirement community, but it could be a matter of life and death for someone leaving an abusive relationship.

Fifth, opponents have charged that the lack of specificity around ‘specific pieces of information’ is a flaw. Again, this was intentional, and the CCPA tasks the Attorney General with the responsibility to: (1) update the categories of personal information (Cal. Civ. Code § 1798.185(a)(1)); (2) establish “rules [and] procedures to ensure that . . . information businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer” (*id.*, § 1798.185(a)(6)); and (3) “establish[] rules and procedures to further the purposes of Sections 1798.110 and 1798.115” The authors of the CCPA intended to allow the Attorney General to define “specific pieces of information,” within the broad parameters of that phrase, and not, as some have suggested, to limit disclosure only to “categories” of information.

Sixth, speakers have charged that CCPA needs to be fixed to ensure that an employee is not able to request the deletion of his or her employee file just as the employee is about to be terminated. Given that Civil Code section 1798.105(d)(8) allows a business to ignore a deletion request in the event the business needs the information to “[c]omply with a legal obligation,” this fix is not necessary, as the legal authority to prevent deletion (compliance with labor laws) is already included in the CCPA. Additionally, with respect to employer-employee issues, section 1798.105(d)(9) addresses the subject completely, i.e. the business does not have to honor a deletion request in the event that the business maintains the information to “[o]therwise use the consumer’s personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.” Even if one made the argument that an employee was a consumer with respect to the business, then clearly s/he expected his or her personal information to be collected by the business for employment purposes.

Finally, one speaker suggested that a 16-year-old high school student could request that her school delete her grades. However, public schools and nonprofits (which would include parochial and every other private school with which we are familiar) are exempt from the law so unless a student attends a for-profit high school, she cannot request that the school delete her grades.

Privacy Regulations Coordinator
March 7, 2019
Page 4

On behalf of Californians for Consumer Privacy, thank you for your consideration of these comments and the proposed regulations

Sincerely,

A handwritten signature in blue ink, appearing to read "James C. Harrison", with a large, stylized initial "J" and a long, sweeping horizontal stroke at the end.

James C. Harrison

JCH:NL
Attachments
(00374112-2)

PROPOSED REGULATIONS TO IMPLEMENT RIGHT TO OPT-OUT

BACKGROUND

Right to opt-out

Section 1789.120 authorizes a consumer to opt-out of the sale of the consumer's personal information. A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information, has not received consent to sell the minor consumer's personal information, is prohibited from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.

Right of Consumer to Use Authorized Agent

Section 1798.135(c) authorizes a consumer to authorize another person to opt-out of the sale of the consumer's personal information on the consumer's behalf.

Obligation of businesses to comply with right to opt-out

Section 1798.135 requires businesses to notify consumers of the right to opt-out of the sale of the consumer's personal information and to refrain from selling the personal information of consumers who have opted-out. It also requires businesses to respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information, and it prohibits businesses from using any personal information collected from the consumer in connection with the submission of the consumer's opt-out request for any purpose other than complying with the opt-out request.

Section 1798.135(c) requires a business to comply with an opt-out request received from "a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General."

Attorney General's obligations with respect to right to opt-out

Section 1798.185(a)(4) requires the Attorney General to adopt rules and regulations to: (1) facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information; (2) govern businesses' compliance with a consumer's opt-out request; and (3) develop a recognizable and uniform opt-out logo or button for use by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

PROPOSED REGULATIONS¹

Use of Opt-Out Agent

A consumer aged 16 or more may authorize another person to opt-out of the sale of the consumer's personal information on the consumer's behalf. A business shall comply with an opt-out request submitted by a person on behalf of the consumer.

Opt-Out Notice

(a) Businesses shall maintain an opt-out button or logo that reflects the opt-out status of the consumer.

(b) If the consumer has opted-out of the sale of the consumer's personal information, the button or logo shall notify the consumer that the business is not selling the consumer's personal information, through a method of display that is clear and obvious to the consumer as to the opt-out status of that consumer, including but not limited to by making the button inactive and displaying a message that the consumer has already opted-out of the sale of their information.

(c) If the consumer has not opted-out of the sale of the consumer's personal information, or if the business is unable to identify the consumer, the opt-out button or logo shall be active so that the consumer may elect to opt-out of the sale of the consumer's personal information.

Opt-Out Notice – 12-Month Bar

Businesses shall not ask a consumer whom the business can identify, or probabilistically identify, and who has opted-out of the sale of their information, to consent to the sale of their information for twelve months following the date the consumer most recently opted-out of the sale of the consumer's personal information, regardless of whether the business interacts with the consumer online or in-person.

¹ To the extent that the proposed regulations use terms defined by the CCPA (e.g., consumer, person, etc.), the definitions set forth therein shall apply to the regulations.

PROPOSED REGULATIONS TO IMPLEMENT VERIFIABLE CONSUMER REQUEST

BACKGROUND

What does a verifiable consumer request apply to?

A consumer must submit a “verifiable consumer request” in order to exercise the consumer’s rights to obtain information about a business’s collection and use of a consumer’s personal information and to request deletion of a consumer’s personal information, as follows:

Sec. 1798.100: Right to request disclosure of: (1) categories of personal information collected and (2) specific pieces of information collected. *(Note that this overlaps with the right in section 1798.110 to request the disclosure of categories of personal information collected and specific pieces of personal information, but section 1798.100 has its own compliance provisions while compliance with section 1798.110 is governed by Section 1798.130. See the note in “What obligations do businesses have with respect to verifiable consumer requests?”, below, for a recommendation about how to address this.)*

Sec. 1798.105: Right to request that a business that has collected personal information from a consumer delete that personal information, unless an exception applies.

Sec. 1798.110: Right to request disclosure of: (1) categories of personal information collected, (2) categories of sources from which personal information is collected, (3) the business purpose or commercial purpose for collecting or selling the consumer’s personal information, (4) the categories of 3rd parties with whom the consumer’s personal information is shared, and (5) specific pieces of personal information.

(Note that section 1798.110(b) requires disclosure pursuant to 1798.130(a)(3), which only addresses disclosure of categories of personal information collected; however, because section 1798.110(a) and (b) establish the right to request such information and the obligation to disclose the information, the Attorney General’s regulation should address all of the information specified in subdivision (a) of section 1798.110.)

Sec. 1798.115: Right to request that a business that sells a consumer’s personal information, or that discloses it for a business purpose, disclose the categories of personal information collected, the categories of personal information sold, the categories of 3rd parties to whom the personal information is sold, the categories of personal information disclosed for a business purpose, and the categories of 3rd parties to whom the personal information is disclosed for a business purpose.

(Note that section 1798.115(a) does not require disclosure of the categories of 3rd parties to whom the personal information is disclosed for a business purpose, but subdivision (b) of section 1798.115 requires compliance with section 1798.130(a)(4), which requires a business to disclose the categories of 3rd

parties to whom the personal information is disclosed for a business purpose, in addition to the categories of 3rd parties to whom the information is sold. The Attorney General's regulations should therefore include disclosure of the categories of 3rd parties to whom the consumer's personal information is disclosed for a business purpose, in addition to the categories of third parties to whom the information is sold.)

What is the definition of a verifiable consumer request?

Sec. 1798.140(y) defines a "verifiable consumer request" as "a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf."

(Note that this definition does not cross-reference section 1798.100, but because that section uses the same term, the Attorney General's regulations should apply equally to requests made pursuant to section 1798.100.)

What obligations do businesses have with respect to verifiable consumer requests?

Section 1798.100, which allows a consumer to request disclosure of the categories of personal information and specific pieces of personal information collected about the consumer by a business, requires a business to "promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable [format] and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period."

(Note that, unlike section 1798.130, which requires that the information be provided within 45 days [with an additional 45 day extension if reasonably necessary], section 1798.100(d) does not impose an express time limit. In addition, it does not address a business's obligation to verify a request. Given the overlap between sections 1798.100 and 1798.110, however, the Attorney General's regulations should apply equally to the submission of verifiable consumer requests under both sections.)

Section 1798.130(a)(1) requires a business to make two or more “designated methods for submitting requests” available to consumers to submit a verifiable consumer request for information pursuant to sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.

(Note that this section does not cross-reference section 1798.100, but as discussed above, the regulations should apply equally to both sections in light of the overlap.)

Section 1798.140(i) defines “designated methods for submitting requests” to mean “a mailing address, email address, Internet Web page, Internet Web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.”

Section 1798.130(a)(2) requires a business, upon receipt of a request from a consumer, to promptly take steps to determine whether the request is a verifiable consumer request. The determination of whether a request is verified does not extend the business’s duty to disclose and deliver the information within 45 days of receipt of the consumer’s request, unless the business reasonably determines that it needs additional time and provides notice of the extension to the consumer within the first 45-day period, in which case the deadline to respond may be extended once by an additional 45 days. “The disclosure shall cover the 12-month period preceding the business’s receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer’s account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer’s option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business shall not require the consumer to create an account with the business in order to make a verifiable consumer request.”

What are the Attorney General’s responsibilities with respect to adopting a regulation to implement the provisions of law relating to a verifiable consumer request?

Section 1798.185(a)(7) requires the Attorney General to “[e]stablish[] rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer’s or the consumer’s authorized agent’s ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business’s determination that a request for information received by a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the

business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter."

PROPOSED REGULATIONS¹

Definition of "verifiable consumer request"

A "verifiable consumer request" means a request submitted by a consumer, by a consumer on behalf of the consumer's minor child aged 13 or less, or by the consumer's authorized agent, pursuant to sections 1798.100, 1798.105, 1798.110, or 1798.115, as to which the business that receives the request authenticates that the consumer who submitted the request, or on whose behalf the request is submitted, is the consumer about whom the request is made.

Definition of "authenticate"

"Authenticate" means to use reasonable measures to verify that a consumer who submits a verifiable consumer request, or on whose behalf a verifiable consumer request is submitted, for the disclosure of information pursuant to sections 1798.100, 1798.110, and 1798.115, or who requests deletion of personal information pursuant to section 1798.105, is the consumer to whom the request pertains, including but not limited to, through the use of a user name and password by a consumer who maintains an account with the business while the consumer is logged into the account, two-factor authentication, knowledge-based challenge-response authentication, or a similar method that offers the consumer an opportunity to verify the consumer's identity to the business, provided that the method is not unduly burdensome to the consumer.

Definition of "two-factor authentication"

"Two-factor authentication" means a security process in which the consumer provides two different pieces of evidence to verify themselves, such as evidence establishing something they know, something they have, or something they are.

Definition of "knowledge-based challenge response"

"Knowledge-based challenge-response" means a security process in which the business asks the consumer a question based on non-public information known to the consumer and the business to which the consumer must provide a correct response.

¹ To the extent that the proposed regulations use terms defined by the CCPA (e.g., consumer, person, etc.), the definitions set forth therein shall apply to the regulations.

Definition of “self-authenticate”

“Self-authenticate” means a process whereby a consumer verifies the consumer’s identity to the business, provided that the method is not unduly burdensome to the consumer, including but not limited to, by providing the consumer’s user name and password to the business while logged into the consumer’s account, providing two different pieces of evidence to the business to verify themselves, responding correctly to a question asked by the business based on some private information known to the consumer, or using a similar method to verify the consumer’s identity directly to the business.

Definition of “authorized agent”

“Authorized agent” means a natural person, or a person registered with the Secretary of State authorized by the consumer, or by a consumer on behalf of the consumer’s minor child aged 13 or less, to act on the consumer’s behalf.

Use of Authorized Agent

A consumer may use an authorized agent to submit a verifiable consumer request to a business on the consumer’s behalf, provided that either: (1) the authorized agent facilitates the submission of the consumer’s verifiable consumer request, and if applicable, the reception of data on the consumer’s behalf, and the consumer is required to self-authenticate; or (2) the consumer provides the agent with the consumer’s power of attorney to submit the request on the consumer’s behalf to the business pursuant to section 4401 of the Probate Code. The power of attorney must be notarized and signed in the presence of two witnesses.

Inclusion of Identifiers in verifiable consumer request

Businesses shall allow consumers who submit a verifiable consumer request to provide the business with the consumer’s verifiable identifiers for the purpose of associating those verifiable identifiers with any personal information previously collected about the consumer by the business. A business that receives or collects personal information from a consumer in connection with the consumer’s submission of a request or the business’s verification of the request shall use that information solely for the purposes of verification and responding to the consumer’s request.

Definition of verifiable identifier

“Verifiable identifier” means an identifier, including but not limited to a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers, provided that the business authenticates that the identifier belongs uniquely to the consumer.

Requirement to respond within 45 days

(a) A business that receives a verifiable consumer request pursuant to sections 1798.100, 1798.110, or 1798.115, shall disclose and deliver the required information to the consumer within 45 days of receipt of the verifiable consumer request. The business may extend this deadline by 45 days, provided that the business determines that it is reasonably necessary and provides notice of the 45-day extension to the consumer. This deadline shall not be extended as a result of the time spent by the business to determine that the request is a verifiable consumer request.

(b) A business that receives a verifiable consumer request pursuant to section 1798.105 shall delete the required information and notify the consumer of its action within 45 days of receipt of the verifiable consumer request. The business may extend this deadline by 45 days, provided that the business determines that it is reasonably necessary and provides notice of the 45-day extension to the consumer. This deadline shall not be extended as a result of the time spent by the business to determine that the request is a verifiable consumer request.

PROPOSED REGULATIONS TO IMPLEMENT EXCEPTION FOR LOYALTY PROGRAMS

BACKGROUND

Non-Discrimination

Section 1798.125 prohibits a business from discriminating against a consumer because the consumer exercised any of the consumer's rights under the CCPA, including, but not limited to, by:

- (A) Denying goods or services to the consumer;
- (B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;
- (C) Providing a different level or quality of goods or services to the consumer; or
- (D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

However, section 1798.125(b)(1) includes an exception for discounts and financial incentives offered to consumers, provided that they are directly related to the value to the business of the consumer's personal information. (Note that, as a result of a typographical error, section 1798.125(a)(2) and (b)(1) refer to the value provided to the "consumer," rather than the "business," from the consumer's data. It is our understanding that AB 25 will propose to correct this error.)

Section 1798.125 includes two additional provisions of note. First, it requires a business to describe the material terms of the financial incentive program and obtain the consumer's opt-in consent to participate in the program, which may be revoked by the consumer at any time. Second, it prohibits a business that offers a financial incentive program from engaging in practices that are unjust, unreasonable, coercive, or usurious in nature.

Attorney General's Obligation

Section 1798.185 requires the Attorney General to establish rules and guidelines regarding financial incentive offerings.

PROPOSED REGULATIONS¹

Definitions

"American consumer" means a natural person who is a resident of the United States.

¹ To the extent that the proposed regulations use terms defined by the CCPA (e.g., consumer, personal information, sale), the definitions set forth therein shall apply to the regulations.

“Loyalty or discount program” means a membership program offered by a business to consumers pursuant to which the business offers consumers financial discounts, financial benefits, rewards or other types of incentives in return for consumers engaging in commercial transactions with the business.

“Member” means any consumer who is part of a loyalty or discount program.

“Revenue per consumer from sale of personal information” means the average annual per consumer gross revenue received by the business from the sale of consumers’ personal information, including any financial or monetary consideration and the fair market value of any other consideration received by the business. If a business does not account separately for its sale of consumers’ personal information and its sale of American consumers’ personal information, “revenue per consumer from the sale of personal information” shall mean the average annual per consumer gross revenue received by the business from the sale of personal information of American consumers.

Loyalty Program

Sec. _____. A business that offers consumers the opportunity to participate in a loyalty or discount program shall be deemed to be in compliance with Section 1798.125, provided that: (a) the business discloses the terms of the program to the consumer in a clear and conspicuous manner pursuant to section _____.; (b) the consumer affirmatively opts into the program; (c) the business provides the consumer with a clear and conspicuous method to opt out of the program at any time; and (d) the business offers a consumer who opts out of the sale of the consumer’s personal information the opportunity to participate as a member in the loyalty or discount program with the same rights and benefits offered to members who have not opted out of the sale of their personal information, provided that the business may charge the consumer an annual membership fee to participate in the discount or loyalty program that is no more than the business’s revenue per consumer from sale of personal information.

Sec. _____. A business that offers a loyalty or discount program shall disclose the terms of the program to consumers, including: (1) the revenue per consumer from sale of personal information ; and (2) the right of the consumer to opt out of the sale of the consumer’s personal information and participate in the program as a member, including the right of the business to charge the consumer an annual membership fee to participate in the discount or loyalty program that is no more than the business’s revenue per consumer from sale of personal information.

PROPOSED REGULATIONS TO IMPLEMENT BUSINESS PURPOSES EXCEPTION

BACKGROUND

Definition of Business Purpose

Section 1798.140(d) defines “business purpose” to mean “the use of personal information for the business’s or a service provider’s operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected.

Business purposes are:

- (1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.
- (2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.
- (3) Debugging to identify and repair errors that impair existing intended functionality.
- (4) Short-term, transient use, provided that the personal information is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer’s experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.
- (5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.
- (6) Undertaking internal research for technological development and demonstration.
- (7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

Definition of Service Provider and Written Contract Requirement

Section 1798.140(v) defines “service provider” to mean “a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.”

Definition of Commercial Purpose

Section 1798.140(i) defines “commercial purpose” to mean “to advance a person’s commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. ‘Commercial purposes’ do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.”

The definition of “service provider” makes clear that a service provider may only use a consumer’s personal information for the commercial purpose of providing the services specified in the contract with the business.

Service Provider Exception

Section 1798.140(t) defines “sell” to exclude the use or sharing of a consumer’s personal information with a service provider “that is necessary to perform a business purpose” if two requirements are met: (1) The business has provided notice that consumers’ personal information is being used or shared in its terms and conditions consistent with Section 1798.135; and (2) the service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

(Note that the definition of service provider also prevents the service provider from “retaining” or “disclosing” the personal information, other than to provide the services specified in the contract.)

Third Party Definition

Section 1798.140(w)(2)(A) defines “third party” to exclude a “person to whom the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract” prohibits the person from selling, retaining, using, or disclosing the personal information other than for the business purpose specified in the contract and includes a certification by the person that it will comply with these restrictions.

As a result of this exception, the transfer of information by a business to a person (which is defined broadly in section 1798.140(n) to include individuals, corporations, associations, etc.) for a business purpose pursuant to a contract that satisfies these terms is not considered a sale of personal information.

PROPOSED REGULATIONS¹

Definition of Contractor

“Contractor” means a person to whom the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the person from selling, retaining, using, or disclosing the consumer’s personal information other than for the business purpose specified in the contract and includes a certification by the person that the person will comply with these restrictions.

Use of Personal Information by Service Provider or Contractor

(a) A service provider or contractor shall only use a consumer’s personal information for the purposes of providing services specified in the written contract to the business. A service provider or contractor shall not further collect, sell, disclose, use, or retain the personal information of the consumer, including but not limited to, for the purpose of enhancing the services it provides to another person.

(b) In order to comply with subdivision (a), a service provider or contractor shall separately maintain or “silo” personal information it receives from a business about a consumer from: (1) personal information it receives about the same consumer from another person and (2) personal information it receives about the same consumer from that consumer’s interaction with the service provider or contractor.

¹ To the extent that the proposed regulations use terms defined by the CCPA (e.g., consumer, person, etc.), the definitions set forth therein shall apply to the regulations.

(c) A service provider or contractor shall be prohibited from using or accessing personal information received from a business or from the consumer's interaction with the service provider or contractor for the purpose of providing services to another person.

(d) A service provider or contractor shall be prohibited from aggregating the personal information it receives about a consumer from a business with the personal information it receives from another person about the same consumer, or with the personal information it receives from the same consumer's interaction with the service provider or contractor.

Retention of Personal Information for Advertising

A person that obtains access to a consumer's personal information for the purpose of preparing a bid for the use of that information for advertising or marketing services shall be required to delete the consumer's personal information to which it had access as part of the bid process if the bid is not successful.

Definition of "advertising or marketing services"

"Advertising or marketing services" means the transmission or receipt of personal information by, or on behalf of, a business for the purposes of inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.

Message

From: Courtney Murphy [REDACTED]
Sent: 1/3/2019 10:38:58 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Suggestions for CCPA of 2018
Flag: Follow up

Dear CA Department of Justice,

I have the following comments/suggestions/requests regarding the CCPA of 2018:

- Can you please include what the “categories of third parties” would be?
- Can you please specify whether businesses will need to also provide the names and contact info of the third parties the PI was sold or disclosed to or whether just the categories of third parties will suffice?
- Can you please specify whether businesses will need to also provide the specific information share with third parties or whether just the categories of PI will suffice?
- Can you please specify whether there is a 45 day extension or a 90 day extension to all business obligations?
- Can you please specify whether business will be obligated to provide the full 12 mos. of PI info as of Jan. 2020? As you can imagine, implementing processes and procedures to track this information and make it readily available will take some time to develop, and requiring businesses to be able to provide the full 12 mos. in 12 mos. from now will be very difficult for businesses to implement.

Regards,

Courtney A. Murphy
Legal Counsel
Just Energy
5251 Westheimer Rd, Suite 1000, Houston, TX 77056

[REDACTED]



Web justenergy.com

This e-mail message is intended only for the use of the recipient(s) named above. This message is an attorney-client communication and as such privileged and confidential. If you are not an intended recipient, you may not review, copy, or distribute this message. If you have received this communication in error, please notify us immediately by e-mail and delete the original message.

Message

From: Melanie Tiano [REDACTED]
Sent: 3/8/2019 3:00:16 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Gerard Keegan [REDACTED]
Subject: Supplemental Comments of CTIA on CCPA
Attachments: 030819 CTIA CCPA Proposed Regulatory Language Comments.pdf

To Whom It May Concern:

Attached please find supplemental written comments in response to the CCPA Rulemaking Process.

Please feel free to contact me with any questions.

Thank you,

Melanie Tiano



Melanie K. Tiano

Director, Cybersecurity and Privacy

1400 16th Street, NW

Washington, DC 20036





Before the
STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
ATTORNEY GENERAL'S OFFICE
Los Angeles, CA 90013

In the Matter of)	
)	
California Consumer Privacy Act Rulemaking)	Public Forums on the California
Process)	Consumer Privacy Act
)	

SUPPLEMENTAL COMMENTS OF CTIA

Gerard Keegan
Vice President, State Legislative Affairs

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th St. NW, Suite 600
Washington, DC 20036
(202) 736-3200
www.ctia.org

March 8, 2019

TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY	3
II.	PROPOSED REGULATORY LANGUAGE	3
1.	The Attorney General Should Issue Regulations that Provide Flexibility In How Businesses Verify Consumer Requests for Information.....	3
2.	Businesses Should Not Be Required To Provide Consumers With “Specific Pieces Of Personal Information” That Create Privacy And Data Security Risks.	5
3.	The Attorney General Should Clarify the Inconsistent Language in Section 1798.125 Regarding Non-Discrimination and Allowable Incentives.....	6
4.	Consumers Should Have More Than an “All-or-Nothing” Choice Regarding Sales of Their Personal Information.	8
5.	Consumers’ Previous Opt-In Choices Should Not Be Subject To A Subsequent Global Opt-Out Choice.....	9
6.	Businesses Should Have Flexibility To Determine Where To Place the “Do Not Sell My Personal Information” Link To Make It Most Useful To Consumers.	10
7.	The Definition of “Sell” Should Be Limited To Forms Of Monetary Consideration.	11
8.	Businesses Should Not Be Obligated To Retain Personal Information.	12
9.	Regulations Should Exclude Certain Employment- And Business-Related Information From The Definition Of “Personal Information.”	13
10.	The Attorney General Should Resolve Inconsistent Obligations Relating To Disclosures About Sales Of Personal Information.....	14
III.	CONCLUSION.	16

I. INTRODUCTION AND SUMMARY

CTIA appreciates the California Attorney General Office's invitation to comment on regulations to implement and further the purposes of the California Consumer Protection Act of 2018 ("CCPA" or "Act").¹ This comment supplements CTIA's comments filed on February 19, 2019,² and provides suggested regulatory language to address key concerns and implementation challenges with the Act that are identified in this and CTIA's earlier filed comments.

As noted in CTIA's Feb 19. comments, we take as a guiding principle the Legislature's intent of protecting consumers' privacy through the CCPA. To that end, CTIA urges the Attorney General to use the authority granted by the Act to develop and implement regulations that bring clarity to the unclear or ambiguous statutory provisions that otherwise will operate to the detriment of consumers and businesses. To the extent the Attorney General does not have the authority to address, through regulation, any of the concerns identified here or in CTIA's prior comment, then CTIA urges that the Attorney General recommend to the Legislature a statutory solution.

II. PROPOSED REGULATORY LANGUAGE

1. The Attorney General Should Issue Regulations that Provide Flexibility In How Businesses Verify Consumer Requests for Information.

The Act requires businesses provide consumers with information about the personal information they hold about them and to take certain other actions upon receipt of a "verifiable consumer request from a consumer."³ The Act also requires the Attorney General

¹ Codified as amended at Cal. Civ. Code § 1798.100 *et seq.* Unless otherwise noted, all statutory citations in this comment are to the codification of AB 375 in the California Civil Code, as amended by SB 1121 (published Sept. 24, 2018 9:00 PM).

² See generally Comments of CTIA, *In the Matter of California Consumer Privacy Act Rulemaking Process* (Feb. 19, 2019) (attached as Appendix A) (hereinafter "CTIA Feb. 19 Comments").

³ See §§ 1798.100(a),(d); 1798.105(c); 1798.110(b); 1798.115(b); 1798.130.

issue regulations “to govern a business’s determination that a request for information received from a consumer is a verifiable consumer request. . .”⁴ Verification is critically important to ensure that information about a consumer is only released when the consumer’s identity can be confirmed.⁵

In developing regulations, CTIA urges the Attorney General to consider, as the Act implicitly acknowledges,⁶ that specific methods or a “one size fits all” verification scheme should not be prescribed. The consumer verification methods that a business employs will depend on a variety of factors, including the nature and context of the consumer’s interaction with a company, the sensitivity of personal information at issue in the consumer’s request, and the harms that could arise from disclosing the information to anyone other than the consumer or a person authorized to act for the consumer. Allowing businesses flexibility in developing methods to verify such consumers and requests will foster the development of innovative and accurate methods to address data security risks to ensure that consumer’s personal information is not erroneously disclosed. Regulations also should provide guidance on how a business should respond to a consumer’s request when it cannot verify the request.

Proposed Regulatory Language⁷

(a) A business shall establish reasonable methods of verifying that a consumer who exercises rights under the Act is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer’s behalf. In establishing such method, the business shall take into consideration the sensitivity of the personal information at issue, the nature of the business’s products or services, the risk of

⁴ See §1798.185(a)(7).

⁵ As noted in our earlier comment, CTIA members already have verification procedures in place to respond to consumer requests, including those that address the difficult privacy and data security challenges that may arise from the creation of sub-accounts or separate profiles, which are common in many industries.

⁶ See §1798.185(a)(7) (requiring that in establishing rules and procedures governing verifying consumer requests, the Attorney General take into account, among other things, available technology, security concerns, and the burden on the business).

⁷ The Attorney General has authority to issue this proposed regulation pursuant to Cal. Civ. Code § 1798.185(a)(7).

unauthorized access to the consumer's personal information and the nature of the consumer's interaction with the business.

(b) If the business cannot reasonably verify the consumer's request based on the information provided, then the business shall send the consumer, or the person authorized by the consumer to act on the consumer's behalf, an explanation that the consumer's identity could not be verified.

2. Businesses Should Not Be Required To Provide Consumers With “Specific Pieces Of Personal Information” That Create Privacy And Data Security Risks.

The Attorney General's regulations should minimize the privacy and data security risks that the CCPA's access provisions could create. Some of the main sources of such risks are Sections 1798.100(a) and 1798.110(c)(5), which require a business to provide “specific pieces of personal information the business has collected” about consumers. Releasing such granular information to consumers can create cybersecurity and fraud risks that would not exist in the absence of these disclosures. For example, if a business is required to re-associate specific pieces of personal information, which might be held in separate databases, with a consumer in order to respond to the consumer's requests, it will make the information more attractive to identity thieves and vulnerable to cybersecurity attacks, an outcome that is contrary to the Legislature's intent.

While the Act does not define “specific pieces of personal information” or how extensive the obligation to provide this information is, certain categories of information that are included in CCPA's definition of personal information, such as social security numbers, driver's license numbers, and passport numbers, are especially attractive to identity thieves.

The California Legislature recognized the sensitivity of certain categories of personal information when it passed California's data security law to protect that information from unauthorized access, destruction, use, modification, or disclosure.⁸ Similarly, Section

⁸ See Cal. Civ. Code § 1798.81.5.

1798.150 provides a private right of action for unauthorized access to or theft of the categories of information enumerated in Section 1798.81.5 resulting from a business's failure to maintain and implement reasonable security practices and procedures.

CTIA therefore recommends that the Attorney General issue regulations to mitigate risks by excluding these and other categories of information that raise particular concerns. Additionally, the Attorney General should exempt businesses from any obligation to provide information that could reveal trade secrets. Such an exception would be consistent with the privacy-promoting purpose of the CCPA – the achievement of which does not require the destruction of companies' investments in their products and services.

Proposed Regulatory Language⁹

A business is not required to provide a consumer with specific pieces of personal information if disclosure to the consumer creates an unreasonable risk to the security of that personal information, the consumer's account with the business, the security of the business's systems or networks, trade secrets or intellectual property rights. For purposes of sections 1798.110, 1798.115, and 1798.130, specific pieces of personal information includes but is not limited to personal information as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5.

3. The Attorney General Should Clarify the Inconsistent Language in Section 1798.125 Regarding Non-Discrimination and Allowable Incentives.

The CCPA provides inconsistent and confusing standards to govern discounts and incentive programs,¹⁰ which are of major consumer and commercial importance. Specifically, Section 1798.125(a)(2) allows businesses to charge consumers different prices or rates, or provide a different level of quality of goods and service, in exchange for uses of the consumer's personal information allowed under the Act, provided that the differences

⁹ The Attorney General has authority to issue this proposed regulation pursuant to Cal. Civ. Code §§ 1798.185(a)(3) and 1798.185(a)(7).

¹⁰ See Cal. Civ. Code § 1798.125.

bear the requisite relationship to the value of the data at issue. That relationship, however, is in need of clarification in two ways.

First, the CCPA provides that the difference must be based on value of the data to the consumer rather than to the business offering the product or service. Focusing on the value of the data to the consumer incorrectly assumes that the consumer has parted with the data, or that its value to the consumer has been diminished, by virtue of the transaction. In fact, even after agreeing to certain uses of his or her data by the business, the consumer simultaneously retains the data and the right to derive value from it over and over again in transactions with multiple businesses.¹¹ What the consumer is actually conveying is the right of the business to derive value from that data. Hence, the pertinent metric is the value of the data to the business. Consumers then can decide whether the incentive being offered is a fair value exchange for the use of their data, and either accept or reject the incentive.

In addition, the Act allows for certain differences related to price or rate, or level or quality of goods and services if they are “reasonably related” to the value of the consumer’s data under Section 125(a)(2), but Section 125(b)(1) requires differences to be “directly related” to the value of the data.

There appears to be no logical rationale for these inconsistent standards. To the extent that the Attorney General has the authority, he should issue regulations to clarify that “directly related to the value of the data” means that there is a reasonable relation between the value of the consumer’s data to the business, and the different price or level or quality of goods or services offered to the consumer.

¹¹ Attempting to determine the value of the data to the consumer would also raise some peculiar, and seemingly unanswerable, questions, e.g., what is the value to a consumer of her age range? *See* Memorandum for Informational Hearing of the Senate Committee on Judiciary on “The State of Data Privacy Protection: Exploring the California Consumer Privacy Act and Its European Counterpart,” at 6 (Mar. 5, 2019) (“[I]t is unclear how ‘the value provided to the consumer by the consumer’s data’ would be measured, and by who.”)

Proposed Regulatory Language¹²

A business shall be deemed in compliance with Section 1798.125 if there is a reasonable basis for the difference in price or rate, or the level or quality of goods and services it offers to a consumer in exchange for the consumer's data.

4. Consumers Should Have More Than an “All-or-Nothing” Choice Regarding Sales of Their Personal Information.

Section 1798.120 provides consumers with the right to opt out of the sale of their personal information. Under Section 1798.135, a business must notify consumers of this opt-out right through a “clear and conspicuous link on the business’s Internet homepage, titled, ‘Do Not Sell My Personal Information.’” Without clarification, these provisions could be interpreted to require that a business provide consumers with a single, globally applicable opt-out choice (except as discussed in Section 5 below on previously made opt-in choices).

In many cases, however, consumers are willing to agree to the sale of their personal information for certain uses or programs, such as business loyalty programs and discounts. A Pew Research Center survey that asked consumers if they would accept lower prices in exchange for allowing a store to track their shopping habits and sell the data to third parties, found that two-thirds of consumers said the arrangement would be acceptable in at least some circumstances.¹³

CTIA recommends that the Attorney General issue regulations clarifying that the Act permits businesses to provide consumers with the ability to make more granular opt-out choices, so long as there is also an option to opt-out of all sales. This interpretation is consistent with the approach taken in the federal Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM ACT),¹⁴ which requires the ability to opt-out

¹² Cal. Civ. Code § 1798.185(a)(6) could provide the Attorney General with the authority to issue this regulation.

¹³ Pew Research Center, *Privacy and Information Sharing*, (Jan. 14, 2016), <http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/>

¹⁴ 15 U.S.C. §§ 7701, *et seq.*

of certain email messages, but allows the initiator of such messages to offer recipients the opportunity to choose the specific types of messages the recipient wants to receive or not receive, so long as an option to not receive any commercial electronic mail is given.¹⁵ CAN-SPAM's granularity provides flexibility for businesses and consumers in the context of commercial email and is a model worth emulating in connection with information sales.

Proposed Regulatory Language¹⁶

A business subject to Section 1798.120 may comply by providing in the "Do Not Sell My Personal Information" link referenced in Section 1798.135(a)(1), a list or menu that includes specific types of personal information, specific types of sales, categories of third parties, or other options, from which the consumer may choose whether to opt out of the sale of personal information, provided that the list or menu includes an option under which the consumer may choose to opt out of all sales of the consumer's personal information.

5. Consumers' Previous Opt-In Choices Should Not Be Subject To A Subsequent Global Opt-Out Choice.

Relatedly, Section 1798.120 does not address situations where consumers have previously opted in to the sale of their personal information. This is problematic because the provision could be interpreted to mean that a consumer's choice to opt in to a specific data practice or program would be automatically negated by a subsequent global "Do Not Sell My Personal Information" choice by the consumer. For example, a consumer who opts in to a retailer's loyalty card program is unlikely to expect that a global opt out offered on the retailer's website would cancel his or her participation in the loyalty program. Moreover, subjecting opt-in choices to a global opt-out would be a disincentive to offering opt-in choices in the first place.

The Attorney General should clarify, therefore, that if a business engages in the sale of personal information pursuant to a consumer's opt-in consent to allow the sale of personal

¹⁵ 15 U.S.C. § 7704(a)(3)(B).

¹⁶ The Attorney General has authority to issue this proposed regulation pursuant to Cal. Civ. Code § 1798.185(a)(4).

information for specific practices or programs, such sales need not be subject to the “Do Not Sell My Personal Information” choice that is required under the Act, so long as businesses provide consumers with a mechanism to subsequently opt out of sales for which they had previously opted in.

Proposed Regulatory Language¹⁷

A business shall be deemed in compliance with Section 1798.120(b) of the Act and need not provide the “Do Not Sell My Personal Information” link described in Section 1798.135(a) when the consumer has previously opted in to the sale of personal information and the business provides the consumer with a mechanism to subsequently opt out.

6. Businesses Should Have Flexibility To Determine Where To Place the “Do Not Sell My Personal Information” Link To Make It Most Useful To Consumers.

Section 1798.135(a), which sets requirements for the placement of a “Do Not Sell My Personal Information” link, presents a serious internal inconsistency that the Attorney General should consider addressing through regulations. The Act requires a business to display this link on its “Internet homepage,”¹⁸ which, in turn, is defined in relevant part as “the introductory page of an Internet Web site and any Internet Web page where personal information is collected. . . .”¹⁹ One challenge with this definition is that some businesses might not maintain a traditional “homepage,” and they need flexibility to be able to present the “Do Not Sell” link where it is likely to reach consumers. At the same time, the definition of “homepage” appears to require the “Do Not Sell” link to appear everywhere that a business collects personal information. In addition to requiring businesses to display a

¹⁷ The Attorney General has authority to issue this proposed regulation pursuant to Cal. Civ. Code § 1798.185(a)(4).

¹⁸ CTIA’s earlier comment raised concerns with the CCPA’s definition of “homepage” since it could be interpreted to require that the “Do Not Sell” link appear on every web page on which a business collects personal information, which would be inconsistent with the word’s common meaning, not necessary for consumers to exercise their opt-out rights, and would create unnecessary costs for businesses. CTIA Feb. 19 Comments at 11.

¹⁹ See Cal. Civ. Code § 1798.140 (defining “homepage” to mean “the introductory page of an Internet Web site and any Internet Web page where personal information is collected. . . .”) (emphasis added).

specific link in a nearly infinite number of locations, this definition could result in the production of yet another privacy notification that consumers will soon learn to ignore.

The Attorney General could help to address the incoherent requirements imposed under Section 1798.135 and the definition of “homepage” by issuing a regulation that provides businesses with flexibility about where to provide the “Do Not Sell” link, so long as the link is in a location that a consumer making a decision about his or her data would easily find it.

Proposed Regulatory Language²⁰

A business shall be deemed in compliance with paragraph (1) of subdivision (a) of Section 1798.135 of the Act where the business places the “Do Not Sell My Personal Information” link or logo clearly and prominently in a location or locations that are reasonably calculated to enable consumers to find the link or logo in the ordinary course of using the businesses products or service.

7. The Definition of “Sell” Should Be Limited To Forms Of Monetary Consideration.

Several of the CCPA’s rights and obligations are tied to the “selling” of personal information, including the right to opt out and certain transparency requirements.²¹ The definition of “selling” (and related terms), in turn, depends on the undefined phrase “valuable consideration.”²² Taken to its extreme, the concept of “valuable consideration” could encompass nearly every benefit that a business derives from its relationship with a third party, resulting in obligations that are unworkably broad and burdensome. For example, consider a company that allows developers to access users’ data without obtaining any form of compensation but nevertheless develops goodwill for providing such access. That goodwill could be considered a type of “valuable consideration” under the definition of “sell.”

²⁰ The Attorney General has the authority to issue this regulation pursuant to Section 1798.185(a)(4).

²¹ See, e.g., Cal. Civ. Code. §§ 1798.115, .120.

²² See *id.* § 1798.140(t)(1).

The Attorney General should define “valuable consideration” through regulations to avoid this outcome. Specifically, limiting “valuable consideration” to the exchange of money or other goods or instruments whose value is readily quantifiable would provide businesses with clear notice of the circumstances in which obligations relating to the sale of personal information apply to them. This clarity would make the CCPA easier to administer, by directing compliance and enforcement efforts to focus on situations in which there is likely to be objective measures of the value of personal information.

The Attorney General should also take steps to prevent the definition of “sell” from causing unintended disruption of online advertising. In particular, the Attorney General should clarify that certain incidental disclosures of personal information to support technical or accounting functions of online advertising are disclosures to service providers for a “business purpose”²³ and therefore are not “sales”²⁴ to third parties.

Proposed Regulatory Language:²⁵

(a). For purposes of paragraph (1) of subdivision (t) of Section 1798.140 of the Act, “valuable consideration” shall mean selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party in exchange for money, a gift, a loan, or other consideration which has a readily ascertainable market value.

(b). Personal information is not “sold” where the disclosure of the personal information is necessary for or incidental to, or to facilitate, the delivery, display, measurement, customization, or analysis of an online advertisement.

8. Businesses Should Not Be Obligated To Retain Personal Information.

The CCPA establishes some unfortunate incentives for businesses to retain personal information that they do not need. Although Section 1798.100(e) provides that a business is

²³ See § 1798.140(d)(1).

²⁴ See, in particular, § 1798.140(t)(2)(C).

²⁵ Section 1798.185(b), which authorizes “additional regulations as necessary to further the purposes” of the CCPA, is a potential source of authority to define “valuable consideration.”

not required to retain personal information collected for a single one-time transaction, the CCPA is silent about businesses' more general data retention obligations. The narrowness of the exception for one-time transactions could be construed to imply that businesses are otherwise required to retain personal information to fulfill consumer data access requests.²⁶

Such an interpretation of the CCPA would create additional privacy and security risks to personal information, by potentially requiring organizations to retain data that they would otherwise delete or destroy, consistent with data security guidance issued by the Federal Trade Commission ("FTC").²⁷ To prevent the CCPA from creating these types of risks and to promote consistency with the FTC's guidance, the Attorney General should issue regulations clarifying that there is no obligation for a business to retain personal information solely for the purposes of fulfilling consumer requests under the Act.

Proposed Regulatory Language:²⁸

A business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the Act.

9. Regulations Should Exclude Certain Employment- And Business-Related Information From The Definition Of "Personal Information."

CTIA reiterates that the broad definitions of "consumer" and "personal information" under the CCPA create negative consequences for consumers and present serious compliance challenges to an array of businesses.²⁹ Of particular concern is the CCPA's possible inclusion of information relating to California residents in their capacities as employees, contractors, or other business-related activities within the definition of "personal information." By appearing to include such information in the definition of "personal

²⁶ See § 1798.130(a) (requiring certain disclosures to cover the 12-month period preceding a verified consumer request).

²⁷ FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (2012) at 28 (recommending that companies implement reasonable restrictions on data retention and dispose of personal data once it is longer necessary for the legitimate purpose for which it was collected).

²⁸ See § 1798.185(a)(7).

²⁹ See CTIA Feb. 19 Comments at 5-8.

information,” the CCPA could affect businesses’ ability to comply with a broad range of laws, from state employment law where, for example, California law already establishes rights and obligations concerning personnel and wage records, to federal anti-money laundering laws.³⁰ While extending the full suite of CCPA rights and obligations to some “professional or employment-related information,”³¹ such as information provided by consumers for posting on employment-related social networks, might be consistent with the main purposes of the Act, extending this treatment to records maintained by employers about their employees is not. Similarly, treating information about corporate officers or board members as personal information could impede efforts to provide and maintain corporate accountability and transparency. CTIA therefore recommends that the Attorney General clarify that “personal information” does not encompass information collected in the course of certain employment or business-related activities.

Proposed Regulatory Language³²

(a). For purposes of paragraph (1) of subdivision (o) of Section 1798.140 of the Act, information shall not constitute “personal information” where the information is collected by a business from an employee or applicant and the information relates to the person’s employment or application for employment with the business.

(b). For purposes of paragraph (1) of subdivision (o) of Section 1798.140 of the Act, information shall not constitute “personal information” where the information is collected by a business collected in connection with an individual’s role as a director, agent, independent contractor or vendor of a business.

10. The Attorney General Should Resolve Inconsistent Obligations Relating To Disclosures About Sales Of Personal Information.

Section 1798.115 sets forth detailed requirements governing how businesses must respond to verified consumer requests regarding sales of personal information to third parties.

³⁰ See *id.* at 5-6.

³¹ Cal. Civ. Code § 1798.140(o)(1)(I).

³² Section 1798.185(b) is a potential source of authority to issue such a regulation.

Unfortunately, the details in the statutory scheme contain a significant conflict between what consumers have the right to request and what businesses have the obligation to provide. Specifically, under Section 1798.115(a)(2), consumers may request the “categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.” Section 1798.130(a)(4) governs responses to such requests and provides, in relevant part, that a business must only “provide the categories of third parties to whom the consumer’s personal information was sold in the preceding 12 months”³³ In other words, Section 115(a)(2) appears to allow requests about personal information disclosed to specific third parties, while Section 130(a)(4) appears to require businesses only to disclose the categories of third parties that have received personal information. Since Section 130 governs the actual response that businesses must provide, CTIA recommends that the Attorney General clarify that businesses do not need to go through the process of correlating types of personal information sold with specific third parties.

Proposed Regulatory Language³⁴

A business shall be in compliance with subdivision (b) of Section 1798.115 if it associates the categories of personal information sold to the categories of third parties to whom information is sold. A business shall not be required to associate categories of personal information sold to each third party to which the information was sold.

³³ Cal. Civ. Code § 1798.130(a)(4)(B).

³⁴ Section 1798.185(b) is a potential source of authority to issue this regulation.

III. CONCLUSION.

CTIA appreciates the opportunity to provide the Attorney General's Office with these comments and proposed regulatory language, and looks forward to continuing to work with the Office as this rulemaking process proceeds.

Respectfully submitted,

/s/ Gerard Keegan
Gerard Keegan
Vice President, State Legislative Affairs

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th St. NW, Suite 600
Washington, DC 20036
[REDACTED]
www.ctia.org

March 8, 2019

Message

From: Courtney Jensen [REDACTED]
Sent: 1/7/2019 6:42:08 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: TechNet CCPA Comments
Attachments: TechNet CCPA Letter.pdf

Good Evening,

Attached is a letter containing TechNet's comments on the CCPA rulemaking. Please let me know if you have any questions regarding our comments.

Also, if you are able to share, is there a timeline when you plan to begin the formal rulemaking process?

Thank you,
Courtney

Courtney Jensen
Executive Director | California and the Southwest
TechNet | The Voice of the Innovation Economy
[REDACTED]



TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Southwest | Telephone [REDACTED]
915 L Street, Suite 1270, Sacramento, CA 95814
www.technet.org | [REDACTED]

January 7, 2019

The Honorable Xavier Becerra
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Dear Mr. Attorney General Becerra,

On behalf of TechNet and our member companies, I thank you for convening public forums regarding the California Consumer Privacy Act ("CCPA"). TechNet is committed to being a productive stakeholder in this process. TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic startups and the most iconic companies on the planet and represents three million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

TechNet member companies place a high priority on consumer privacy. At a high level, the rights under the CCPA are sensible; however, the law was drafted quickly and is still in need of refinement. CCPA contains drafting errors and unclear requirements that raise significant operational and compliance problems that do not advance privacy or data security. Fortunately, there is still time to clear up concerns with the law through regulations and legislation to make this law workable and meaningful for California consumers and businesses.

TechNet believes regulations and legislation can address a number of definitional and operational problems with the law. To provide just one of many examples, under the law as passed, companies must provide specific pieces of information, but the law does not explain or define what it means by "specific pieces" of personal information. Providing certain information, such as a consumer's social security number or driver's license number, in response to such requests, creates unnecessary risks to both the security of the consumer's information and the business' ability to protect such information. Other issues to highlight for future discussion include: definition of consumer; opt-out mechanism where a consumer has already expressly opted-in; pseudonymized data; verifiable requests; retention of data; definition of homepage; and establishing guidelines regarding a "financial incentive." TechNet

looks forward to discussing these issues and others throughout the rulemaking process to ensure California consumers are protected and California business can comply with the CCPA.

Thank you,
Courtney Jensen
Executive Director, California and the Southwest
TechNet

Message

From: Courtney Jensen [REDACTED]
Sent: 3/8/2019 6:03:25 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: TechNet CCPA Written Comments
Attachments: TechNet CCPA Rulemaking Letter 3.8.19.pdf

Good Afternoon,

Attached please find TechNet's written comments regarding CCPA rulemaking.

Please do not hesitate to reach out with any questions.

Thank you,
Courtney

Courtney Jensen
Executive Director | California and the Southwest
TechNet | The Voice of the Innovation Economy
[REDACTED]



TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Southwest | Telephone [REDACTED]
915 L Street, Suite 1270, Sacramento, CA 95814
www.technet.org | [REDACTED]

March 8, 2019

The Honorable Xavier Becerra
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Dear Mr. Attorney General Becerra,

TechNet appreciates your efforts to convene public forums regarding the California Consumer Privacy Act ("CCPA") as an initial opportunity for the public to participate in the CCPA rulemaking process. This process has brought to light a number of issues with the CCPA that are being dealt with by a diverse group of businesses, nonprofits, and others. TechNet offers the comments below that reflect issues we believe the Attorney General should consider during the formal rulemaking process.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic startups and the most iconic companies on the planet and represents three million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

TechNet member companies place a high priority on consumer privacy. We appreciate the aim of the CCPA to meaningfully enhance data privacy; however, the law was drafted quickly and is still in need of refinement. CCPA contains drafting errors and unclear requirements that raise significant operational and compliance problems that do not advance privacy or data security. The Legislature has looked to the Attorney General on some issues to create cohesive rules based on a statute that in some parts is unclear. Fortunately, there is time for the Attorney General to provide clear regulations, even while statutory amendments are being considered, to make this law workable and meaningful for California consumers and businesses.

TechNet believes regulations can address a number of concerns with the law. In addition to the specific comments in this letter, we believe the Attorney General, at this stage, should consider the following:

1. Avoid prescriptive rules or requirements while the statute is a moving target. Rather, the Attorney General can satisfy the statute and best serve California consumers and businesses by adopting simple rules that require "reasonable" methods of compliance without dictating specific, unworkable methods.
2. Provide guidance on interpretation and implementation. The Attorney General can serve a constructive role for consumers and businesses by providing guidance on how it intends to interpret key terms in the law and how it intends to enforce the statute. Such guidance would

help facilitate compliance on the part of businesses, while ensuring that consumers have clear expectations about what companies are and are not allowed to do with personal information.

3. Advise the legislature on issues that should be addressed in amendments to the statute. We believe the Attorney General can provide guidance to the legislature on the numerous problems, contradictions, and ambiguities in the law that make it difficult to comply with and difficult to enforce.

The comments below include specific issues and regulatory language that we hope to work with the Attorney General on during the formal rulemaking process. We believe these regulatory proposals could address a number of issues that currently make the CCPA difficult or impossible to comply with.

Definitions

Personal Information: AB 375, the original bill containing CCPA, was subsequently amended through SB 1121. SB 1121, signed by the governor on September 23, 2018, modified the initial paragraph of the definition of “Personal Information” by adding the text underlined below.

“Personal information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

The addition of this text clarifies that the scope of “Personal Information” should not extend beyond information that “identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly” with a particular consumer or household. To avoid ambiguity, the Attorney General should clarify that truly pseudonymized data that cannot be linked directly or indirectly with a particular consumer, as well as deidentified data, as defined, are outside the scope of “Personal Information.”

Proposed Regulatory Language.

For purposes of paragraph (1) of subdivision (a) of Section 1798.140 of the Act, information shall not constitute “personal information” where the information is pseudonymized or deidentified, or is aggregate information.

Sale: The first paragraph of the definition of “sell,” “selling,” “sale” or “sold” in the Act, reads as follows: 1798.140....(t) (1) “Sell,” “selling,” “sale,” or “sold,” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.

The phrase “valuable consideration,” however, is undefined. The Attorney General should clarify that “valuable consideration” is limited to similar monetary consideration to avoid any ambiguity on what was intended by this provision. “Sales” should be limited to those instances where a third party obtains independent rights to ongoing use of Personal Information in exchange for actual monetary consideration. Additionally, in order to avoid a disruption to the online advertising ecosystem, which this

Act does not appear intended to reach, the Attorney General should clarify that disclosures for such specified purposes in connection with the delivery, measurement, and auditing of online advertising are outside the scope of what constitutes a “sale.”

Proposed Regulatory Language

For purposes of paragraph (1) of subdivision (t) of Section 1798.140 of the Act, “valuable consideration” shall mean selling, renting, releasing, disclosing, disseminating, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to a third party, directly in exchange for money or monetary consideration to the business providing the personal information. Personal information is not “sold” where the disclosure of the personal information is necessary for or incidental to the delivery, display, measurement, customization, auditing or analysis of an advertisement.

Specific Pieces of Information. The Attorney General should clarify that companies are not required to provide specific pieces of information to consumers in response to an access request, especially if doing so would create an unreasonable risk to the security of that information. Indeed, the California legislature has recognized the importance of data security as it relates to certain data elements as outlined in 1798.81.5 in California law, which is also referenced in the Act in Section 1798.150.

Proposed Regulatory Language

Under no circumstances shall a business be required to provide a consumer with specific pieces of personal information if such disclosure unreasonably risks the security of that personal information, the security of the consumer’s account with the business, or the security of the business’s services, systems or networks, including but not limited to personal information as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5.

Exceptions and Exclusions

Employee data. The Attorney General, through regulatory language proposed below, can clarify that section 1798.140 does not cover personal information collected by a business in connection with an individual’s role as an employee. Making this clarification is consistent with the Act and ensures that the CCPA would not impact and conflict with the already existing framework in California for employee access to their employment information.¹

Proposed Regulatory Language

For purposes of paragraph (1) of subdivision (o) of Section 1798.140 of the Act, information shall not constitute “personal information” where the information is collected by a business from an employee, applicant, or recruitment candidate and the information relates to the person’s employment or application for employment with the business.

Exclusion of other non-consumer data. In addition to excluding personal information collected in the employment context as noted above, the Attorney General should similarly clarify that personal

¹ See e.g., [Labor Code 1198.5](#) and corresponding Department of Industrial Relations guidance available at https://www.dir.ca.gov/dlse/FAQ_RightToInspectPersonnelFiles.htm; [Labor Code 226\(b\)](#), and [Labor Code 432](#).

information does not include personal information collected in connection with an individual's role as a director, agent, independent contractor or vendor of a business.

Proposed Regulatory Language

For purposes of paragraph (1) of subdivision (o) of Section 1798.140 of the Act, information shall not constitute "personal information" where the information is collected by a business in connection with an individual's or entity's role as a director, employee, agent, independent contractor or vendor of a business or when an individual is acting on behalf of a business.

Right to Know. Currently in the CCPA there are no exceptions in the right to know unlike in the right to delete. Personal information often empowers businesses with data in order to protect people. For example, information is used for risk, authentication, security, and safety to protect people from bad actors. The CCPA, as currently written and without clarity, could allow bad actors to request their personal information under the CCPA's right to know and bad actors would be able to gain information businesses have on them to bifurcate the security, especially in e-commerce, and safety systems harming the rest of the community that the business serves. For example, a business may want to exclude convicted rapists, pedophiles, and fraudsters from being allowed into people's homes. Exceptions should be made within the CCPA for personal information, such as identifiers and characteristics, from a consumer's right to know under 1798.100 that match the exceptions for the right to deletion in order to address this potential abuse.

Federal law. Although 1798.196 includes certain application limitations for the Act, with respect to access requests made by consumers, the Attorney General should further clarify that a business is not required to make disclosures in violation or in conflict with federal law.

Proposed Regulatory Language

Pursuant to paragraph (1) of subdivision (a) of Section 1798.145, a business shall not be required to disclose any personal information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household if such disclosure would violate or conflict with any federal law or regulation, including any order issued by a federal agency.

Opt-Out and Information Request Mechanisms

"Do Not Sell My Personal Information" link location. Due to an ambiguity as to where this link needs to appear, resulting from the language in Section 1798.135(a), coupled with the definition of "homepage" in Section 1798.140(l), the Attorney General, through the regulatory language proposed below, can resolve such ambiguity. In particular, when a business or a brand does not maintain what may be traditionally perceived as a "homepage," flexibility is needed as to where such a link should be placed in order to best reach consumers. For example, it may make sense for the opt-out choice to be offered alongside or in conjunction with a company's privacy policy or page, as that is the location that consumers generally visit to learn about their choices and manage any offered preferences.

Proposed Regulatory Language

A business shall be deemed in compliance with paragraph (1) of subdivision (a) of Section 1798.135 of the Act where the business places the "Do Not Sell My Personal Information" link

or logo on a privacy page clearly and conspicuously posted on the business's Internet Web site or within an online service, such as a mobile application.

"Do Not Sell My Personal Information" choices. The Attorney General should clarify that a business may comply with Section 1798.20 by providing a consumer with the ability to make more granular opt-out choices with respect to the sale of information, so long as there is also an option to opt-out of all sales. This interpretation is consistent with the approach in the federal Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM ACT). The CAN-SPAM Act, which requires the ability to opt-out of certain email messages, allows the initiator of such messages to offer recipients the opportunity to choose the specific types of messages the recipient wants to receive or not receive, so long as an option to not receive any commercial electronic mail messages from the sender is also made available.²

Proposed Regulatory Language

A business that is required to comply with Section 1798.120 may comply by providing the consumer a list or menu from which the consumer may choose different types of sales, categories of third parties, or other options, provided that the list or menu includes an option under which the consumer may choose to opt out of all sales of the consumer's personal information.

"Do Not Sell My Personal Information" safe harbor for opt-in choices. The Attorney General should clarify that if a business engages in the sale of personal information pursuant to an individual's opt-in consent only, such sales need not be included as part of the global "Do Not Sell My Personal Information" choice that is required under the law. Any interpretation to the contrary results in a disincentive for businesses to engage in sales only following opt-in consent. If a customer opting in to sales would then be reversed by the required "global" "Do Not Sell My Personal Information" choice, companies will lack incentive to offer opt-in choices. Moreover, consumers would not expect that if they had affirmatively opted-in to particular program, that it would be "undone" by a global "Do Not Sell My Personal Information" choice. A consumer would expect to interface with the company specifically as it relates to that program if they decide to no longer opt in. Accordingly, so long as businesses provide individuals with a mechanism to subsequently opt-out of sales for which they had previously opted in, such opt-out need not be included in the global "Do Not Sell My Personal Information" choice.

Proposed Regulatory Language.

A business shall be deemed in compliance with Section 1798.135 of the Act and shall not need to provide the "Do Not Sell My Personal Information" link or logo where the business requires the consumer to opt in to the sale of personal information and provides the consumer a mechanism to subsequently opt out.

Notices

² 15 U.S.C. § 7704(a) (3) (B). *"More detailed options possible. The person initiating a commercial electronic mail message may comply with subparagraph (A)(i) by providing the recipient a list or menu from which the recipient may choose the specific types of commercial electronic mail messages the recipient wants to receive or does not want to receive from the sender, if the list or menu includes an option under which the recipient may choose not to receive any commercial electronic mail messages from the sender."*

Disclosures to consumers. Section 1798.115 sets forth what companies have to disclose to consumers, upon a verifiable request, with regard to personal information that is sold or disclosed for a business purpose. 1798.115(a)(2) requires businesses to provide consumers with the categories of personal information sold, as well as the categories of third parties to whom the information was sold. The section then continues and says that this disclosure has to correlate the categories of personal information to each third party. Since the requirement is only for the disclosure of categories of third parties, the correlation of the categories of personal information is intended to be to the categories of third parties. However, as noted, because of the ambiguity of the language, there exists a lack of clarity on what is in fact required.

Proposed Regulatory Language

Pursuant to paragraph (2) of subdivision (a) of Section 1798.115, a business shall not be required to correlate the categories of personal information sold to each third party to whom the information was sold. A business shall be in compliance with the paragraph if it correlates the categories of personal information sold to the categories of third parties to whom information is sold.

Financial Incentives

The Attorney General should adopt a simple rule that, consistent with the statute, explicitly permits the use of financial incentives. Any specific rules or requirements that the Attorney General puts in place that have the effect of hampering the ability of companies to offer consumers the benefits that come from consumer-friendly programs like frequent buyer programs, or other discounted offerings, would run contrary to the law and place these programs and the benefits consumer derive from them at risk.

Verifiable Consumer Request

The Act requires businesses to take certain action upon receipt of a “verifiable consumer request.” This presents significant, material security and privacy concerns for consumers that the Attorney General needs to address. Verification is critically important to ensure that information about a consumer is only released when identity can be confirmed. Businesses should have flexibility in how they verify such consumers and requests, and specific methods should not be delineated. This will allow for the development of innovative methods to ensure that information is not incorrectly disclosed. Considering the potential harm if information about a consumer is disclosed to the wrong consumer, businesses should have the discretion to determine whether a consumer has been properly verified, particularly when the consumer does not hold an account with the business. Very often, businesses verify individuals during the course of account formation – when an account is lacking, verification is more difficult. Businesses should be erring on the side of caution and should not disclose information when a consumer has not been properly verified.

The Attorney General should, in its regulations, outline a business’s requirements with respect to verifying consumer requests and clarify that if a business is unable to verify a request that they communicate that to the consumer. In addition, the Attorney General should clarify the role of service providers in connection with access and deletion requests, by clarifying how service providers should respond to such requests, and how they should provide assistance to businesses.

The Attorney General should also outline that a request from a consumer (or authorized third party) does not require the business to re-identify data that has been de-identified, pseudonymized, or

otherwise stripped of any data that may connect it to the requesting party. Holding otherwise may force companies to take steps that are detrimental to the privacy of individuals.

Proposed Regulatory Language

(i) A business shall establish a reasonable and accessible method, based on the sensitivity of the personal information requested, the nature of the business's products or services, the risk of unauthorized access to the consumer's personal information, and whether the consumer has an account or registration with the business, for verifying that a consumer making a request to exercise rights under the Act is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf. If the business cannot reasonably verify the consumer's request based on the information provided, then the business shall send the consumer, or the person authorized by the consumer to act on the consumer's behalf, an explanation that the consumer's identity could not be verified.

(ii) If a service provider receives a request from a consumer, the service provider may respond with an explanation that the request should be submitted to the business with the direct relationship with the consumer, if known. The service provider shall, taking into account the nature of the processing and the relationship with the business, upon the business's request, assist the business in fulfilling the business's obligation to respond to the consumer's request, insofar as this is reasonably possible.

Data Retention

In its regulations, the Attorney General should clarify that there is no obligation for a business to retain personal information solely for the purposes of fulfilling a consumer request under the Act. Although 1798.100(e) states that a business is not required to retain certain personal information, the Attorney General should make a clarification to cover all the obligations under the Act. Any interpretation to the contrary would actually create additional privacy and security risk to personal information, by potentially requiring organizations to retain data that they otherwise would not.

Proposed Regulatory Language

Under no circumstances is a business required to retain personal information solely for the purpose of fulfilling a consumer request made under the Act.

Effective Date

The effective date of the Act is January 1, 2020, however, it is ambiguous as to when access obligations would start to "run" with regard to a business's obligations to disclose how information is processed, shared or sold. Accordingly, the Attorney General should clarify that those obligations apply on a prospective basis, as of January 1, 2020.

Proposed Regulatory Language

A business must comply with a consumer request made under the Act only as it pertains to data collected, processed, disclosed, or sold by the business after January 1, 2020.

TechNet thanks you for taking the time to consider these issues and proposed regulatory language. Again, we believe these suggestions will go a long way toward providing businesses and consumers

clarity with regards to the CCPA. Such guidance would help facilitate compliance on the part of businesses, while ensuring that consumers have clear expectations about what companies are and are not allowed to do with personal information.

If you have any questions regarding this comment letter, please contact Courtney Jensen, Executive Director, at [REDACTED] or [REDACTED]

Thank you,
Courtney Jensen
Executive Director, California and the Southwest
TechNet

Message

From: Friedrich, Kate (TR General Counsel) [REDACTED]
Sent: 3/5/2019 12:22:36 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Friedrich, Kate (TR General Counsel) [REDACTED]
Subject: Thomson Reuters Written Comments to CA Department of Justice/Atty General CCPA Pre-Rulemaking
Attachments: Thomson Reuters Comment Ltr to CA Dept of Justice Final.pdf
Importance: High
Flag: Follow up

Attached please find Thomson Reuters written comments in response to the Attorney General's CCPA Public Fora (pre-rulemaking phase). If you have any questions, please do not hesitate to be in contact with me.

Sincerely,

Kate Friedrich
Vice President, Global Government Affairs

Thomson Reuters

the answer company

[REDACTED]
thomsonreuters.com



THOMSON REUTERS

March 5, 2019

Via Email and Mail

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

RE: CCPA Regulations

To Whom It May Concern:

Thomson Reuters appreciates the opportunity to provide these comments in connection with the Attorney General's rulemaking to implement the California Consumer Privacy Act ("CCPA"). Thomson Reuters provides important legal, regulatory, and business information to our law enforcement, government, and business customers through Westlaw (our core online legal research service), our CLEAR (Consolidated Lead Enforcement and Reporting) service, and our similar services. Our customers use these information services for a variety of purposes that promote the public interest, including to find missing children, investigate money-laundering activity, prevent and investigate criminal and terrorist activities, verify identities to prevent fraud, investigate fraud, comply with laws and regulations (such as "know your customer" requirements), and prepare for litigation (e.g., locating witnesses). Thomson Reuters must make information from publicly-available records and other sources commercially available so that its customers can use it for these important public interest purposes.

We commend the Attorney General for its diligence in soliciting feedback from the public to ensure that the statute, as interpreted and applied through the Attorney General's regulations, is both effective in protecting consumers' privacy and workable in practice. Below, we respectfully ask that the Attorney General make several clarifications through its implementing regulations to achieve this goal:

- reinforce existing exemptions for law enforcement, fraud prevention, and similar public interest purposes;
- refine when "publicly available" information will be deemed to be "personal information" under the statute;
- clarify the "explicit notice" requirement for third-party sales of personal information;
- harmonize the meaning of "consumer" with existing California privacy laws;
- reiterate that the CCPA does not interfere with the application of other financial privacy laws;





- avoid interpretations that would enable bad actors to use the CCPA's opt-out to frustrate the "sale" of personal information for anti-fraud and similar public interest purposes;
- provide additional detail as to what information must be disclosed to consumers upon their request;
- clarify how the law will apply to the definition of "personal information";
- permit businesses to tailor verification methods to their industry; and
- specify that government is not a "person" for purposes of the CCPA.

Each of these requests is discussed in more detail in the following sections.

I. Reinforce existing exemptions for law enforcement, fraud prevention, and similar public interest purposes.

Section 1798.185(a)(3) empowers the Attorney General to implement regulations "necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights." The CCPA clearly intended to ensure that private litigants, potential defendants, law enforcement agencies, and other authorities were free to investigate and enforce legal violations and claims. See §§ 1798.145(a)(1)-(4). It also intended to ensure that businesses could continue meeting their legal obligations and exercising all their rights under federal, state, and local law. § 1798.145(a)(1).

Nevertheless, the current text of the CCPA potentially could be interpreted in a manner that falls short of these goals. Specifically, § 1798.145(a)(2) permits businesses to comply with outreach from authorities *only* if that outreach has the force of law behind it, and there is no specific language protecting a business' abilities to voluntarily comply with law enforcement requests where permissible. Section 1798.145(a)(3) appears to be similarly narrow. It protects a business' ability to cooperate with law enforcement agencies regarding illegal activity, but does not explicitly recognize that a business may need to provide personal information about consumers in connection with a civil or investigatory matter to courts, legal professionals, or investigators. And while § 1798.145(a)(4) does give a business the ability to exercise or defend legal claims, no exception explicitly protects a business' ability to detect or prevent fraud or other unlawful activity, conduct lawful screening and vetting activities, or verify identities.

Moreover, because the scope of the public interest exemptions within the statute are uncertain, they leave businesses (like Thomson Reuters) that are trying to protect consumers and further the public interest activities of government, law enforcement, and other businesses at risk of engaging in illegal conduct when they do so. Unintentionally, the law thereby prioritizes consumers' choices about the use of their data at the risk of limiting public protection. To enable industry to continue cooperating with government agencies, law enforcement, and other customers by making personal information commercially available for purposes that promote the public interest, businesses need clear exceptions that permit the broad collection, use, disclosure, and sale of personal information in connection with legal and investigatory matters. These businesses also need protection when they are detecting and preventing unlawful activity, screening, and verifying identities. Accordingly, Thomson Reuters encourages the Attorney General to enact the following language in its regulations:



Nothing in this title shall apply to personal information collected, processed, sold or disclosed in order to (i) respond to requests from law enforcement; (ii) provide personal information to courts, legal professionals, or investigators, concerning conduct or activity that the entity reasonably and in good faith believes may be related to a legal or investigatory matter; (iii) detect or prevent fraud or other unlawful activity; (iv) conduct lawful screening activity; (v) verify identities; or (vi) help another entity engage in the activities identified in this section.

II. Refine when “publicly available” information will be deemed to be “personal information” under the statute.

Section 1798.185(a)(1) authorizes the Attorney General to update the categories of “personal information” under § 1798.140(o) in order to address “obstacles to implementation.” The definition of “publicly available” information in § 1798.140(o)(2) creates significant compliance challenges and frustrates the goals of the CCPA because it is unnecessarily narrow. As explained below, the Attorney General’s regulations can clarify the meaning of this definition to avoid this issue.

Under the current text of the CCPA, “publicly available” information is excluded from the definition of “personal information” to ensure that businesses continue to have broad access to information that governments and other entities have decided should be made widely accessible to the public, for the benefit of the public. However, the statute appears to impose additional conditions that would substantially diminish the circumstances in which publicly available information will be carved out from the statutory requirements. For example, the language could be interpreted to require that there be conditions associated with such publicly-available information. Therefore, if a government agency wants to make information public, it would have to jump through hoops -- making sure that there is a condition associated with the information to take the information outside the scope of “personal information” regulated by the statute. Additionally, the CCPA’s definition of “publicly available” information requires that the publicly available information be used only for purposes that are compatible with the purposes for which the personal information is publicly maintained, regardless of whether the government agency or entity wanted to subject the publicly available information to such a condition.

At best, these restrictions create an arbitrary and subjective test for determining whether information is “publicly available.” At worst, limiting the use of such information could chill activities that are protected under the First Amendment and depend on the use of publicly available information. For example, although census data is published to ensure that each community gets an appropriate number of representatives in government, it is also used for a wide variety of secondary research and other purposes. Requiring entities to use publicly available information consistent with the “purpose for which the data is maintained” therefore imposes significant regulatory burdens on the public and the business community without conferring any meaningful benefit to consumers. Once a governmental entity makes the decision that information should be made public, it determines that consumers will not be harmed by having this information widely accessible by the public. This level of scrutiny is



sufficient to ensure that consumers' privacy is protected, while also balancing the public's interest in publicly available data and free speech.¹

For these reasons, Thomson Reuters asks that the Attorney General enact the following language in its regulations clarifying the statute's definition of "personal information:"

The following is a non-exhaustive list of conditions which satisfy § 1798.140(o)(2)'s requirement that "publicly available" information have associated conditions (i) if the information is found in a specific format- including electronic or hard-copy form, (ii) if viewings of the information must be conducted at a specific time (e.g. during normal business hours at a government office), (iii) if you have to go to a specific place to view the information (e.g. a government office or government website), or (iv) if a party has to request a copy of the information to view it.

With regards to § 1798.140(o)(2), the purpose of a use is not compatible with the purpose for which the data is maintained and made available in the government records, or for which it is publicly maintained, only if the purpose of the use directly contradicts the stated purpose for which the data is maintained.

III. Clarify the "explicit notice" requirement for third-party sales of personal information.

Section 1798.185(a)(6) authorizes the Attorney General to establish "rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer." Section 1798.115(d) prohibits third parties from selling a consumer's personal information unless the consumer received explicit notice and the opportunity to opt out of the sale. However, the law is silent regarding which entity is responsible for providing this notice and consent mechanism to the consumer. This ambiguity could lead to an unintended outcome in which the average consumer is inundated with notices regarding the sale of their information from businesses with which that consumer is not familiar, becomes overwhelmed, and is therefore not able to effectively exercise his or her right to opt out of the sale of personal information.

To prevent overwhelming consumers and confusing them, the business that has the direct relationship with the consumer from which a given piece of data originated should be responsible for providing the consumer with notice and the opportunity to opt out of the sale of that piece of data. Accordingly, Thomson Reuters proposes the following language:

¹ Notably, these conditions were not part of the ballot initiative that motivated the CCPA. Instead, the ballot initiative defined publicly available information as "information that is lawfully made available from federal, state, or local government records or that is available to the general public. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge." CCPA Ballot Initiative §1798.106(b).



The party responsible for providing a consumer with explicit notice, and the opportunity to opt out, of a third party's sale of certain data is the party with the direct relationship with the consumer from which that data originated. The third party must disclose in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its Internet Web site, the category or categories of consumers' personal information it has sold.

IV. Harmonize the meaning of "consumer" with existing California privacy laws.

Section 1798.185(a)(3) empowers the Attorney General to adopt regulations "necessary to comply with state or federal law." When enacting the CCPA, the California legislature cited several examples of other existing California consumer privacy laws, which collectively laid the foundation for consumer privacy in California. CCPA Legislative Findings § 2(b). However, the CCPA's definition of "consumer" could be interpreted in ways that are incongruent with these other California privacy laws.

Specifically, the CCPA's definition of "consumer" appears to include individuals who interact with businesses as employees or independent contractors. This unprecedented expansion moves the CCPA out of line with how a consumer is understood under existing California privacy law.² In order to ensure consistency with other California privacy requirements and to help avoid creating an inefficient and inconsistent set of compliance mechanisms for businesses, Thomson Reuters asks the Attorney General to interpret the definition of "consumer" as follows when enforcing the CCPA's requirements:

An individual is a consumer if he or she provides personal information to a business during the creation, or throughout the duration, of an established business relationship if the business relationship is primarily for personal, family, or household purposes.

V. Reiterate that the CCPA does not interfere with the application of other financial privacy laws.

As previously noted, § 1798.185(a)(3) directs the Attorney General to adopt regulations "necessary to comply with state or federal law." Currently the exemption in § 1798.145(e) applies to personal information collected, processed, sold, or disclosed "pursuant to" the Gramm-Leach-Bliley Act (GLBA) and the California Financial Information Privacy Act (CFIPA). Entities regulated by the GLBA and CFIPA sometimes disclose personal information to other businesses (such as Thomson Reuters) who are not themselves subject to these laws but must treat the information received subject to the GLBA's and CFIPA's restrictions.

² See Cal. Civil Code § 1798.80(c) ("Customer" means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business); Cal. Civil Code § 1798.83(e)(1) ("Customer" means an individual who is a resident of California who provides personal information to a business during the creation of, or throughout the duration of, an established business relationship if the business relationship is primarily for personal, family, or household purposes.").



Consequently, the Attorney General should clarify in the CCPA regulations so that it is unambiguous that an entity that receives information subject to GLBA or CFIPA restrictions are exempt under the CCPA to the extent they process such regulated information. Specifically, the Attorney General's regulations should state the following:

This title shall not apply to personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code).

- VI. Avoid interpretations that would enable bad actors to use the CCPA's opt-out to frustrate the "sale" of personal information for anti-fraud and similar public interest purposes.**

Section 1798.185(a)(4) requires the Attorney General to issue regulations to govern consumers' submissions of opt-out requests, business' compliance with opt-out requests, and the opt-out button or logo that businesses must provide. Because the opt-out right is specific to the sale of the consumer's information, the Attorney General should clarify the definition of "sale" under this section to ensure that bad actors cannot opt out of disclosures of their information in ways that facilitate fraudulent, malicious, or unlawful activity.

For example, a business might discover that an individual was using another person's credit card in an unauthorized manner. Because the CCPA's definition of "personal information" is so broad, the fact that a bad actor was using another person's credit card relates to the bad actor and therefore is the bad actor's "personal information" under § 1798.140(o)(1). It clearly would not promote the goals of privacy and security if a business is required to allow the bad actor to opt out of having their personal information sold to other businesses whose purpose is to help these other businesses detect, prevent, and investigate other suspected fraudulent activity.

To avoid this unintended outcome, Thomson Reuters suggests adopting the following regulation:

A party does not sell a consumer's personal information when the personal information is collected, used, or disclosed to (1) provide services to federal, state, or local authorities, legal professionals, or investigators for lawful purposes or (2) exercise or defend legal claims, detect or prevent fraud or other unlawful activity, conduct lawful screening and vetting activities, or for identity verification.

- VII. Provide additional detail as to what information must be disclosed to consumers.**

Section 1798.185(a)(7) directs the Attorney General to establish "rules and procedures to further the purposes of Sections 1798.110 and 1798.115," which are the data access provisions. Currently, the CCPA does not provide clear instruction to businesses regarding how they can comply with these requirements. Although one interpretation could be that businesses must provide a copy of the personal information maintained about and requested by the consumer,



this interpretation does not appear to be intended by the legislature for at least two reasons. First, if businesses are required to provide a list of categories of the information it has collected about a particular consumer, this would create (in essence) a road map that a threat actor targeting a particular consumer could use to more easily canvas what information the business has and use that information to decide how best to access and retrieve the consumer's data. Secondly, if a business is required to disclose a copy of all the pieces of personal information that is maintained, a threat actor could gain sufficient information to verify a consumer's identity across many services, allowing the attacker to gain access to the consumer's data across those other services and creating more risk to the consumer. In order to effectively thwart this type of threat actor activity, Thomson Reuters offers the following language for your consideration:

If a business discloses the categories relevant to all consumers, that disclosure is sufficient to satisfy the business' obligations under §§ 1798.100(a)-(b), 1798.110(a)(1)-(2), 1798.110(a)(4), 1798.110(c)(1)-(2), 1798.110(c)(4), 1798.115(a)(1)-(3), 1798.130(a)(3)(B), and 1798.130(a)(4)(B)-(C). If a business discloses a list describing the specific pieces of information the business collects, the business satisfies its obligations under §§ 1798.100(a), 1798.110(a)(5), and 1798.110(c)(5).

VIII. Clarify how the law will apply to the definition of "personal information."

As previously discussed, § 1798.185(a)(1) authorizes the Attorney General to edit the categories of "personal information" under § 1798.140(o) in order to address "obstacles to implementation." Currently, the CCPA defines "personal information" as information that is "capable of being associated" with a particular consumer or household. Because any information *theoretically* could be associated with a consumer or household, this provision, unfortunately, has the effect of categorizing any information a business collects that is only tangentially related to a consumer as personal information, regardless of whether the unauthorized access to that information would actually harm the consumer. To avoid this unreasonably expansive conception of personal information, Thomson Reuters asks the Attorney General to clarify through the following regulation:

Information is capable of being associated with a particular consumer if a business can reasonably link the personal information to a particular consumer.

IX. Permit businesses to tailor verification methods to their industry.

Section 1798.185(a)(7) requires the Attorney General to issue regulations governing "a business's determination that a request for information received by a consumer is a verifiable consumer request." As drafted, the CCPA requires all businesses to verify consumer requests. However, the CCPA does not take into account that different businesses already rely on a variety of existing methods to identify and verify their customers, based (for example) on the sensitivity of the information being accessed and the nature of the business.



However, the CCPA does not take into account that different businesses already rely on a variety of existing methods to identify and verify their customers, based (for example) on the sensitivity of the information being accessed and the nature of the business.

Consequently, the Attorney General should avoid enacting prescriptive regulations that could unnecessarily supplant existing verification procedures and instead provide businesses flexibility to use any reasonable verification method:

A business must establish a reasonable method for verifying its consumers' identities within a reasonable period of time for purposes of fulfilling consumers' requests to exercise their rights under the statute. If, after the consumer completes the verification process, the business does not have a reasonably high level of confidence that the requesting party is the consumer about whom the business collected personal information, then the business need not comply with the consumer's request but must send an explanation to the consumer explaining that the consumer's identity could not be verified.

X. Specify that government is not a "person" for purposes of the CCPA.

Section 1798.185(b) authorizes the Attorney General to "adopt additional regulations as necessary to further the purposes of this title." It is clear that the purpose of the title is to regulate how businesses share consumers' personal information with other commercial entities. CCPA Legislative Findings § (2)(i)(2). However, as written, the CCPA potentially could be interpreted to also apply to a business' sale of personal information to governmental entities. Specifically, the CCPA defines a "third party" as a "person" that does not satisfy certain conditions. CCPA § 1798.140(w). The law defines the term "person" as follows:

"Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

§ 1798.140(n). As drafted, the CCPA does not expressly define governmental entities, nor does it purport to impose any obligations on governmental entities with respect to processing consumers' personal information. One possible interpretation of the phrase "any other organization or group of persons acting in concert" is that it could cover a governmental entity. To avoid a broader application of the CCPA than was intended, and to help ensure that government agencies and law enforcement can continue to receive personal information that is needed to conduct their public interest activities, Thomson Reuters requests that the AG adopt the following regulation:

A governmental entity does not constitute a "person" for purposes of this title.

* * *



THOMSON REUTERS

Thomson Reuters appreciates the opportunity to provide these comments to assist the Attorney General with the adoption of regulations related to the CCPA and welcomes the opportunity to discuss any of the above points further. We are committed to protecting consumers' privacy, while also continuing to serve the public interest by protecting public safety, and we look forward to working with the Attorney General toward this common goal.

Sincerely,

Steve Rubley
Managing Director, Government Segment

Message

From: Determann, Lothar [REDACTED]
Sent: 3/9/2019 11:00:21 AM
To: Lisa Kim [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Lisa Kimf4f]; Stacey Schesser [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Stacey Schesser131]
Subject: letter to legislature
Attachments: Determann Letter to legislature re. CCPA corrections final 2019-3-8.pdf

Also, separately, attached is my open letter to the legislature on technical error corrections, please let me know your thoughts and if you have any questions.

This message may contain confidential and privileged information. If it has been sent to you in error, please reply to advise the sender of the error and then immediately delete this message. Please visit https://urldefense.proofpoint.com/v2/url?u=http-3A__www.bakermckenzie.com_disclaimers&d=DwIFAw&c=uASjV29gZuJt5_5J5CPRuQ&r=6KsThfIRVOY8401451xSKyd3fNlVHCA7PtD2SlHcFuE&m=rbaUMvtE855cEaw2FAFXEDUrnuQeQTreZAaI5hpCo4E&s=KbSg-hS5sZQJpaixiyxVYEHsqnhy-VX0o7j5q3qsucc&e= for other important information concerning this message.

-----Original Message-----

From: Determann, Lothar
Sent: Saturday, March 09, 2019 10:52 AM
To: 'Lisa Kim'; Stacey Schesser
Subject: RE: CCPA regs

Yes, Lisa, can you access the attachment?

Copying it also into the email body, I recommend that the Attorney General includes in regulations to further the purposes of Cal. Civ. Code §1798.185(a)(3) a provision according to which

No business shall be obligated under the California Consumer Privacy Act to disclose, destroy or forego a trade secret, as defined and protected under 18 U.S. Code §1839[3] or Cal. Civ. Code § 3426.1[d]); copy, distribute or destroy a work of authorship protected under 17 U.S.C. §102(a), or otherwise forego or compromise intellectual property rights under applicable law, including U.S. Federal or California law.

Such a provision is necessary, because the rights under Cal. Civ. Code §1798.100(d) and other sections of the California Consumer Privacy Act are not sufficiently limited and Cal. Civ. Code §1798.185(a)(3) calls upon the California Attorney General to establish exceptions relating to trade secrets and intellectual property rights. While deletion rights are subject to a number of exceptions under Cal. Civ. Code §1798.105(d), these do not yet sufficiently take property rights under Federal and State laws into account. Access rights under Cal. Civ. Code §1798.100(d) are not expressly limited at all. Without limitations in regulations, this would have very harmful consequences, which are not justifiable by potential benefits for privacy, for example, if individuals demand from employers, schools, universities, concert halls, newspapers, grocery stores and any other business copies or deletion of any personal information (excessively broadly defined to include any information relating to a California resident) in any emails, security camera footage, audio recordings or information in structured or unstructured data pertaining to them, which may be contained in confidential whistleblower reports, company-internal investigation memos, technical research and development notes, paintings, photos, unpublished journalistic articles, concert performances, data bases with information for training of artificial intelligence or self-driving cars, recorded university lectures, exam evaluations, team work in school, panel discussions at conference, and numerous other instances. Without meaningful limitations, unfettered information access and deletion rights will mean the end of confidential communications and have grave chilling effects on free speech, art, journalism, education, intellectual property and other valued features of our society and economy. I submit this proposal on my own behalf, not on behalf of my law schools, law firm, clients or others. Lothar Determann

-----Original Message-----

From: Lisa Kim [REDACTED]
Sent: Tuesday, March 05, 2019 9:13 AM
To: Determann, Lothar; Stacey Schesser
Subject: [EXTERNAL] RE: CCPA regs

Thanks Lothar. Did you mean to attach something or just that you will prepare something? Thanks.

Lisa

From: Determann, Lothar [REDACTED]
Sent: Monday, March 4, 2019 7:20 PM
To: Stacey Schesser; Lisa Kim
Subject: CCPA regs


Hi Stacey and Lisa,

Good seeing you today. Given your interest, I prepare a submission regarding exceptions to data access rights based on Cal. Civ. Code §1798.185(a)(3).

Please let me know if you have any questions.

Best regards,
Lothar

This message may contain confidential and privileged information. If it has been sent to you in error, please reply to advise the sender of the error and then immediately delete this message. Please visit [CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient\(s\). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.](https://urldefense.proofpoint.com/v2/url?u=http-3A__www.bakermckenzie.com_disclaimers&d=DwMFAw&c=uASjV29gZuJt5_5J5CPRuQ&r=6KsThfIRVOY8401451xSKyd3fNlVHCA7PtD2S1HcFuE&m=jUjFzhts5_juA-JZkaV4GUeNKIibAFtxYm4LFHHQzwo&s=18fQPewzs9prchM48pr14gdzHAPppux2ozmM8RL7Rq4&e=>https://urldefense.proofpoint.com/v2/url?u=http-3A__www.bakermckenzie.com_disclaimers&d=DwIFAW&c=uASjV29gZuJt5_5J5CPRuQ&r=6KsThfIRVOY8401451xSKyd3fNlVHCA7PtD2S1HcFuE&m=rbaUMvtE855cEaw2FAFXEDUrnuQeQTreZAaI5hpCo4E&s=KbSg-hS5sZQJpaixiyxVYEHsqnhy-VX0o7j5q3qsucc&e=<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.bakermckenzie.com_disclaimers&d=DwMFAw&c=uASjV29gZuJt5_5J5CPRuQ&r=6KsThfIRVOY8401451xSKyd3fNlVHCA7PtD2S1HcFuE&m=jUjFzhts5_juA-JZkaV4GUeNKIibAFtxYm4LFHHQzwo&s=18fQPewzs9prchM48pr14gdzHAPppux2ozmM8RL7Rq4&e=> for other important information concerning this message.</p></div><div data-bbox=)

Lothar Determann
2 Embarcadero Center, 11th Floor
San Francisco, CA 94111


San Francisco, March 8, 2019

Assemblymember Ed Chau, Chair
Assembly Privacy and Consumer Protection Committee
State Capitol, Room 5016
Sacramento, CA 95814

Re. California Consumer Privacy Law Corrections

Dear Chairman Chau,

As one of the principal commentators, scholars, teachers and advisors on California privacy law, I want to first congratulate you and the California Legislature on the passage of many innovative and cutting-edge information privacy and security laws over the years, making California one of the leading jurisdictions globally, as I frequently note in my publications and presentations.

To maintain this leadership position, I respectfully recommend that you and your staff consider advancing a number of technical corrections to the California Consumer Privacy Act of 2018 ("CCPA") and to other California privacy laws that have become obsolete or redundant due to the passage of the CCPA. In making these recommendations, I do not mean to comment on any bills or proposals intended to substantively modify the CCPA.

What I do propose in this letter are strictly technical corrections that are urgently necessary: necessary to rationalize and harmonize California's myriad privacy statutes; necessary to keep California in its leadership role as one of the most advanced and innovative jurisdictions worldwide when it comes to information technologies and privacy laws; necessary to make a compelling case against broad federal statutory preemption; necessary to allow businesses to understand and comply with applicable law; and necessary to achieve the very purpose of privacy laws – to protect the personal information of the people of California. I would welcome an opportunity to meet with your staff to go over my proposals.

First, the California Legislature *should correct all remaining typographical and other manifest errors in the CCPA* (the presence of which is understandable given the fast track legislative history and ballot initiative background), including the following:

- Cal. Civ. Code §1798.100(e) and Cal. Civ. Code §1798.110(d)(1) should be deleted as they contradict the remainder of the CCPA. These sections each state "This section shall not require a business to retain any personal information," but no provision of the CCPA requires any business

to retain any information, and the general approach of the CCPA is to encourage minimization of information collection/retention.

- In Cal. Civ. Code §1798.105(d)(1), the words "perform actions that are" should be inserted immediately before the words "reasonably anticipated."
- Cal. Civ. Code §1798.110(c)(5) states, "A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130: The specific pieces of personal information the business has collected about that consumer." In the interest of data privacy, "specific pieces of information" should not be disclosed in an online privacy policy, on the website of a company, but rather only "categories" of personal information as contemplated in 1798.110(c)(1). Accordingly, subsection 1798.110(c)(5) should be deleted.
- Cal. Civ. Code §1798.120(c) states "... the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age" This results in an inconsistent rule for 16 year-olds, which could be avoided by revising the clause to read "consumer who is at least 13 but not yet 16 years of age."
- In Cal. Civ. Code §1798.125(a)(2) and (b)(1) "... value provided to the consumer by the consumer's data" should be corrected to read "... value provided to the business by the consumer's data."
- The reference in Cal. Civ. Code §1798.140(b) to "an individual's deoxyribonucleic acid (DNA)" is erroneous because DNA is not data but rather human material from which data can be obtained. This error could be corrected by deleting this reference, as information about DNA is covered sufficiently by other categories as "personal information."
- Cal. Civ. Code §1798.140(d)(7): The words "manufactured for" should be deleted from the phrase, "that is owned, manufactured, manufactured for, or controlled by the business."
- Cal. Civ. Code §1798.140(k): The definition of "Health insurance information" should be deleted as this term is not used elsewhere in the CCPA.
- In Cal. Civ. Code §1798.140(o)(2), the sentence, "'Publicly available' does not include consumer information that is deidentified or aggregate consumer information" should be corrected by replacing the term "Publicly available" with the term "Personal information."
- Cal. Civ. Code §1798.140(s)(9): In the sentence, "Subjected by the business conducting the research to additional security controls limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose," the word "that" should be inserted immediately before the word "limit."
- Cal. Civ. Code §1798.140(o)(2) reads, "For these purposes, 'publicly available' means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information." The last phrase ("if any ...") is incomplete and should be deleted.
- Cal. Civ. Code §1798.145(a)(6): The last sentence (including "shall not permit a business from storing") should be deleted.
- In Cal. Civ. Code §1798.145(c)(1)(B), the term "patient information" should be replaced by the term "personal information." If a business voluntarily protects any personal information as if it were subject to the strict rules of HIPAA or CMIA, it should not also have to comply with the CCPA. Also, the term "patient information" is not defined.

Second, *the California Legislature should consider repealing or updating all other California privacy laws that the CCPA subsumes*, including the following:

- Cal. Civ. Code § 1798.83 (Shine the Light) contains different disclosure requirements, definitions and specifications for website privacy policies, link placement and exceptions, which are now subsumed by the broader regime established by the CCPA.
- Cal. Bus. & Prof. Code §§ 22575–22579, the California Online Privacy Protection Act (CalOPPA), prescribes different disclosure requirements, definitions and rules for online privacy policies, which are subsumed by the CCPA (applicable offline and online).
- Cal. Bus. & Prof. Code § 22584 and § 22584.5, the Student Online Personal Information Protection Act (SOPIPA) and the Early Learning Personal Information Protection Act (ELPIPA) protect the privacy of minors through disclosure and consent requirements, which are now subsumed by the CCPA's requirements for parental consent and opt-in consent from minors up to age sixteen.
- Cal. Civ. Code § 1749.60, *et seq.*, the Supermarket Club Card Disclosure Act of 1999, imposes restrictions on the sale of personal information collected by supermarkets in the context of loyalty cards. Such restrictions are subsumed by the broader CCPA.
- The definitions, scope, requirements and liability provisions in Cal. Civ. Code §1798.82 (the existing breach notification law), Cal. Civ. Code §1798.90.5 (existing rules for automated license plate scan data bases) and Cal. Civ. Code §1798.150 (CCPA liability provision) should be harmonized and streamlined to help businesses understand and comply with these related obligations.

For privacy advocates and lawmakers, it is more exciting to create new privacy laws than to revise the existing statutes. For businesses and other organizations, however, it is increasingly difficult or impractical to keep track of California's numerous privacy laws (in addition to laws of other states and countries). For better or worse, the CCPA is extremely broad and prescriptive. Companies that establish compliance with the CCPA over the next year should not also be required to analyze and apply additional California privacy laws with overlapping, inconsistent or outdated requirements pertaining to the collection and sharing of personal information. The best way to ensure that organizations follow California's new privacy laws is to make compliance with those laws as simple as possible. Investing in a measure of code clean-up would materially assist them in that new compliance challenge.

Please let me know if you have any questions or if I can be of any assistance. I am submitting this letter on my own behalf, not on behalf of my law schools, law firm, clients or others.

Best regards,



Lothar Determann

Attachments, separately submitted:

- biographical information
- publications

LOTHAR DETERMANN BIOGRAPHY

Prof. Dr. Lothar Determann teaches and practices international data privacy, technology, commercial and intellectual property law.

He has been a member of the Association of German Public Law Professors since 1999 and teaches Data Privacy Law, Computer Law and Internet Law at Freie Universität Berlin (since 1994), University of California, Berkeley School of Law (since 2004), Hastings College of the Law (since 2010), Stanford Law School (2011) and University of San Francisco School of Law (2000-2005). He has introduced and first taught courses on privacy law at three law schools in California, including a course specifically dedicated to California Privacy Law at Hastings College of the Law.

He has authored more than 120 articles and treatise contributions as well as 5 books, including Determann's Field Guide to Data Privacy Law (3^d Edition, 2017, also available in Chinese, German, Japanese and Russian) and California Privacy Law - Practical Guide and Commentary (3^d Ed. 2018), which covers every California and U.S. Federal data privacy law.

At Baker & McKenzie LLP in San Francisco and Palo Alto, he has been counseling companies since 1998 on data privacy law compliance and taking products, business models, intellectual property and contracts international. Admitted to practice in California and Germany, he has been recognized as one of the top 10 Copyright Attorneys and Top 25 Intellectual Property Attorneys in California by the San Francisco & Los Angeles Daily Journal and as a leading lawyer by Chambers, Legal 500, IAM and others. For more information see www.bakermckenzie.com.

Message

From: Determann, Lothar [REDACTED]
Sent: 3/9/2019 10:52:07 AM
To: Lisa Kim [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Lisa Kimf4f]; Stacey Schesser [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Stacey Schesser131]
Subject: RE: CCPA regs
Attachments: CCPA regs proposal re. trade secrets, IP.pdf

Yes, Lisa, can you access the attachment?

Copying it also into the email body, I recommend that the Attorney General includes in regulations to further the purposes of Cal. Civ. Code §1798.185(a)(3) a provision according to which

No business shall be obligated under the California Consumer Privacy Act to disclose, destroy or forego a trade secret, as defined and protected under 18 U.S. Code §1839[3] or Cal. Civ. Code §3426.1[d]); copy, distribute or destroy a work of authorship protected under 17 U.S.C. §102(a), or otherwise forego or compromise intellectual property rights under applicable law, including U.S. Federal or California law.

Such a provision is necessary, because the rights under Cal. Civ. Code §1798.100(d) and other sections of the California Consumer Privacy Act are not sufficiently limited and Cal. Civ. Code §1798.185(a)(3) calls upon the California Attorney General to establish exceptions relating to trade secrets and intellectual property rights. While deletion rights are subject to a number of exceptions under Cal. Civ. Code §1798.105(d), these do not yet sufficiently take property rights under Federal and State laws into account. Access rights under Cal. Civ. Code §1798.100(d) are not expressly limited at all. Without limitations in regulations, this would have very harmful consequences, which are not justifiable by potential benefits for privacy, for example, if individuals demand from employers, schools, Universities, concert halls, newspapers, grocery stores and any other business copies or deletion of any personal information (excessively broadly defined to include any information relating to a California resident) in any emails, security camera footage, audio recordings or information in structured or unstructured data pertaining to them, which may be contained in confidential whistleblower reports, company-internal investigation memos, technical research and development notes, paintings, photos, unpublished journalistic articles, concert performances, data bases with information for training of artificial intelligence or self-driving cars, recorded university lectures, exam evaluations, team work in school, panel discussions at conference, and numerous other instances. Without meaningful limitations, unfettered information access and deletion rights will mean the end of confidential communications and have grave chilling effects on free speech, art, journalism, education, intellectual property and other valued features of our society and economy.

I submit this proposal on my own behalf, not on behalf of my law schools, law firm, clients or others.
Lothar Determann

This message may contain confidential and privileged information. If it has been sent to you in error, please reply to advise the sender of the error and then immediately delete this message. Please visit https://urldefense.proofpoint.com/v2/url?u=http-3A__www.bakermckenzie.com_disclaimers&d=DwIFAw&c=uASjV29gZuJt5_5J5CPRUQ&r=6KsThfIRVOY8401451xSKyd3fNlVHCA7PtD2SlHcFuE&m=14uUpr2m_a1i4EB5fXQ8iHZ0U66Wqur-Zu5_BuTfqTg&s=M-Y5Ipn3JH-u9EXowqFSiX1Q81lw6CJ7wl1tNGm8Pwc&e for other important information concerning this message.

-----Original Message-----

From: Lisa Kim [REDACTED]
Sent: Tuesday, March 05, 2019 9:13 AM
To: Determann, Lothar; Stacey Schesser
Subject: [EXTERNAL] RE: CCPA regs

Thanks Lothar. Did you mean to attach something or just that you will prepare something? Thanks.

Lisa

From: Determann, Lothar [REDACTED]
Sent: Monday, March 4, 2019 7:20 PM
To: Stacey Schesser; Lisa Kim
Subject: CCPA regs

Hi Stacey and Lisa,

Good seeing you today. Given your interest, I prepare a submission regarding exceptions to data access rights based on Cal. Civ. Code §1798.185(a)(3).

Please let me know if you have any questions.

Best regards,
Lothar

This message may contain confidential and privileged information. If it has been sent to you in error, please reply to advise the sender of the error and then immediately delete this message. Please visit <[CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient\(s\). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.](https://urldefense.proofpoint.com/v2/url?u=http-3A__www.bakermckenzie.com_disclaimers&d=DwMFAw&c=uASjV29gZuJt5_5J5CPRuQ&r=6KsThfIRVOY8401451xSKyd3fNlVHCA7PtD2S1HcFuE&m=jUjFzhts5_juA-JZkaV4GUeNKIibAFtxYm4LFHHQzwo&s=18fQPewZs9prchM48prl4gdzHAPppux2ozmM8RL7Rq4&e=>https://urldefense.proofpoint.com/v2/url?u=http-3A__www.bakermckenzie.com_disclaimers&d=DwMFAw&c=uASjV29gZuJt5_5J5CPRuQ&r=6KsThfIRVOY8401451xSKyd3fNlVHCA7PtD2S1HcFuE&m=14uUpr2m_a1i4EB5fXQ8iHZ0U66Wqur-Zu5_BuTfqTg&s=M-Y5Ipn3JH-u9EXowqFSiX1Q81lw6CJ7w1ltNGm8Pwc&e=<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.bakermckenzie.com_disclaimers&d=DwMFAw&c=uASjV29gZuJt5_5J5CPRuQ&r=6KsThfIRVOY8401451xSKyd3fNlVHCA7PtD2S1HcFuE&m=jUjFzhts5_juA-JZkaV4GUeNKIibAFtxYm4LFHHQzwo&s=18fQPewZs9prchM48prl4gdzHAPppux2ozmM8RL7Rq4&e=> for other important information concerning this message.</p></div><div data-bbox=)

I recommend that the Attorney General includes in regulations to further the purposes of Cal. Civ. Code §1798.185(a)(3) a provision according to which

No business shall be obligated under the California Consumer Privacy Act to disclose, destroy or forego a trade secret, as defined and protected under 18 U.S. Code §1839[3] or Cal. Civ. Code § 3426.1[d]); copy, distribute or destroy a work of authorship protected under 17 U.S.C. §102(a), or otherwise forego or compromise intellectual property rights under applicable law, including U.S. Federal or California law.

Such a provision is necessary, because the rights under Cal. Civ. Code §1798.100(d) and other Sections of the California Consumer Privacy Act are not sufficiently limited and Cal. Civ. Code §1798.185(a)(3) calls upon the California Attorney General to establish exceptions relating to trade secrets and intellectual property rights. While deletion rights are subject to a number of exceptions under Cal. Civ. Code §1798.105(d), these do not yet sufficiently take property rights under Federal and State laws into account. Access rights under Cal. Civ. Code §1798.100(d) are not expressly limited at all. Without limitations in regulations, this would have very harmful consequences, which are not justifiable by potential benefits for privacy, for example, if individuals demand from employers, schools, Universities, concert halls, newspapers, grocery stores and any other business copies or deletion of any personal information (excessively broadly defined to include any information relating to a California resident) in any emails, security camera footage, audio recordings or information in structured or unstructured data pertaining to them, which may be contained in confidential whistleblower reports, company-internal investigation memos, technical research and development notes, paintings, photos, unpublished journalistic articles, concert performances, data bases with information for training of artificial intelligence or self-driving cars, recorded university lectures, exam evaluations, team work in school, panel discussions at conference, and numerous other instances. Without meaningful limitations, unfettered information access and deletion rights will mean the end of confidential communications and have grave chilling effects on free speech, art, journalism, education, intellectual property and other valued features of our society and economy.

I submit this proposal on my own behalf, not on behalf of my law schools, law firm, clients or others.

Lothar Determann

Message

From: Crenshaw, Jordan [REDACTED]
Sent: 3/8/2019 11:49:15 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: US Chamber Privacy Comments
Attachments: CA AG Privacy Comments .pdf; ATT00001.htm

To Whom It May Concern,

Please find attached the U.S. Chamber of Commerce's comments in the current privacy rulemaking.

Thank you.

Best,

Jordan Crenshaw
Assistant Policy Counsel
C_TEC
[REDACTED]

**CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA**

TIM DAY
SENIOR VICE PRESIDENT
CHAMBER TECHNOLOGY
ENGAGEMENT CENTER (C_TEC)

HAROLD KIM
CHIEF OPERATING OFFICER
U.S. CHAMBER INSTITUTE
FOR LEGAL REFORM

March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA90013

Re: California Consumer Privacy Act Rulemaking

Dear Attorney General Xavier Becerra:

The U.S. Chamber of Commerce (“Chamber”) and the U.S. Chamber Institute for Legal Reform (“ILR”) respectfully submit these comments in response to the public forums hosted by the Attorney General. The Chamber recognizes the importance of consumer privacy, and for this reason, it recently released model privacy legislation¹ which includes a nationwide privacy framework that protects privacy based upon risk to consumers, encourages transparency, and promotes innovation through collaboration between government and private stakeholders. As you continue to adopt regulations and the Legislature pursues further action in response to the California Consumer Privacy Act (“CCPA” or “Act”), the Chamber urges you to consider the principles espoused by the model legislation in order to develop greater certainty for both consumers and business.

I. CONSUMERS BENEFIT FROM THE DATA-DRIVEN ECONOMY

The data-driven economy continues to have a tremendously positive impact for consumers and the national economy, and in particular for California. The information sector contributed over \$271 million in 2017 to California’s GDP² and accounted for nearly 543,000 jobs³ in the state in 2018. While the industry sector numbers alone are impressive, the Chamber recognizes the fact that

¹ See U.S. Chamber of Commerce Model Privacy Bill (February 13, 2019) available at https://www.uschamber.com/sites/default/files/uscc_dataprivacymodellegislation.pdf (hereinafter “Model Bill”).

² See “GDP and Personal Income,” U.S. DEPARTMENT OF COMMERCE, BUREAU OF ECONOMIC ANALYSIS (2017) available at https://apps.bea.gov/iTable/iTable.cfm?reqid=70&step=30&isuri=1&major_area=0&area=06000&year=2017&tableid=505&category=1505&area_type=0&year_end=-1&classification=naics&state=0&statistic=-1&yearbegin=-1&unit_of_measure=levels.

³ See “Economy at a Glance—California,” U.S. DEPARTMENT OF LABOR, BUREAU OF LABOR STATISTICS (Dec. 2018) available at https://www.bls.gov/eag/eag.ca.htm#eag_ca.f.4.

data-driven innovation is changing and benefiting consumers that receive products and services from every sector.

The value of the digital economy has a significant effect on the national economy and the welfare of individual Americans. For example, according to one study, digital advertising was projected to overtake other forms of ads this year, topping over \$100 billion in value.⁴ Data-driven services are beneficial to consumers. For example, the vast majority of Americans prefer targeted advertising.⁵ Revenues obtained by providers from advertisers help reduce prices consumers must pay for products and services.⁶

In addition to direct commercial benefits for consumers, the private sector's use of data is improving society. California localities are partnering with private companies to install gunshot detection technology in order to save lives and enhance public safety.⁷ Data obtained through social media can also be used to prevent and contain disease outbreaks.⁸

The Federal Trade Commission, across administrations, has explained that the appropriate use of consumer data not only results in more efficient markets, it has the potential to "create opportunities for low-income and underserved communities."⁹ Financial services companies are now using data to widen the pool of applicants that have access to credit.¹⁰

Data is changing mobility as well. In the future, autonomous vehicles, which have the potential to reduce the 40,000 road fatalities each year (of which 94 percent are caused by human error),¹¹ will potentially use and transmit up to 4 terabytes of data per day.¹² This technology will be of particular benefit to the elderly, the blind, and the economically disadvantaged as it will increase their mobility whether for purposes of gaining employment or visiting loved ones.

⁴ Sean Fleming, "Digital now accounts for half of all US advertising," World Economic Forum (Oct. 18, 2018) available at <https://www.weforum.org/agenda/2018/10/digital-now-accounts-for-half-of-all-us-advertising/>.

⁵ See IAB, "The Value of Targeted Advertising to Consumers," (citing 2016 survey stating 71 percent of consumers prefer targeted advertising) available at <https://www.iab.com/wp-content/uploads/2016/05/Value-of-Targeted-Ads-to-Consumers2.pdf>.

⁶ Laurence Green, "Does advertising increase consumer prices?" Advertising Association, available at <https://www.adassoc.org.uk/advertisings-big-questions/does-advertising-increase-consumer-prices/>.

⁷ Ryan Johnston, "Gunshot detection expands reach in California city to cover campuses," *State Scoop* (Feb. 23, 2018) available at <https://statescoop.com/fresno-police-department-extend-contract-with-gunshot-detection-system-company/>.

⁸ Dr. Utz Lederbogen, "Predicting flu epidemics with Twitter data-Cooperation between Onsaubrick University and IBM," Informationsdienst Wissenschaft (Mar. 8, 2019) available at <https://idw-online.de/de/news657258>.

⁹ Federal Trade Commission, *Big Data: A Tool for Inclusion or Exclusion?* 5-6 (Jan. 2016), available at <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>.

¹⁰ Ann Carnns, "New type of credit score aims to widen pool of borrowers," *The Seattle Times* (Nov. 3, 2018) available at <https://www.seattletimes.com/business/new-type-of-credit-score-aims-to-widen-pool-of-borrowers/>.

¹¹ See Chamber Technology Engagement Center Comments to Department of Transportation at 1-2, *In the Matter of Automated Vehicle Policy Summit* (Mar. 9, 2018) available at https://www.uschamber.com/sites/default/files/c_tec_av_3.0_comments_1.pdf.

¹² Kathy Winter, "Meaning Behind One Big Number: 4 Terabytes," Intel Newsroom (Apr. 14, 2017) available at <https://newsroom.intel.com/editorials/self-driving-cars-big-meaning-behind-one-number-4-terabytes/>.

The information-driven economy will also require massive investment in communications infrastructure. The 5G networks that will transfer the mass amounts of data necessary to power smart cities and the Internet of Things could produce over 3 million new jobs and \$500 billion in increased GDP over the next decade.¹³

Data and laws regulating privacy affect *every* industry and it is important that policymakers recognize regulations should be flexible to address this reality. The retail, financial services, insurance, transportation, communications, entertainment, health, energy, and manufacturing sectors all rely on data and are impacted by its regulation. California is home to nearly one tenth of the nation's *Fortune 500* companies¹⁴, representing a wide variety of industries, which all use data in order to improve the products and services they offer to their customers. Any regulation imposed upon data collected, used, or shared by California businesses or about California residents has far-reaching national implications, and it is for this reason that the U.S. Chamber of Commerce offers its comments to improve how the CCPA operates.

II. THE ATTORNEY GENERAL'S RULEMAKING SHOULD DRAW UPON THE CHAMBER'S CONSENSUS PRINCIPLES.

a. The Chamber's Proposal

The U.S. Chamber of Commerce convened over 200 member companies and trade associations to release model privacy legislation based upon its privacy principles¹⁵ and elements of CCPA. Although the Chamber supports a federal privacy law, the business community believes that its privacy principles should be instructive to the current rulemaking.

Given the effect of data on interstate commerce and US economic prosperity, today's current technological and state regulatory environment necessitates a federal privacy law that preempts state and local privacy laws. A national privacy framework also will bolster continued U.S. leadership in trade internationally and facilitate interoperable cross-border data transfer frameworks. Policies that promote the free flow of data across state and national borders will facilitate numerous consumer benefits, economic growth, and trade.

While the best approach is one national privacy framework, the Chamber offers its suggestions for ways to improve and enhance California's already-enacted privacy law. The Chamber believes that privacy protections should be risk-focused. Privacy protections should be considered in light of the benefits provided to consumers and the economy and the privacy risks presented by the data being used, and the way a business uses it. Enforcement should focus on cases in which consumers suffer actual harm, as opposed to mere speculative injuries or technical

¹³ See Accenture Strategies, "Smart Cities: How 5G Can Help Municipalities Become Vibrant Smart Cities," at 1 (2017) available at https://www.accenture.com/20170222T202102_w_us-en_acnmedia/PDF-43/Accenture-5G-Municipalities-Become-Smart-Cities.pdf.

¹⁴ "Number of U.S. companies listed in the Fortune 500 in 2018," Statista (2019) available at <https://www.statista.com/statistics/303696/us-fortune-500-companies-by-state/>.

¹⁵ U.S. Chamber of Commerce Privacy Principles (Sept. 6, 2018) available at https://www.uschamber.com/sites/default/files/9.6.18_us_chamber_-_ctec_privacy_principles.pdf.

violations of the law. The Chamber's privacy legislation discussion draft draws upon these principles.

At the same time, the Chamber agrees with the fundamental privacy protections offered by CCPA and believes that consumers should have a say as to how personally identifiable information about them is shared. That is why the Chamber's model legislation offers consumers the ability to opt out of data sharing with third parties. At the same time, companies using and sharing consumer data should be able to continue innovating and not be hindered by consumer consent outcomes and regulations that do not take into consideration the risks and benefits of data.

Consumers, upon verified request, should be given the qualified ability to request that information about them be deleted. Any proposed right of deletion, like the CCPA, must allow for reasonable exceptions to such requests. Data deletion rights though should not impede a company's ability to, among other things, provide the goods or services for which a consumer and business contract, maintain good data hygiene, conduct security-protected research, combat fraud and security threats, and comply with legal obligations.

b. The Definition of "Personal Information"

The definition of "personal information" is the capstone of any privacy framework. The Chamber urges the Attorney General to take great care in interpreting this important definition. The Act generally defines "personal information" as:¹⁶

[I]nformation that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked directly or indirectly, with a particular consumer or household...

Specifically, the Chamber supports a definition of "personal information" that is not overly expansive and could capture data that is not truly personal. The Chamber recommends that personal information should be defined as "information that identifies a consumer."¹⁷ Privacy regulators should avoid overly-expansive definitions of "personal information" and not focus on data that could hypothetically be connected to an individual. Similarly, the Chamber cautions against an expansive view of the definition of "household" which could create confusion for both consumers and businesses.

The Chamber also recognizes that certain practices that work to eliminate connecting data to and preventing harm to individuals should not be considered "personal information." For example, the Chamber generally suggests that aggregated, de-identified and pseudonymous data should not

¹⁶ SB 1121 § 9(o)(1) (2018).

¹⁷ See Model Bill at § 1(7).

be considered “personal information.” The CCPA and the Chamber both support similar definitions of “pseudonymization”:¹⁸

[I]nformation process in such a manner that it can no longer be attributed to a specific consumer without the use of additional information, provided that such additional information is kept separately and is subject to technical and organization measures to ensure that the personal information do not identify, or cannot reasonably identify, a natural person.

California should interpret “personal information” to exclude pseudonymized information. As a matter of public policy, the Attorney General should encourage companies to protect information through innovative means. In fact, the General Data Protection Regulation in Europe promotes the use of pseudonymization as means to protect individual privacy.¹⁹

The CCPA also carves out “publicly available information” from the definition of “personal information.”²⁰ The Chamber urges the Attorney General to interpret the term “publicly available information” in a manner that protects the First Amendment rights of those who process and share personal information.

c. Definition of Consumer

Finally, the Chamber advocates for exempting information pertaining to employees from obligations under the CCPA. Specifically, business records about an employee’s job duties cannot be subject to regulations that allow an individual to request to review or delete identifying data about them. Interpretation of the Act should not include obligations for employees or contractors of a business acting in their role as employee or contractor.

d. Protection of Loyalty Programs

The Chamber requests that the Attorney General also consider the impact that CCPA will have on consumer loyalty programs. These loyalty programs offered by retailers, banks, airlines, restaurants, and entertainment companies greatly benefit consumers. According to one study, the overwhelming majority of consumers agree that loyalty programs save them money.²¹

California’s Act has fomented uncertainty in the business community about its impact on loyalty programs. Section 6 of the CCPA amends California law to prohibit businesses from discriminating against a consumer because a consumer exercised any of the consumer’s privacy

¹⁸ See Model Bill § 1(8); See also SB 1121 § 9(r).

¹⁹ See Recital 28 General Data Protection Regulation (“The application of pseudonymization to personal data can reduce the risks to data subjects concerned and help controllers and processors to meet their data-protection regulations.”).

²⁰ See SB 1121 at § 9(0)(2).

²¹ Emily Collins, “How Consumers Really Feel About Loyalty Programs,” FORRESTER (May 8, 2017) available at <http://www.oracle.com/us/solutions/consumers-loyalty-programs-3738548.pdf>.

rights under the Act²² According to the Act, discrimination could be done in the form of denying goods or services, “charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposes penalties,” or differing levels of quality.²³ The Chamber strongly urges the Attorney General to interpret that the loyalty programs that consumers overwhelmingly enjoy and benefit from are not negatively impacted by Section 6 of the CCPA and are not considered to discriminate against a consumer for exercising privacy rights. We urge the Attorney General and the Legislature to protect these consumer-friendly programs.

III. DATE OF ENFORCEMENT

Currently, the CCPA states that “the Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.”²⁴ The Chamber additionally requests that the Attorney General clarify that, when enforcement starts, any enforcement that occurs will only be based on business conduct or alleged business non-compliance that takes place on or after the enforcement date. Enforcement should not be based on conduct that occurs between the effective date—January 1, 2020—and the enforcement date of the Act.

IV. CALIFORNIA’S APPROACH TO ENFORCEMENT MAY BE INCONSISTENT WITH BEST PRACTICES AND IS UNLIKELY TO IMPROVE DATA PRIVACY.

There are laudable parts of the CCPA and California is influencing national discussions about privacy. But there are some areas of significant concern, especially from an enforcement perspective. Enforcement mechanisms are a key component of any legal regime. The CCPA contemplates enforcement by the Attorney General. It also contemplates enforcement through a private right of action for the “unauthorized access and exfiltration, theft, or disclosure” of “nonencrypted or unredacted personal information” “as a result of [a] business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.”²⁵ The private right of action authorizes uncapped statutory damages “in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.”²⁶

There are well-documented problems with this sort of approach. *First*, enforcement provisions of data privacy laws should only apply where there is demonstrable, concrete harm to individuals proximately caused by a violation of the statute.²⁷ When it enacted the CCPA, the Legislature expressed its intent to prevent “devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm” that

²² See SB 1121 at § 6.

²³ *Id.*

²⁴ See § 1798.185(c).

²⁵ § 1798.150(a)(1).

²⁶ § 1798.150(a)(1)(A).

²⁷ See *Privacy Principles*, at 2; cf. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1550 (2016) (dismissing suit for lack of standing where plaintiff alleged a “procedural violation” of the Fair Credit Reporting Act but no “concrete harm”).

might result from a data breach.²⁸ These are worthy goals, but the text of CCPA’s private right of action does not clearly require a showing of harm, setting the stage for the type of enforcement drift and litigation abuse we have seen under certain federal statutes.²⁹

Second, experience shows that private rights of action coupled with uncapped statutory damages invite abusive litigation seeking jackpot paydays for plaintiffs’ attorneys rather than improved outcomes for consumers. That problem is magnified where, as here, there is no clear statutory requirement for a potential plaintiff to show concrete harm, and lawyers are incentivized by statutory damages to cobble together class actions seeking enormous payouts for *de minimus* procedural or technical violations of the statute.

The federal Telephone Consumer Protection Act (“TCPA”) provides a cautionary example. Although that statute was designed to target unscrupulous scam telemarketers, trial lawyers often uses it to bring cases against legitimate American businesses, big and small, that are often simply attempting to reach out to their own customers using numbers provided by those customers.³⁰ For example, in a recent case examining a rule promulgated under the TCPA, the D.C. Circuit expressed shock that a pharmaceutical company might be held liable in state court for \$150 million in damages for a seemingly benign error like “failing to include opt-out notices on faxes that the recipients had given [the company] permission to send.”³¹ Unfortunately, such astronomical figures are common in the TCPA context and the plaintiffs’ bar frequently assembles classes based on similarly innocent mistakes. Some have even built a cottage industry of victims that let calls—and damages accrue—to secure larger payouts. ILR believes companies should be held responsible when negligent mistakes result in harm. But permitting suits for uncapped statutory damages where there is no showing of harm is a recipe for abusive litigation that stifles economic growth and innovation.

Because the Legislature is considering amendments to the CCPA, California has an opportunity to correct problems with the CCPA before the law goes into effect. Unfortunately, press reports indicate that that you are seeking legislative amendments that would make the statute *worse*, not better, by deleting a provision which gives companies an opportunity to cure data breaches within 30 days, and by creating new liability for violations that are unrelated to the disclosure of personal information.³² Your proposal reportedly also would eliminate the ability of companies to seek guidance from the Attorney General on how to comply with certain vague

²⁸ AB 375 § 2 (2018).

²⁹ See, e.g., ILR, *The Juggernaut of TCPA Litigation: The Problems with Uncapped Statutory Damages* 1 (2013) (“Juggernaut”) (“It is rare these days to see TCPA litigation brought against its original intended target—abusive telemarketers.”), available at https://www.instituteforlegalreform.com/uploads/sites/1/TheJuggernautofTCPALit_WEB.PDF.

³⁰ See ILR, *TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Lawsuits* 2 (2017), available at https://www.instituteforlegalreform.com/uploads/sites/1/TCPA_Paper_Final.pdf.

³¹ See *Bais Yaakov of Spring Valley v. FCC*, 852 F.3d 1078, 1081 (D.C. Cir. 2017) (“Let that soak in for a minute: Anda was potentially on the hook for \$150 million for failing to include opt-out notices on faxes that the recipients had given Anda permission to send.”), cert. denied, 138 S. Ct. 1043 (2018).

³² See, e.g., Alexei Koseff, *California attorney general looks to expand new data privacy law*, San Francisco Chronicle (Feb. 25, 2019), <https://www.sfchronicle.com/politics/article/California-attorney-general-looks-to-expand-new-13644242.php>.

provisions in the CCPA, raising significant due process concerns.³³ Such moves would reduce incentives to engage in reasonable privacy risk management, which is a key part of standards like those promulgated by the National Institute of Standards and Technology (NIST) in the United States Department of Commerce.³⁴

ILR has also seen mention of proposals to authorize localities to bring lawsuits under the CCPA. Authorizing municipal lawsuits would be a mistake. It would threaten the administration of justice by diverting awards away from consumers and into municipal coffers. Worse, by incentivizing localities to bring speculative claims in the hope of large payouts, it would dilute the judicial resources allocated to potentially meritorious claims. Fundamentally, authorizing municipalities to bring lawsuits to enforce state law upsets the traditional balance of power between local and state government and threatens California's role in setting state policy.³⁵

Attorneys are already gearing up to bring a wave of injury-free lawsuits over privacy and technology issues.³⁶ The *in terrorem* effect of vague obligations and multimillion-dollar judgments will not improve consumer welfare. Such proposals will undermine a successful data privacy policy and divert resources from risk-based compliance efforts into litigation that enriches lawyers but does not protect consumers.

Our shared goal should be, as the Chamber and ILR have explained, a regulatory regime that facilitates transparency and predictability for consumers and encourages collaboration and constant improvement.³⁷ Thus, enforcement should be focused on harm to consumers, with discretion vested in the government, not private actors or local governments. It should be predictable and reward prudent risk management. And, it should ensure that damages are commensurate with harm.³⁸ Additionally, the Attorney General should remain available as a resource to private organizations that want guidance. California should revise the CCPA to reflect these principles.

³³ See *id.*; cf. *Christopher v. SmithKline Beecham Corp.*, 567 U.S. 142, 158–59 (2012) (“It is one thing to expect regulated parties to conform their conduct to an agency’s interpretations once the agency announces them; it is quite another to require regulated parties to divine the agency’s interpretations in advance or else be held liable when the agency announces its interpretations for the first time in an enforcement proceeding[.]”).

³⁴ In its recent revision to Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, at 8, available at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf> NIST observed that “[w]ithout adequate risk management preparation at the organizational level, security and privacy activities can become too costly, demand too many skilled security and privacy professionals, and produce ineffective solutions.” Efforts across government support privacy risk management, such as the Privacy Framework that NIST intends to be a tool for use across the economy. See, e.g., *Live Webinar: Outlining the NIST Privacy Framework*, <https://www.nist.gov/news-events/events/2019/03/live-webinar-outlining-nist-privacy-framework>

³⁵ Cf. *California Redevelopment Assn. v. Matosantos*, 267 P.3d 580, 597 (Cal. 2011) (“In our federal system the states are sovereign but cities and counties are not; in California as elsewhere they are mere creatures of the state and exist only at the state’s sufferance.” (citation omitted)).

³⁶ See Brief of Amici CTIA–The Wireless Association[®] et al. at 11, *FCA US LLC v. Flynn*, No. 18-8010 (U.S.), available at <https://www.wileyrein.com/assets/htmldocuments/SCOTUS%20Motion%20and%20Amicus%20Brief%20-%20Hacking%20Suit%2010.30.2018%20003.pdf> (describing reports of plaintiffs firms “salivating” over the prospect of privacy and security litigation)

³⁷ See *Privacy Principles*, at 2.

³⁸ See *id.*; see also *Juggernaut*, at 12 (explaining the success of regimes with reasonable damages caps).

V. THE RULEMAKING SHOULD PROVIDE REGULATORY SAFE HARBORS THAT OFFER PREDICTABILITY, ENCOURAGE BEST PRACTICES, AND LIMIT LIABILITY UNDER ANY PRIVATE RIGHT OF ACTION.

The CCPA's private right of action creates potential liability for a business's "violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information" where that violation results in the disclosure of "nonencrypted or nonredacted personal information."³⁹ To secure passage of the CCPA, privacy advocates assured lawmakers that this language was designed to create statutory "safe harbors" that would protect businesses operating in good faith and taking reasonable precautions to protect their customers' data from disclosure.⁴⁰

Safe harbors are routine in California and elsewhere to encourage good behavior and provide predictability. Examples abound.⁴¹ Safe harbors will be particularly useful in addressing privacy and data security practices, which often are built into product and service offerings with longer lifecycles, and also may need to evolve over time to meet shifting threats and challenges. Safe harbors have been effectively used in the context of global data transfers,⁴² Internet platform operations,⁴³ the regulation of marketing to children,⁴⁴ compliance with anti-kickback laws,⁴⁵ and numerous other settings. Safe harbors can take the form of immunities from suit, or they can be affirmative defenses, as in the case of Ohio's new cybersecurity regime, which protects organizations from liability if they have taken certain actions.⁴⁶

³⁹ § 1798.150(a)(1).

⁴⁰ See *Understanding the Rights, Protections, and Obligations Established by the California Consumer Privacy Act of 2018: Where should California go from here?: Informational Hearing Before the Comm. On Privacy and Consumer Protection*, 2019 Leg. Sess. (Cal. 2019) (statement of Alastair Mactaggart, Chairman, Californians for Consumer Privacy, explaining purpose of safe harbor provisions), available at <https://www.assembly.ca.gov/media/assembly-committee-privacy-consumer-protection-20190220/video>.

⁴¹ See *Lopez v. Nissan N. Am., Inc.*, 201 Cal. App. 4th 572, 592 (2011) (recognizing that state law in "provides a safe harbor against UCL claims complaining about the accuracy of odometers"); *Bourgi v. W. Covina Motors, Inc.*, 166 Cal. App. 4th 1649, 1661 (2008) (noting that "[t]he California Legislature has provided as a matter of policy that new vehicle dealers are afforded a safe harbor by complying with the damage disclosure law"). Likewise, Proposition 65 has safe harbors, see, e.g., *Env'tl. Law Found. v. Wykle Research, Inc.*, 134 Cal. App. 4th 60, 66, (2005). "When specific legislation provides a 'safe harbor,' plaintiffs may not use the general unfair competition law to assault that harbor." *Cel-Tech Comm'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 182 (1999).

⁴² See, e.g., Federal Trade Commission, *U.S.-EU Safe Harbor Framework* (Sept. 4, 2015), <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework>.

⁴³ See, e.g., *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1036 (9th Cir. 2013) (applying "safe harbor" protection under the Digital Millennium Copyright Act)

⁴⁴ See Federal Trade Commission, *Children's Online Privacy Protection Act Safe Harbor Program* (last visited Mar. 8, 2019), <https://www.ftc.gov/safe-harbor-program>.

⁴⁵ Federal "'safe harbor' regulations describe various payment and business practices that, although they potentially implicate the Federal anti-kickback statute, are not treated as offenses under the statute." <https://oig.hhs.gov/compliance/safe-harbor-regulations/index.asp>

⁴⁶ Ohio S.B. 220, Data Protection Act, providing a "safe harbor" for companies that implement a program that complies with the Framework for Improving Critical Infrastructure Cybersecurity developed by NIST. Business can choose from frameworks, including NIST SP 800-171, NIST SP 800-53 and 800-53(a), the Federal Risk and Authorization Management Program (FedRAMP), Center for Internet Security (CIS) Critical Security Controls, the ISO 27000 Family, the HIPAA Security Rule, Graham-Leach-Bliley Act, or the Federal Information Security Modernization Act (FISMA).

The Attorney General should make good on the Legislature's intent by seeking comment on the scope of the CCPA's safe harbors and clarifying that they are intended to protect businesses.⁴⁷ *First*, the rules promulgated by the Attorney General should address the promised safe harbor for businesses that "implement and maintain reasonable security procedures and practices appropriate to the nature of the information."⁴⁸ The rules should clarify that this standard is met when a business adopts information or data security practices that are recommended by an appropriate body such as an industry specific regulator or trade association,⁴⁹ or when businesses can otherwise show that they have made good faith efforts to adopt compliance programs appropriate for the risks associate with the data they maintain.⁵⁰

Second, the rules promulgated by the Attorney General should address the statutory safe harbors for "[e]ncrypted" or "[r]edacted" "personal information."⁵¹ In addition, because the CCPA incorporates an existing statutory definition of "personal information" as (1) an "individual's first name or first initial and his or her last name in combination with" any one of several statutorily identified data elements "when either the name or the data elements are not encrypted or redacted" or (2) a "username or email address in combination with a password or security question and answer that would permit access to an online account,"⁵² the rules should clarify that the safe harbors cover partially encrypted or redacted information where at least one element is redacted or encrypted and the unencrypted or unredacted data is either publicly available or cannot be linked with any specific individual.

Third, the rules promulgated by the Attorney General should clarify that a business that implements "reasonable security procedures and practices" following a data breach will be found to have "cured" the breach within the meaning of the CCPA.⁵³ As currently enacted, the CCPA is designed to afford businesses 30 days to cure a data breach and thereby to avoid "individual statutory damages or class-wide statutory damages"⁵⁴ Affording businesses this reasonable

⁴⁷ See §§ 1798.155(a) ("Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title"), 1798.185(c) ("The Attorney General may adopt additional regulations as necessary to further the purposes of this title.").

⁴⁸ § 1798.150(a)(1).

⁴⁹ For example, the U.S. Department of Health and Human Services has issued voluntary cybersecurity guidelines to reduce cybersecurity and data breach risks for health care organizations of varying sizes. See HHS, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (2019), available at <https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf>. Similarly, the Communications Security, Reliability and Interoperability Council, a federal advisory committee operating under the auspices of the Federal Communications Commission, regularly develops security recommendations for entities in the telecommunications industry. See, e.g., FCC, *Communications Security, Reliability and Interoperability Council VI* (Jan. 3, 2019), <https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-0>. Businesses that demonstrate compliance with such standards are engaging in reasonable security procedures and practices, and the Attorney General's interpretation of the CCPA should reflect that reality.

⁵⁰ See *Privacy Principles*, at 1 (explaining that "data controls should match the risk associated with the data and be appropriate for the business environment in which it is used.").

⁵¹ § 1798.150(a)(1).

⁵² See Cal. Civ. Code § 1798.81.5(d)(1)(A).

⁵³ § 1798.150(a), (b).

⁵⁴ § 1798.150(b).

opportunity to cure deficiencies before private action is initiated will encourage greater transparency and cooperation between businesses, regulators, and consumers.⁵⁵ The rulemaking should therefore strengthen this commonsense cure provision by clarifying the Attorney General's interpretation that adoption of an appropriate security program is sufficient to cure an actionable disclosure. Even with such a clarification, businesses will remain eager to adopt appropriate security programs ex ante; in addition to the negative publicity that often accompanies a data breach, the CCPA makes clear that a plaintiff may still recover "actual damages" independent of any cure.⁵⁶

VI. CONCLUSION

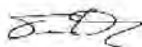
Data is important to every business in the United States whether it be credit reporting companies enabling consumers to be able to access credit in a matter of minutes as opposed to days, marketers presenting tailored products and services to consumers, or automakers and technology firms contributing to the reduction of traffic deaths. Effective, innovative, and responsible use of data is improving the lives of Americans in significant ways. Large amounts of data are being used, analyzed, and shared to bring about these positive societal and economic changes, and companies must respect the privacy of individuals.

While a national privacy standard is preferable, the Chamber recognizes the important work being done in California to protect consumer privacy and asks that the Attorney General interpret CCPA from a risk-based perspective that protects consumers while promoting innovation. California should seek to avoid overly expansive definitions of personal information and protect popular consumer loyalty programs.

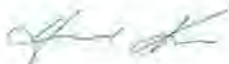
The U.S. Chamber Institute for Legal Reform urges California to amend the CCPA to ensure that its enforcement regime is focused on actual harm to consumers and not on incentivizing potentially destructive litigation that does little to help consumers. Consistent with that goal, ILR urges the Attorney General to consider in the current rulemaking the means outlined above for strengthening the statutory safe harbors enacted by the Legislature.

The Chamber and ILR stand ready to work with the Attorney General to protect consumer privacy and innovation.

Respectfully Submitted,



Tim Day
Senior Vice President
Chamber Technology Engagement Center



Harold Kim
Chief Operating Officer
U.S. Chamber Institute for Legal Reform

⁵⁵ See *Privacy Principles*, at 2.

⁵⁶ § 1798.150(b).

Message

From: Diana Bohn [REDACTED]
Sent: 12/21/2018 6:59:03 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy
Flag: Follow up

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Diana Bohn

[REDACTED]

Message

From: Brad Walker - CA-SIG [REDACTED]
Sent: 3/7/2019 9:05:59 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: 'Clay Jackson' [REDACTED]; 'Greg Famous' [REDACTED]
[REDACTED]
Subject: Workers' Compensation Exemption from CCPA
Attachments: California Exemption Letter.pdf

Please see attached from the California Alliance of Self-Insured Groups (CA-SIG)

Warmest regards,



Brad Walker

Executive Director

CA-SIG
[REDACTED]

The information contained herein is privileged and confidential. It is intended for the use of the addressee only. If you are not the intended recipient, you are hereby advised that any distribution, dissemination, or copying of the contents of this transmittal is strictly prohibited. If you have received this transmittal in error, please immediately notify the sender by telephone and destroy this transmittal.



March 6, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

VIA US MAIL and EMAIL

Dear Sir/Madam:

The following comments are submitted on behalf of the California Alliance of Self-Insured Groups (CA-SIG) and its members. (See: www.ca-sig.org.)

**The Attorney General Should Exempt the Workers' Compensation System
From the California Consumer Privacy Act**

The California Consumer Privacy Act (CCPA) directs the Attorney General to adopt regulations to further the purposes of the CCPA, including "...[e]stablishing any exceptions necessary to comply with state or federal law, ... within one year of passage of this title and as needed thereafter."¹

An Exception From the CCPA is Necessary to Comply With the California Constitution
and State Laws Governing the Workers' Compensation System

1) The workers' compensation system is established and regulated pursuant to the California Constitution.

The California Constitution confers plenary power on the Legislature to enact a comprehensive worker's compensation system. Section 4 of Article XIV of the California Constitution vests the Legislature with "plenary power, unlimited by any provision of this Constitution, to create, and enforce a complete system of workers' compensation, by appropriate legislation."² This constitutional mandate gives the Legislature "complete, absolute and unqualified power to create and enact the workers' compensation system."³

California courts have interpreted this grant of broad power to mean that "absolutely nothing" in Section 4 "purports to limit the Legislature's authority to enact additional appropriate legislation for the protection of employees."⁴

¹ Civil Code §1798.185 (a) (3)

² Cal Const. Article XIV, § 4

³ *Facundo-Guerrero v. Workers' Comp. Appeals Bd.* (2008) 163 Cal.App.4th 640, 650 [intent behind Section 4 "was to endow [the Legislature] expressly with exclusive and 'plenary' authority to determine the contours and content of our state's workers' compensation system"].

⁴ *City and County of San Francisco v. Workers' Comp. Appeals Bd. (Wiebe)* (1978) 22 Cal.3d 103, 114

The constitutional grant of power has “compelled the conclusion” that Section 4 of Article XIV of the California Constitution supersedes the California Constitution’s Due Process clause with respect to legislation passed under the Legislature’s plenary powers over the workers’ compensation system.¹ Courts have held that, even if conflicts existed between Section 4 [workers’ compensation] and other California Constitutional provisions governing Separation of Powers or Due Process, “the plenary powers conferred by Section 4 would still control.”²

The courts have unambiguously held that the provisions of the California Constitution governing workers’ compensation are not limited by other provisions of the California Constitution, including the Due Process and Separation of Powers clauses.

These interpretations lead to a likely conclusion that, by its own terms, the constitutional provisions governing workers’ compensation will also control over state constitutional provisions in Section 1 of Article I pertaining to the right to Privacy, so long as the Legislature has employed its “...plenary power, *unlimited by any provision of this Constitution*, to create, and enforce a complete system of workers’ compensation, by appropriate legislation.”³

1) Pursuant to its constitutional mandate, the Legislature has enacted a comprehensive workers’ compensation system by statute.

Section 4 of Article XIV of the California Constitution provides in part that “[a] complete system of workers’ compensation includes...full provision for vesting power, authority and jurisdiction in an administrative body with all the requisite governmental functions to determine any dispute or matter arising under such legislation.” The intent behind Section 4 “was to endow [the Legislature] expressly with exclusive and ‘plenary’ authority to determine the contours and content of our state’s workers’ compensation system.”⁴ The only limitations on the Legislature’s plenary powers are that the Legislature cannot act outside of its authority to create and to enforce a complete system of workers’ compensation or enact a provision that conflicts with federal law.⁵ The California Constitution, and the cases interpreting it, confirm that “nearly any exercise of the Legislature’s plenary powers over workers’ compensation is permissible so long as the Legislature finds its action to be ‘necessary to the effectiveness of the system of workers’ compensation.’”⁶

Acting under this power, the Legislature enacted the workers’ compensation law to govern compensation to California workers who are injured in the course of their employment.⁷

¹ *Hustedt v. Workers’ Comp. Appeals Bd.* (1981) 30 Cal.3d 329, 343 [“It is well established that adoption of [Section 4] ‘effected a repeal pro tanto’ of any state constitutional provisions which conflicted with that amendment”]; see also *Greener v. Workers’ Comp. Appeals Bd.* (1993) 6 Cal.4th 1028 [article VI of the California Constitution governing courts’ jurisdiction inapplicable to extent Legislature has exercised its powers under Section 4]

² *Stevens v. Workers’ Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

³ (Emphasis added) Cal Const. Article XIV, § 4

⁴ *Facundo-Guerrero v. Workers’ Comp. Appeals Bd.* (2008) 163 Cal.App.4th 640, 650

⁵ *Hustedt v. Workers’ Comp. Appeals Bd.* (1981) 30 Cal.3d 329; see also, *Stevens v. Workers’ Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

⁶ *Stevens v. Workers’ Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

⁷ Division 4 (commencing with Section 3200) of the Labor Code

The underlying premise behind this statutorily created system is the “compensation bargain, [under which] the employer assumes liability for industrial personal injury or death without regard to fault in exchange for limitations on the amount of that liability. The employee is afforded relatively swift and certain payment of benefits to cure or relieve the effects of industrial injury without having to prove fault but, in exchange, gives up the wider range of damages potentially available in tort.”⁸ The workers’ compensation law requires employers to secure the payment of workers’ compensation benefits either by purchasing third-party insurance or by self-insuring with permission from the Department of Industrial Relations.⁹

In addition, where the “conditions of compensation” exist, the right to recover such compensation is the “sole and exclusive remedy” of the employee or his or her dependents against the employer when acting within the scope of his or her employment.¹⁰

2) Existing privacy protections in the workers’ compensation system

There are several privacy requirements within the Labor Code directly applicable to workers’ compensation. Labor Code Section 138.7 provides in part:

“A person or public or private entity not a party to a claim for workers’ compensation benefits shall not obtain individually identifiable information obtained or maintained by the division on that claim. For purposes of this section, ‘individually identifiable information’ means any data concerning an injury or claim that is linked to a uniquely identifiable employee, employer, claims administrator, or any other person or entity.”

There are limited exceptions to that rule, but it is unlawful for any person who has received individually identifiable information from the division pursuant to this section to provide that information to any person who is not entitled to it.¹¹ In a similar way, Labor Code Section 3762 (c) states:

“An insurer, third-party administrator retained by a self-insured employer pursuant to Section 3702.1 to administer the employer’s workers’ compensation claims, and those employees and agents specified by a self-insured employer to administer the employer’s workers’ compensation claims, are prohibited from disclosing or causing to be disclosed to an employer, any medical information, as defined in Section 56.05 of the Civil Code, about an employee who has filed a workers’ compensation claim, except as follows: (1) Medical information limited to the diagnosis of the mental or physical condition for which workers’ compensation is claimed and the treatment provided for this condition. (2) Medical information regarding the injury for which workers’ compensation is claimed that is necessary for the employer to have in order for the employer to modify the employee’s work duties.”

⁸ *Charles J. Vacanti, M.D., Inc. v. State Comp. Ins. Fund* (2001) 24 Cal.4th 800, 811. See also, *Shoemaker v. Myers* (1990) 52 Cal.3d 1

⁹ Labor Code § 3700

¹⁰ Labor Code § 3602 (a)

¹¹ Labor Code § 138.7

Insofar as electronic billing purposes are concerned, Labor Code Section 4603.4 (b) specifies that that billing standards developed by the Division of Workers' Compensation (DWC), "...shall be consistent with existing standards under the federal Health Insurance Portability and Accountability Act of 1996."

Labor Code Section 4610.5 (m) states that when a claims administrator is transmitting medical records pursuant to a request for independent medical review, "The confidentiality of medical records shall be maintained pursuant to applicable state and federal laws." Confidentiality of medical information was also addressed by the Legislature in Labor Code Section 4903.6 (d):

"With the exception of a lien for services provided by a physician as defined in Section 3209.3, a lien claimant shall not be entitled to any medical information, as defined in subdivision (g) of Section 56.05 of the Civil Code, about an injured worker without prior written approval of the appeals board. Any order authorizing disclosure of medical information to a lien claimant other than a physician shall specify the information to be provided to the lien claimant and include a finding that the information is relevant to the proof of the matter for which the information is sought."

In summary, privacy protections within the Labor Code extensively address protection of medical information.

3) Workers' Compensation is a comprehensive statutory medical, legal and adjudicatory system that is incompatible with the provisions of the CCPA.

Each day, personal and medical information concerning hundreds of thousands of injured workers is circulated from a Medical Provider Network (MPN) or insurance claims administrator to the physician, to the physician specialist to whom an injured worker may be referred, to the Utilization Review Organization, an Independent Medical Review (IMR) service, an Independent Bill Review (IBR) organization, and Electronic Billing Review organization, Pharmacy Benefit Managers, Vocational Rehabilitation Counselors, Job Training and Supplemental Job Displacement Benefit entities, and more.

Additionally, MPN administrators and self-insured employers are required to report injured workers' medical information to the Office of Self-Insured Plans, Workers' Compensation Information System, Workers' Compensation Appeals Board and the Workers' Compensation Insurance Rating Bureau, all mandatory reporting requirements that would trigger disclosure notifications under the CCPA.

Because an injured worker cannot, and would clearly not wish to frustrate the adjusting of a claim by not allowing information to be disclosed to those who are integral to the workers' compensation medical treatment and benefit payment system, the disclosures nevertheless must be provided to the workers' compensation claimant or applicant. Failure to do so can result in penalties and enforcement actions from the California Department of Justice and the Department of Industrial Relations.

For example, Civil Code § 1798.115(a) of the CCPA states that the consumer has a right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer (1) the categories of personal information that the business collected about the consumer, (2) the categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold, and (3) the categories of personal information that the business disclosed about the consumer for a business purpose.

Section 1798.115(a) would likely apply to nearly all workers' compensation claims transactions. As noted above, medical records are sent to a medical provider network (MPN), medical records are sent to a utilization review organization (URO), and medical records are sent to an independent review organization (IRO). "Personal information" would clearly include payment information sent to a payment processing center falling within the definition of "service provider." A vocational evaluator would clearly need to know "professional or employment-related information" that is included within the definition of "personal information" in Civil Code Sec. 1798.140(o)(1)(I).

During the routine administration of a workers' compensation claim, especially a claim involving indemnity benefits, considerable "personal information," as defined in Civil Code Sec. 1798.140(o), must be collected so that the claim can be processed and the injured worker can be treated and compensated. For physicians and other service providers, an injured worker's personal information is collected during the payment and remittance process. In addition, the placement of insurance, including providing and disclosure claims information, is a vital function in the workers' compensation system.

By law, workers' compensation claimants are considered "consumers" for purposes of the Insurance Information and Privacy Protection Act.¹² Therefore, the notice of information practices required by Insurance Code Sec. 791.04 applies to workers' compensation insurers.

Although these are just a few examples, the fact remains that each and every referral or transmittal cited above would, pursuant to the CCPA, trigger a disclosure notification to the injured worker. The sheer number of notices that would be generated pursuant to the CCPA has, in the case of one large MPN doing business in the state, been estimated to generate nearly 61 million pieces of paper for each 150,000 claims during routine claims processing operations.

Yet, every one of these transactions are already governed by a comprehensive body of *existing state law*. Moreover, because workers' compensation is the sole and exclusive remedy for all injuries and illnesses that occur within the course and scope of employment, the injured employees would not be allowed to opt out of participation as is provided for within the CCPA.

Therefore, although an injured worker cannot prevent the adjusting of a claim by refusing to allow information to be given to workers' compensation service providers, the notification disclosures nevertheless must be sent if the CCPA were to apply. Failure to do so can result in penalties and enforcement actions from the Department of Justice.

4) A regulatory exception from CCPA is needed in order to comply with the comprehensive constitutionally mandated and legislatively enacted workers' compensation system.

The workers' compensation system is a unique body of state law that is breathtaking in its scope and applicability. The workers' compensation system has its own legal and court adjudication system. Medical treatment offered within the workers' compensation system is completely separate and apart from the state's health care delivery system. Nearly every aspect of an injured worker's medical care, vocational rehabilitation, and benefit payments is governed by state law and subject to extensive oversight by the Division of Workers' Compensation within the state Department of Industrial Relations.

¹² Insurance Code § 791 et seq.

This petition for an exception from CCPA in order to comply with state law, as authorized pursuant to Civil Code Section 1798.185 (a) (3), is presented herein on account of the fact that these extremely complex and comprehensive transactions that take place every day concerning the medical treatment and monetary benefits of injured workers in this state are already regulated extensively by an all-inclusive statutory structure.

Importantly, the right to recover compensation and treatment under the workers' compensation system is the sole and exclusive remedy for injury or death of an employee against the employer or co-employee acting within the scope of his or her employment,¹³ making participation in the workers' compensation system mandatory for both employers and employees.

Thus, we respectfully submit that all aspects of the workers' compensation statutory and constitutional system should be exempted entirely from CCPA. We therefore strongly urge that the Attorney General adopt regulations to establish an exception from the CCPA for the workers' compensation system, as specifically authorized in Civil Code Section 1798.185 (a) (3):

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas: [...]

(3) *Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.* (Emphasis added)

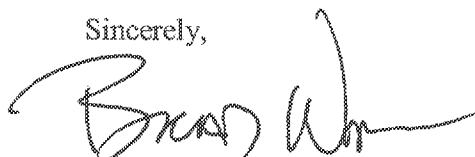
Workers' compensation is a heavily regulated industry, with an extensive body of statutory and constitutional laws governing it. We strongly believe that exempting workers' compensation from the CCPA is appropriate, and we respectfully urge this action be taken as it is "...*necessary to comply with state law...*"¹⁴

Suggested regulatory language is provided as follows:

Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code does not apply to medical or personal information collected by a business, medical provider network, third party administrator, insurer or other third-party entity for the purpose of providing medical treatment or administering claims pursuant to Division 4 (commencing with Section 3200) of the Labor Code.

Thank you for your consideration.

Sincerely,



Brad Walker
Executive Director
California Alliance of Self-Insured Groups

¹³ See, Labor Code, § 3602 (a)

¹⁴ Civil Code § 1798.185 (a) (3)

Message

From: Jennifer Sheridan [REDACTED]
Sent: 3/8/2019 9:42:31 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Jennifer Sheridan [REDACTED]
Subject: Written Comments re CCPA

Dear Attorney General:

I appreciate your (and your team's) willingness to solicit and review public comments on the California Consumer Privacy Act (CCPA).

My comments address two issues:

1. IP addresses as personal data and covered by CCPA; and
2. Verification of consumer requests under the CCPA.

I am an attorney who has practiced for twenty plus years as both in-house and outside counsel to Silicon Valley technology companies. My suggestions reflect concerns raised by my clients whose goal is to reduce friction in business processes. They are happy to comply with reasonable regulations where the rules of the road are clear and transparent in their operation.

I represent a wide range of companies but here I am focusing on my clients who neither meet the either the \$25 m revenue threshold nor the data broker threshold. They may meet the second threshold - handles data of more than 50,000 persons or devices.

1. What is personal data?

I have attended both hearings held by the State Assembly and Senate on the CCPA. At both hearings Alistair MacTaggart spoke to the respective committees. On this question of whether a company was covered by the CCPA for collecting (or handling) IP addresses alone, he seemed to indicate that the law was not meant to include IP addresses (in his opinion).

I find this interesting because in my client work for GDPR compliance, I advise my clients that IP addresses are considered personal data under the GDPR.

I advise them to consider implementing a data retention policy where they do not store/retain this data so that their obligations for access are more reasonably managed.

Recommendation: Clarification on whether IP addresses (and device data more generally) is covered in the 50,000 threshold.

2. Verification of user request

This question has been amply covered in the public hearings. I just wanted to note that my clients would like workable clear rules of the road on how to implement this process.

Best regards,

Jennifer (Jenny) Sheridan, Esq.
[REDACTED]

Message

From: Randall G. [REDACTED]
Sent: 2/6/2019 3:46:40 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write as both Californians who are quite concerned about the sale of our data to third parties without our permission (and in most cases, without even our knowledge), and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we discover in the press, usually after the fact, occasionally the price we pay for such services is the exposure of our private data to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to those who don't opt out. This means that higher prices can be targeted to customers who choose privacy. That can be a slippery slope.

At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Randall G.

[REDACTED]

Message

From: Samuel Durkin [REDACTED]
Sent: 2/1/2019 9:38:29 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Samuel Durkin
[REDACTED]

Message

From: Mark Bartleman [REDACTED]
Sent: 12/21/2018 8:10:28 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Mark Bartleman
[REDACTED]

Message

From: Alison Victor [REDACTED]
Sent: 12/21/2018 8:10:20 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Alison Victor
[REDACTED]

Message

From: Therese Ryan [REDACTED]
Sent: 12/21/2018 8:06:57 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Therese Ryan
[REDACTED]

Message

From: Charlie K [REDACTED]
Sent: 12/21/2018 8:06:43 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 per year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Charlie K
[REDACTED]

Message

From: Caryn Graves [REDACTED]
Sent: 12/21/2018 8:05:13 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Caryn Graves
[REDACTED]

Message

From: Sahar Driver [REDACTED]
Sent: 12/21/2018 8:02:31 AM
To: Privacy Regulations [REDACTED]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Sahar Driver
[REDACTED]

Message

From: Nancy Warfield [REDACTED]
Sent: 12/21/2018 8:01:39 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,

[REDACTED]

Message

From: Robert Duckson [REDACTED]
Sent: 12/21/2018 7:58:27 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Robert Duckson
[REDACTED]

Message

From: Catherine George [REDACTED]
Sent: 12/21/2018 7:56:27 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Catherine George
[REDACTED]

Message

From: Steven C. Serbins [REDACTED]
Sent: 12/21/2018 7:52:25 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Steven C. Serbins
[REDACTED]

Message

From: Obie Hunt [REDACTED]
Sent: 2/1/2019 9:31:53 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Obie Hunt
[REDACTED]

Message

From: David Snope [REDACTED]
Sent: 12/21/2018 7:41:52 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,

[REDACTED]

Message

From: Erin Garcia [REDACTED]
Sent: 12/21/2018 7:40:26 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Erin Garcia
[REDACTED]

Message

From: John Kyrk [REDACTED]
Sent: 12/21/2018 7:39:20 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
John Kyrk
[REDACTED]

Message

From: R.G. Tuomi [REDACTED]
Sent: 12/21/2018 7:37:40 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
R.G. Tuomi
[REDACTED]

Message

From: Joan Smith [REDACTED]
Sent: 12/21/2018 7:32:56 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Joan Smith
[REDACTED]

Message

From: Urmila Padmanabhan [REDACTED]
Sent: 12/21/2018 7:30:42 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Urmila Padmanabhan
[REDACTED]

Message

From: Michelle Orengo-McFarlane [REDACTED]
Sent: 12/21/2018 7:21:12 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Michelle Orengo-McFarlane
[REDACTED]

Message

From: Chad Johnson [REDACTED]
Sent: 12/21/2018 7:14:40 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Chad Johnson
[REDACTED]

Message

From: Katherine McNeill [REDACTED]
Sent: 12/21/2018 7:12:37 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Katherine McNeill
[REDACTED]

Message

From: paul Runion [REDACTED]
Sent: 12/21/2018 7:10:17 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
paul Runion
[REDACTED]

Message

From: Joyce Lee [REDACTED]
Sent: 1/10/2019 11:54:36 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Joyce Lee
[REDACTED]

Message

From: Carol Figueiredo [REDACTED]
Sent: 12/21/2018 7:08:57 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Carol Figueiredo
[REDACTED]

Message

From: Klaudia Englund [REDACTED]
Sent: 12/21/2018 7:06:57 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Klaudia Englund
[REDACTED]

Message

From: Richard Patenaude [REDACTED]
Sent: 12/21/2018 7:05:59 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Richard Patenaude
[REDACTED]

Message

From: Paul Kattner [REDACTED]
Sent: 12/21/2018 7:03:07 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Paul Kattner
[REDACTED]

Message

From: J Furstoss [REDACTED]
Sent: 12/21/2018 7:01:52 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise. This is important. Thank you.

Sincerely,
J Furstoss
[REDACTED]

Message

From: Joyce Lee [REDACTED]
Sent: 1/10/2019 11:54:01 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Joyce Lee

[REDACTED]

Message

From: james roberts [REDACTED]
Sent: 12/30/2018 1:21:36 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
james roberts
[REDACTED]

Message

From: allan reed [REDACTED]
Sent: 12/30/2018 10:35:37 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
allan reed
[REDACTED]

Message

From: Paul Williams [REDACTED]
Sent: 12/29/2018 6:25:18 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Paul Williams
[REDACTED]

Message

From: Lilithe Magdalene [REDACTED]
Sent: 12/29/2018 2:33:08 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Lilithe Magdalene
[REDACTED]

Message

From: Neal Tomblin [REDACTED]
Sent: 12/27/2018 5:19:40 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Neal Tomblin
[REDACTED]

Message

From: Randall G. [REDACTED]
Sent: 12/27/2018 2:37:08 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We have discovered that your office has a big task in front of it to make this new law operational and functional.

We write to you as both Californians who are concerned about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the present CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Randall G.

[REDACTED]

Message

From: Paul Williams [REDACTED]
Sent: 2/1/2019 10:51:43 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Paul Williams
[REDACTED]

Message

From: Sharon Paltin [REDACTED]
Sent: 12/26/2018 3:10:53 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Sharon Paltin
[REDACTED]

Message

From: Terry Twitchell [REDACTED]
Sent: 12/26/2018 1:17:51 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Terry Twitchell
[REDACTED]

Message

From: Don Fogg [REDACTED]
Sent: 12/26/2018 1:04:32 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Don Fogg
[REDACTED]

Message

From: john s [REDACTED]
Sent: 12/25/2018 7:23:22 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
john s
[REDACTED]

Message

From: Mike Hall [REDACTED]
Sent: 12/24/2018 10:55:09 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Mike Hall
[REDACTED]

Message

From: Alfa Santos [REDACTED]
Sent: 12/23/2018 1:45:22 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Alfa Santos

[REDACTED]

Message

From: CT Bross [REDACTED]
Sent: 12/23/2018 11:56:26 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
CT Bross

[REDACTED]

Message

From: James Massar [REDACTED]
Sent: 12/23/2018 8:43:01 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
James Massar

[REDACTED]

Message

From: Sharon Lieberman [REDACTED]
Sent: 12/22/2018 8:53:42 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Sharon Lieberman
[REDACTED]

Message

From: STACIE CHARLEBOIS [REDACTED]
Sent: 12/22/2018 8:44:58 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
STACIE CHARLEBOIS
[REDACTED]

Message

From: Barbara Harper [REDACTED]
Sent: 2/1/2019 9:23:41 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Barbara Harper
[REDACTED]

Message

From: James Michael "Mike" Henderson [REDACTED]
Sent: 12/22/2018 7:09:20 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
James Michael "Mike" Henderson
[REDACTED]

Message

From: Mary Behm-Steinberg [REDACTED]
Sent: 12/22/2018 3:17:34 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Mary Behm-Steinberg
[REDACTED]

Message

From: Callie Riley [REDACTED]
Sent: 12/22/2018 2:39:30 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Callie Riley

[REDACTED]

Message

From: j hester [REDACTED]
Sent: 12/22/2018 1:03:15 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Privacy is a right, not a commodity.

Sincerely,

j hester
[REDACTED]

Message

From: Rachel Rose [REDACTED]
Sent: 12/22/2018 12:56:42 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Rachel Rose
[REDACTED]

Message

From: B. Chan [REDACTED]
Sent: 12/22/2018 11:07:41 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
B. Chan
[REDACTED]

Message

From: Victoria Miller [REDACTED]
Sent: 12/22/2018 7:39:43 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Victoria Miller
[REDACTED]

Message

From: Ian Turner [REDACTED]
Sent: 12/22/2018 6:11:16 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Ian Turner



Message

From: Karen Berger [REDACTED]
Sent: 12/22/2018 12:12:00 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Karen Berger

[REDACTED]

Message

From: ORPHA DESS WILSON [REDACTED]
Sent: 12/21/2018 11:26:50 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
ORPHA DESS WILSON
[REDACTED]

Message

From: Joe Salazar [REDACTED]
Sent: 2/1/2019 8:23:43 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Joe Salazar
[REDACTED]

Message

From: Dylan Nguyen [REDACTED]
Sent: 12/21/2018 9:33:08 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Dylan Nguyen
[REDACTED]

Message

From: Jon Bazinet [REDACTED]
Sent: 12/21/2018 9:26:41 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Jon Bazinet
[REDACTED]

Message

From: diana koeck [REDACTED]
Sent: 12/21/2018 8:32:02 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
diana koeck
[REDACTED]

Message

From: Chris OMeara Dietrich [REDACTED]
Sent: 12/21/2018 6:34:21 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

I applaud California's passing the nation's first comprehensive consumer privacy legislation, but I write to you today as a consumer of modest means who uses a large assortment of services online and offline where my personal information may be collected.

But finding out in the press, usually after the fact, that the service companies have grown very rich selling my personal information at a volume and scope that is mind boggling and concealing that they did it angers me because the trade has not been of much value to me as a consumer.

CCPA will do a lot to help me understand what my choices are and what the consequences of my decisions will be. I appreciate the opportunity to opt out if I don't want those consequences.

But I am concerned about the non-discrimination clause.

While CCPA does contain a non-discrimination clause so consumers can't be punished if they choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out.

As I understand this, companies spent years stealing my personal information, making billions off it, and now that California mandates that I get information about what information they want and have the opportunity to opt out, I can pay more because I now have the privacy they previously took and sold.

And since I engage in data-laden transactions with hundreds of companies every year, this means possibly lots more cost to me if I opt out--fees like \$5 or \$10 year, if applied multiple by multiple companies every year, are going to add up quickly.

I don't have an extra hundred or two laying around that I what to contribute to these companies earnings. Remember, they're rich, I'm not and they got rich by stealing from me.

And I am not interested in sorting among the available opt-outs to pick the particular companies in order to get the most bang for my limited privacy buck. That is a time wasting onerous task slogging through legalese. Yuck!

Without regulatory constraints, I feel the current CCPA language will wind up to be of limited use to ordinary web users like me—the communities most victimized by identity theft and predatory marketers.

To really support California consumers, the regulation should have concise language that details what information I get, an easy way to opt out, eliminate future re-opting out, and not allow increased charges for opting out.

I ask that you not allow the right to opt-out to turn the CCPA into a paper right that few will actually exercise either

because of the monetary burden or the onerous chore of figuring out what the real choice is.

Sincerely,

Chris OMeara Dietrich



Message

From: Claire Perricelli [REDACTED]
Sent: 12/21/2018 6:18:09 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Claire Perricelli
[REDACTED]

Message

From: Barbara Harper [REDACTED]
Sent: 12/21/2018 6:10:48 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Barbara Harper
[REDACTED]

Message

From: Dennis McCoy [REDACTED]
Sent: 12/21/2018 4:22:20 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Dennis McCoy
[REDACTED]

Message

From: Carl Estes [REDACTED]
Sent: 12/21/2018 3:00:51 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Carl Estes
[REDACTED]

Message

From: Michael Kast [REDACTED]
Sent: 12/21/2018 2:59:05 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Michael Kast
[REDACTED]

Message

From: Leonard Tremmel [REDACTED]
Sent: 12/21/2018 2:59:01 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Leonard Tremmel
[REDACTED]

Message

From: B. E. [REDACTED]
Sent: 2/1/2019 4:26:21 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
B. E.

[REDACTED]

Message

From: Linda Weiner [REDACTED]
Sent: 12/21/2018 2:49:09 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Linda Weiner

[REDACTED]

Message

From: Dr. and Mrs. Phil and Lynn Fischer [REDACTED]
Sent: 12/21/2018 2:20:55 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,

Dr. and Mrs. Phil and Lynn Fischer
[REDACTED]

Message

From: Steven Hernandez [REDACTED]
Sent: 12/21/2018 2:02:27 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Steven Hernandez
[REDACTED]

Message

From: Michael Denton [REDACTED]
Sent: 12/21/2018 1:49:36 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Michael Denton
[REDACTED]

Message

From: Ed Green [REDACTED]
Sent: 12/21/2018 12:32:20 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Ed Green



Message

From: David Adams [REDACTED]
Sent: 12/21/2018 12:22:07 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
David Adams
[REDACTED]

Message

From: Colleen Bergh [REDACTED]
Sent: 12/21/2018 12:08:34 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Colleen Bergh
[REDACTED]

Message

From: Ann Bein [REDACTED]
Sent: 12/21/2018 12:04:11 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Ann Bein
[REDACTED]

Message

From: Gabriel Lautaro [REDACTED]
Sent: 12/21/2018 11:46:34 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Gabriel Lautaro

[REDACTED]

Message

From: jesse calderon [REDACTED]
Sent: 12/21/2018 11:45:59 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
jesse calderon
[REDACTED]

Message

From: Michael Denton [REDACTED]
Sent: 2/1/2019 2:37:31 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Michael Denton
[REDACTED]

Message

From: Susan Walp [REDACTED]
Sent: 12/21/2018 11:33:55 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Susan Walp
[REDACTED]

Message

From: Lucienne O'Keefe [REDACTED]
Sent: 12/21/2018 11:33:07 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Lucienne O'Keefe
[REDACTED]

Message

From: Jonathan Boyne [REDACTED]
Sent: 12/21/2018 11:28:49 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Jonathan Boyne
[REDACTED]

Message

From: Monica M Gallichio [REDACTED]
Sent: 12/21/2018 11:23:17 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Monica M Gallichio

[REDACTED]

Message

From: Eileen Massey [REDACTED]
Sent: 12/21/2018 11:21:39 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Eileen Massey
[REDACTED]

Message

From: Lauren Linda [REDACTED]
Sent: 12/21/2018 11:12:25 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Lauren Linda
[REDACTED]

Message

From: Arlene Baker [REDACTED]
Sent: 12/21/2018 11:08:01 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Arlene Baker

[REDACTED]

Message

From: Ricardo Frustockl [REDACTED]
Sent: 12/21/2018 11:01:16 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Ricardo Frustockl
[REDACTED]

Message

From: Claudia Frantz [REDACTED]
Sent: 12/21/2018 11:00:17 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Claudia Frantz
[REDACTED]

Message

From: Katherine Schaff [REDACTED]
Sent: 12/21/2018 10:44:49 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Katherine Schaff
[REDACTED]

Message

From: Susan Walp [REDACTED]
Sent: 2/1/2019 1:12:27 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Susan Walp
[REDACTED]

Message

From: Lois Corrin [REDACTED]
Sent: 12/21/2018 10:40:17 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Lois Corrin

[REDACTED]

Message

From: Jaime Nahman [REDACTED]
Sent: 12/21/2018 10:40:13 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Jaime Nahman
[REDACTED]

Message

From: gloriana casey [REDACTED]
Sent: 12/21/2018 10:32:13 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise**, READ Amendment 4-- because this 3rd party action=unreasonable search & seizure!

Sincerely,
gloriana casey
[REDACTED]

Message

From: Lara Dale [REDACTED]
Sent: 12/21/2018 10:13:03 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Lara Dale
[REDACTED]

Message

From: troy troyer [REDACTED]
Sent: 12/21/2018 10:11:01 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
troy troyer

[REDACTED]

Message

From: Michael Garitty [REDACTED]
Sent: 12/21/2018 10:09:22 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Michael Garitty
[REDACTED]

Message

From: Max Kaehn [REDACTED]
Sent: 12/21/2018 10:07:51 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Max Kaehn

[REDACTED]

Message

From: Ann Thryft [REDACTED]
Sent: 12/21/2018 9:56:50 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Ann Thryft
[REDACTED]

Message

From: MICHAEL WALTER [REDACTED]
Sent: 12/21/2018 9:56:05 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
MICHAEL WALTER
[REDACTED]

Message

From: Vic DeAngelo [REDACTED]
Sent: 12/21/2018 9:55:46 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Vic DeAngelo
[REDACTED]

Message

From: Urmila Padmanabhan [REDACTED]
Sent: 2/1/2019 11:16:32 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Urmila Padmanabhan
[REDACTED]

Message

From: Carol Vallejo [REDACTED]
Sent: 12/21/2018 9:54:32 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Carol Vallejo
[REDACTED]

Message

From: Stephen Rosenblum [REDACTED]
Sent: 12/21/2018 9:30:56 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Stephen Rosenblum
[REDACTED]

Message

From: Isaac Wingfield [REDACTED]
Sent: 12/21/2018 9:17:53 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Isaac Wingfield
[REDACTED]

Message

From: Karl Koessel [REDACTED]
Sent: 12/21/2018 9:14:01 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Karl Koessel

[REDACTED]

Message

From: James Dawson [REDACTED]
Sent: 12/21/2018 9:06:10 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
James Dawson



Message

From: james roberts [REDACTED]
Sent: 12/21/2018 9:05:49 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
james roberts

[REDACTED]

Message

From: Susan Hathaway [REDACTED]
Sent: 12/21/2018 9:05:45 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Susan Hathaway

[REDACTED]

Message

From: Nicole Fountain [REDACTED]
Sent: 12/21/2018 8:57:36 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Nicole Fountain
[REDACTED]

Message

From: Tom Voorhees [REDACTED]
Sent: 12/21/2018 8:57:24 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Tom Voorhees
[REDACTED]

Message

From: Nora Roman [REDACTED]
Sent: 12/21/2018 8:56:15 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent. I personally am sick of the permission for corporations to invade my privacy by selling my information, and by allowing other corporations to call my house with robots and humans to disturb me to pressure me to buy things I don't want. I am 100% opposed to having to PAY companies not to sell my information. This is ridiculous...They should have to pay me if they sell my information.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Nora Roman

[REDACTED]

Message

From: Ann Thryft [REDACTED]
Sent: 2/1/2019 10:16:30 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Ann Thryft
[REDACTED]

Message

From: David Waggoner [REDACTED]
Sent: 12/21/2018 8:52:23 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
David Waggoner

[REDACTED]

Message

From: bill gisbrecht [REDACTED]
Sent: 12/21/2018 8:52:03 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
bill gisbrecht
[REDACTED]

Message

From: Joel Levine [REDACTED]
Sent: 12/21/2018 8:49:34 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Joel Levine
[REDACTED]

Message

From: Scott Barlow [REDACTED]
Sent: 12/21/2018 8:48:19 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Scott Barlow

[REDACTED]

Message

From: Kathleen Rippey [REDACTED]
Sent: 12/21/2018 8:42:10 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Kathleen Rippey
[REDACTED]

Message

From: Karynn Merkel [REDACTED]
Sent: 12/21/2018 8:28:15 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Karynn Merkel

[REDACTED]

Message

From: Prisca Gloor [REDACTED]
Sent: 12/21/2018 8:27:49 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Prisca Gloor

[REDACTED]

Message

From: Jonathan Tachibana [REDACTED]
Sent: 12/21/2018 8:26:49 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Jonathan Tachibana



Message

From: karoline hatch-berens [REDACTED]
Sent: 12/21/2018 8:24:38 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
karoline hatch-berens

[REDACTED]

Message

From: Jared Laiti [REDACTED]
Sent: 12/21/2018 8:15:51 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget." Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise,

Sincerely,
Jared Laiti

[REDACTED]

Message

From: Adrian Martinez [REDACTED]
Sent: 2/22/2019 1:46:12 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: We Can Only Pay So Much For Privacy

Dear Coordinator Privacy Regulations,

California has taken an innovative step by passing the nation's first comprehensive consumer privacy legislation. We understand that your office has a big task in front of it to make this new law operational and functional.

We write to you today as both Californians who worry about the sale of our data to third parties without our consent and as consumers of modest means who use a large assortment of services online and offline where our personal information may be collected. Like most people, to at least some extent, we enjoy some of the convenience that comes with targeted services. But as we find out in the press, usually after the fact, sometimes the price we pay for such services is the exposure of our personal information to parties we never expected. It wouldn't always be worth it if we knew what we were doing.

CCPA will do a lot to help us understand what the consequences of our decisions will be, and give us the opportunity to opt out if we don't want those consequences. But we have some concerns about the non-discrimination clause. CCPA does contain a non-discrimination clause so we can't be punished if we choose to opt out, but it leaves the door open for companies to charge lower prices to people who don't opt out. This means that higher prices can be charged to customers who choose privacy. That can be a slippery slope.

We want to caution that many consumers, if not most, engage in data-laden transactions with hundreds of companies every year. While all may not be subject to CCPA, it seems clear that consumers will be making opt-in or opt-out decisions at least dozens of times annually. California has one of the highest costs of living in the nation. Many working class households and people of modest means are without significant disposable income that would cover a "privacy budget". Even seemingly modest fees like \$5 or \$10 year, if applied multiple times every year, are going to add up, especially for large families, renters struggling to meet the highest rental costs in the nation, single parents, minimum wage workers and others who are already struggling. Despite being very concerned about the privacy of their data, if it is a choice between food on the table and consumer privacy, food on the table will always win. A process of sorting among the available opt-outs to pick the particular companies whose practices are most egregious in order to get the most bang for the limited privacy buck, is an onerous task for a literal privacy expert and a lot to expect from a minimum wage worker or a busy single parent. At best, without regulatory constraints, the current CCPA language can create privacy-haves and privacy have-nots and be of limited use to the communities most victimized by identity theft and predatory marketers.. At worst, without appropriate regulation, it will turn the right to opt-out into a paper right that few will actually exercise.

Sincerely,
Adrian Martinez
[REDACTED]

Message

From: Diane Love [REDACTED]
Sent: 3/8/2019 9:00:00 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: AG should exempt the WC from CCPA
Attachments: CCPA.pdf

Hi- Here is a letter from our company stating how we would like to see the vote.

Thanks



Diane Love

Office Manager, Brady Company/Los Angeles, Inc.

[REDACTED] a: P.O. Box 470, Anaheim, CA 92815

w: www.brady.com/los-angeles/ e: [REDACTED]



This email has been scanned for email related threats and delivered safely by Mimecast.
For more information please visit <http://www.mimecast.com>



March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

VIA US MAIL and EMAIL

TO WHOM IT MAY CONCERN:

The following comments are submitted on behalf of Kaiser, Sharp Rees Stealy, One Call, Healthnet, Peninsula Healthcare and Washington Hospital.

**The Attorney General Should Exempt the Workers' Compensation System
From the California Consumer Privacy Act**

The California Consumer Privacy Act (CCPA) directs the Attorney General to adopt regulations to further the purposes of the CCPA, including "...[e]stablishing any exceptions necessary to comply with state or federal law, ... within one year of passage of this title and as needed thereafter."¹

**An Exception From CCPA is Necessary to Comply With the California Constitution
and State Laws Governing the Workers' Compensation System**

1) The workers' compensation system is established and regulated pursuant to the state Constitution.

The state Constitution confers plenary power on the Legislature to enact a comprehensive worker's compensation system. Section 4 of Article XIV of the state Constitution vests the Legislature with "plenary power, unlimited by any provision of this Constitution, to create, and enforce a complete system of workers' compensation, by appropriate legislation."² This constitutional mandate gives the Legislature "complete, absolute and unqualified power to create

¹ Civil Code §1798.185 (a) (3)

² Cal Const. Article XIV, § 4

and enact the workers' compensation system."³ California courts have interpreted this grant of broad power to mean that "absolutely nothing" in Section 4 "purports to limit the Legislature's authority to enact additional appropriate legislation for the protection of employees."⁴

The constitutional grant of power has "compelled the conclusion" that Section 4 of Article XIV of the state Constitution supersedes the state Constitution's Due Process clause with respect to legislation passed under the Legislature's plenary powers over the workers' compensation system.⁵ Courts have held that, even if conflicts existed between Section 4 [workers' compensation] and other state Constitutional provisions governing Separation of Powers or Due Process, "the plenary powers conferred by Section 4 would still control."⁶

The courts have unambiguously held that the provisions of the California Constitution governing workers' compensation are not limited by other provisions of the state Constitution, including the Due Process and Separation of Powers clauses.

These interpretations lead to a likely conclusion that, by its own terms, the constitutional provisions governing workers' compensation will also control over state constitutional provisions in Section 1 of Article I pertaining to the right to Privacy, so long as the Legislature has employed its "...plenary power, *unlimited by any provision of this Constitution*, to create, and enforce a complete system of workers' compensation, by appropriate legislation."⁷

2) Pursuant to its constitutional mandate, the Legislature has enacted a comprehensive workers' compensation system by statute.

Section 4 of Article XIV of the state Constitution provides in part that "[a] complete system of workers' compensation includes...full provision for vesting power, authority and jurisdiction in an administrative body with all the requisite governmental functions to determine any dispute or matter arising under such legislation." The intent behind Section 4 "was to endow [the Legislature] expressly with exclusive and 'plenary' authority to determine the contours and content of our state's workers' compensation system."⁸ The only limitations on the Legislature's plenary powers are that the Legislature cannot act outside of its authority to create and to enforce a complete system of workers' compensation or enact a provision that conflicts with federal

³ *Facundo-Guerrero v. Workers' Comp. Appeals Bd.* (2008) 163 Cal.App.4th 640, 650 [intent behind Section 4 "was to endow [the Legislature] expressly with exclusive and 'plenary' authority to determine the contours and content of our state's workers' compensation system"].

⁴ *City and County of San Francisco v. Workers' Comp. Appeals Bd. (Wiebe)* (1978) 22 Cal.3d 103, 114

⁵ *Hustedt v. Workers' Comp. Appeals Bd.* (1981) 30 Cal.3d 329, 343 ["It is well established that adoption of [Section 4] 'effected a repeal pro tanto' of any state constitutional provisions which conflicted with that amendment"]; see also *Greener v. Workers' Comp. Appeals Bd.* (1993) 6 Cal.4th 1028 [article VI of the state Constitution governing courts' jurisdiction inapplicable to extent Legislature has exercised its powers under Section 4]

⁶ *Stevens v. Workers' Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

⁷ (Emphasis added) Cal Const. Article XIV, § 4

⁸ *Facundo-Guerrero v. Workers' Comp. Appeals Bd.* (2008) 163 Cal.App.4th 640, 650

law.⁹ The state Constitution, and the cases interpreting it, confirm that “nearly any exercise of the Legislature’s plenary powers over workers’ compensation is permissible so long as the Legislature finds its action to be ‘necessary to the effectiveness of the system of workers’ compensation.’”¹⁰

Acting under this power, the Legislature enacted the workers’ compensation law to govern compensation to California workers who are injured in the course of their employment.¹¹

The underlying premise behind this statutorily created system is the “compensation bargain, [under which] the employer assumes liability for industrial personal injury or death without regard to fault in exchange for limitations on the amount of that liability. The employee is afforded relatively swift and certain payment of benefits to cure or relieve the effects of industrial injury without having to prove fault but, in exchange, gives up the wider range of damages potentially available in tort.”¹² The workers’ compensation law requires employers to secure the payment of workers’ compensation benefits either by purchasing third-party insurance or by self-insuring with permission from the Department of Industrial Relations.¹³

In addition, where the “conditions of compensation” exist, the right to recover such compensation is the “sole and exclusive remedy” of the employee or his or her dependents against the employer when acting within the scope of his or her employment.¹⁴

3) Existing privacy protections in the workers’ compensation system

There are several privacy requirements within the Labor Code directly applicable to workers’ compensation. Labor Code Section 138.7 provides in part:

“A person or public or private entity not a party to a claim for workers’ compensation benefits shall not obtain individually identifiable information obtained or maintained by the division on that claim. For purposes of this section, ‘individually identifiable information’ means any data concerning an injury or claim that is linked to a uniquely identifiable employee, employer, claims administrator, or any other person or entity.”

⁹ *Hustedt v. Workers’ Comp. Appeals Bd.* (1981) 30 Cal.3d 329; see also, *Stevens v. Workers’ Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

¹⁰ *Stevens v. Workers’ Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

¹¹ Division 4 (commencing with Section 3200) of the Labor Code

¹² *Charles J. Vacanti, M.D., Inc. v. State Comp. Ins. Fund* (2001) 24 Cal.4th 800, 811. See also, *Shoemaker v. Myers* (1990) 52 Cal.3d 1

¹³ Labor Code § 3700

¹⁴ Labor Code § 3602 (a)

There are limited exceptions to that rule, but it is unlawful for any person who has received individually identifiable information from the division pursuant to this section to provide that information to any person who is not entitled to it.¹⁵ In a similar way, Labor Code Section 3762 (c) states:

“An insurer, third-party administrator retained by a self-insured employer pursuant to Section 3702.1 to administer the employer’s workers’ compensation claims, and those employees and agents specified by a self-insured employer to administer the employer’s workers’ compensation claims, are prohibited from disclosing or causing to be disclosed to an employer, any medical information, as defined in Section 56.05 of the Civil Code, about an employee who has filed a workers’ compensation claim, except as follows: (1) Medical information limited to the diagnosis of the mental or physical condition for which workers’ compensation is claimed and the treatment provided for this condition. (2) Medical information regarding the injury for which workers’ compensation is claimed that is necessary for the employer to have in order for the employer to modify the employee’s work duties.”

Insofar as electronic billing purposes are concerned, Labor Code Section 4603.4 (b) specifies that that billing standards developed by the Division of Workers’ Compensation (DWC), “...shall be consistent with existing standards under the federal Health Insurance Portability and Accountability Act of 1996.”

Labor Code Section 4610.5 (m) states that when a claims administrator is transmitting medical records pursuant to a request for independent medical review, “The confidentiality of medical records shall be maintained pursuant to applicable state and federal laws.” Confidentiality of medical information was also addressed by the Legislature in Labor Code Section 4903.6 (d):

“With the exception of a lien for services provided by a physician as defined in Section 3209.3, a lien claimant shall not be entitled to any medical information, as defined in subdivision (g) of Section 56.05 of the Civil Code, about an injured worker without prior written approval of the appeals board. Any order authorizing disclosure of medical information to a lien claimant other than a physician shall specify the information to be provided to the lien claimant and include a finding that the information is relevant to the proof of the matter for which the information is sought.”

In summary, privacy protections within the Labor Code extensively address protection of medical information.

4) Workers’ Compensation is a comprehensive statutory medical, legal and adjudicatory system that is incompatible with the provisions of the CCPA.

Each day, personal and medical information concerning hundreds of thousands of injured workers is circulated from a Medical Provider Network (MPN) or insurance claims administrator

¹⁵ Labor Code § 138.7

to the physician, to the physician specialist to whom an injured worker may be referred, to the Utilization Review Organization, an Independent Medical Review (IMR) service, an Independent Bill Review (IBR) organization, and Electronic Billing Review organization, Pharmacy Benefit Managers, Vocational Rehabilitation Counselors, Job Training and Supplemental Job Displacement Benefit entities, and more.

Additionally, MPN administrators and self-insured employers are required to report injured workers' medical information to the Office of Self-Insured Plans, Workers' Compensation Information System, Workers' Compensation Appeals Board and the Workers' Compensation Insurance Rating Bureau, all mandatory reporting requirements that would trigger disclosure notifications under the CCPA.

Because an injured worker cannot, and would clearly not wish to frustrate the adjusting of a claim by not allowing information to be disclosed to those who are integral to the workers' compensation medical treatment and benefit payment system, the disclosures nevertheless must be provided to the workers' compensation claimant or applicant. Failure to do so can result in penalties and enforcement actions from the California Department of Justice and the Department of Industrial Relations.

For example, Civil Code § 1798.115(a) of the CCPA states that the consumer has a right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer (1) the categories of personal information that the business collected about the consumer, (2) the categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold, and (3) the categories of personal information that the business disclosed about the consumer for a business purpose.

Section 1798.115(a) would likely apply to nearly all workers' compensation claims transactions. As noted above, medical records are sent to a medical provider network (MPN), medical records are sent to a utilization review organization (URO), and medical records are sent to an independent review organization (IRO). "Personal information" would clearly include payment information sent to a payment processing center falling within the definition of "service provider." A vocational evaluator would clearly need to know "professional or employment-related information" that is included within the definition of "personal information" in Civil Code Sec. 1798.140(o)(1)(I).

During the routine administration of a workers' compensation claim, especially a claim involving indemnity benefits, considerable "personal information," as defined in Civil Code Sec. 1798.140(o), must be collected so that the claim can be processed and the injured worker can be treated and compensated. For physicians and other service providers, an injured worker's personal information is collected during the payment and remittance process. In addition, the placement of insurance, including providing and disclosure claims information, is a vital function in the workers' compensation system.

By law, workers' compensation claimants are considered "consumers" for purposes of the Insurance Information and Privacy Protection Act.¹⁶ Therefore, the notice of information practices required by Insurance Code Sec. 791.04 applies to workers' compensation insurers.

Although these are just a few examples, the fact remains that each and every referral or transmittal cited above would, pursuant to the CCPA, trigger a disclosure notification to the injured worker. The sheer number of notices that would be generated pursuant to the CCPA has, in the case of one large MPN doing business in the state, been estimated to generate nearly 61 million pieces of paper for each 150,000 claims during routine claims processing operations.

Yet, every one of these transactions are already governed by a comprehensive body of *existing state law*. Moreover, because workers' compensation is the sole and exclusive remedy for all injuries and illnesses that occur within the course and scope of employment, the injured employees would not be allowed to opt out of participation as is provided for within the CCPA.

Therefore, although an injured worker cannot prevent the adjusting of a claim by refusing to allow information to be given to workers' compensation service providers, the notification disclosures nevertheless must be sent if the CCPA were to apply. Failure to do so can result in penalties and enforcement actions from the Department of Justice.

5) A regulatory exception from CCPA is needed in order to comply with the comprehensive constitutionally mandated and legislatively enacted workers' compensation system.

The workers' compensation system is a unique body of state law that is breathtaking in its scope and applicability. The workers' compensation system has its own legal and court adjudication system. Medical treatment offered within the workers' compensation system is completely separate and apart from the state's health care delivery system. Nearly every aspect of an injured worker's medical care, vocational rehabilitation, and benefit payments is governed by state law and subject to extensive oversight by the Division of Workers' Compensation within the state Department of Industrial Relations.

This petition for an exception from CCPA in order to comply with state law, as authorized pursuant to Civil Code Section 1798.185 (a) (3), is presented herein on account of the fact that these extremely complex and comprehensive transactions that take place every day concerning the medical treatment and monetary benefits of injured workers in this state are already regulated extensively by an all-inclusive statutory structure.

Importantly, the right to recover compensation and treatment under the workers' compensation system is the sole and exclusive remedy for injury or death of an employee against the employer or co-employee acting within the scope of his or her employment,¹⁷ making participation in the workers' compensation system mandatory for both employers and employees.

¹⁶ Insurance Code § 791 et seq.

¹⁷ See, Labor Code, § 3602 (a)

Thus, we respectfully submit that all aspects of the workers' compensation statutory and constitutional system should be exempted entirely from CCPA. We therefore strongly urge that the Attorney General adopt regulations to establish an exception from the CCPA for the workers' compensation system, as specifically authorized in Civil Code Section 1798.185 (a) (3):

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas: [...]

(3) *Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.* (Emphasis added)

Workers' compensation is a heavily regulated industry, with an extensive body of statutory and constitutional laws governing it. We strongly believe that exempting workers' compensation from the CCPA is appropriate, and we respectfully urge this action be taken as it is "...*necessary to comply with state law...*"¹⁸

Suggested regulatory language is provided as follows:

Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code does not apply to medical or personal information collected by a business, medical provider network, third party administrator, insurer or other third-party entity for the purpose of providing medical treatment or administering claims pursuant to Division 4 (commencing with Section 3200) of the Labor Code.

Thank you for your consideration.

Sincerely,



Bill Saddler
President
Brady Company/Los Angeles, Inc.

¹⁸ Civil Code § 1798.185 (a) (3)

Message

From: Mullon, Walter [REDACTED]
Sent: 3/8/2019 8:44:20 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Gordon, Philip L. [REDACTED]; Sarchet, Bruce J. [REDACTED]
Subject: Comments on CCPA
Attachments: WPI Comments - CCPA of 2018.pdf

To Whom It May Concern:

On behalf of Littler's Workplace Policy Institute, please see the attached comments in regards to the California Consumer Privacy Act of 2018.

Thank you.

Walt Mullon
Sr. Manager - Workplace Policy Institute

[REDACTED]
815 Connecticut Avenue, NW, Suite 400 | Washington, DC 20006-4046



Labor & Employment Law Solutions | Local Everywhere

This email may contain confidential and privileged material for the sole use of the intended recipient(s). Any review, use, distribution or disclosure by others is strictly prohibited. If you are not the intended recipient (or authorized to receive for the recipient), please contact the sender by reply email and delete all copies of this message.

Littler Mendelson, P.C. is part of the international legal practice Littler Global, which operates worldwide through a number of separate legal entities. Please visit www.littler.com for more information.

March 8, 2019

The Honorable Xavier Becerra
Attorney General of California
Office of the Attorney General
California Department of Justice
300 South Spring Street
Los Angeles, CA 90013

SENT VIA E-MAIL TO PRIVACYREGULATIONS@DOJ.CA.GOV

Re: California Consumer Privacy Act of 2018

Dear Attorney General Becerra:

The Littler Workplace Policy Institute ("WPI") submits these comments in response to the Request for Information by the California Department of Justice, Office of the Attorney General ("Department") regarding Assembly Bill 375, the California Consumer Privacy Act of 2018 ("Act" or "CCPA").

We are writing today on behalf of the employer members of WPI. WPI seeks to impact workplace public policy on behalf of the employer community.

Section 1798.185 of the CCPA empowers the Department to clarify the categories of personal information included within the CCPA that may create "obstacles to implementation." As defined in the Act, "personal information" includes any information that "is capable of being associated with, or could reasonably be linked, directly or indirectly with a particular consumer or household . . ." CCPA §1798.140(o)(1). This extremely broad definition encompasses such a large swath of information that it could be read to include almost any individually identifiable information maintained by an employer about its own employees who are California residents purely for the employer's own internal employment purposes.

As explained below, such a literal reading of the Act would be inconsistent with the legislature's intent to protect consumers in the eCommerce context and would certainly present obstacles to implementation. Accordingly, consistent with §1798.185, WPI urges the Department to issue a regulation clarifying that the CCPA's definition of personal information excludes any personal information maintained by an employer

about its prospective, current, and former employees exclusively in connection with the administration of the employment relationship.¹

A. The text of the statute indicates that the legislature did not intend to include employees' personal information held by employers.

As an initial matter the text of the act itself makes clear that the legislature did not intend to include employee data in the scope of "personal information" protected by the CCPA. Neither the legislative findings nor the Act itself ever uses the word "employer" or "employee"; instead, the findings reference only "consumers" and "businesses." Furthermore, the Act defines "business" by reference to the entity's annual gross revenue; the number of consumers, households or devices about which the entity processes personal information; or the percentage of the entity's annual revenue derived from selling consumers' personal information. *See* Cal. Civ. Code §1798.140(c). By contrast, employment laws almost uniformly define an employer by reference to the number of the entity's employees. *See, e.g.*, 42 U.S.C. §2000e(b) (defining "employer" for purposes of federal anti-discrimination law as an entity with 15 or more employees); Cal. Gov't Code. §12926(d) (defining "employer" for purposes of California anti-discrimination law as an entity with 5 or more employees).

The Act's requirement to notify consumers of their right to opt out of the sale of their personal information, one of the central new rights conferred on consumers, also supports the conclusion that the CCPA is not intended to address personal information collected during the employment relationship. The Act mandates delivery of that notice through the business' publicly facing "Internet webpage." *See* Cal. Civ. Code §1798.135(a)(1), (a)(2) That method of notification would be anomalous in the employment context where mandatory notices to employees customarily are delivered by physically posting them in the workplace, delivering them directly to employees, or including them in an employee handbook. *See, e.g.*, Cal. Lab. Code §247 (requiring that employers "display a poster in a conspicuous place" regarding their sick leave policies); Cal. Code Regs. tit. 2, §11049 (requiring that if an employer maintains an employee handbook, "that employer shall include a description of reasonable accommodation,

¹ WPI notes that this position is consistent with that espoused by several organizations which participated in the public forum. On February 5, 2019, in Sacramento, Sara Boot provided comment for the California Chamber of Commerce and noted that "employees...do not have a true consumer relationship with the business" and were "not really meant to be included within the law in this way in their role as employees." *See* Transcript of Public Hearing, February 5, 2019, Pgs. 16-17, *available at* <https://oag.ca.gov/privacy/ccpa>. Likewise, Pete Isberg of the National Payroll Reporting Consortium noted "[t]here is widespread confusion and inconsistent analyses over whether employment records in the employment context generally are regulated by the CCPA" *Id.* at 30-31. Similar concerns were expressed at the January 8, 2019 meeting by Ellen Langshel, the General Counsel of California Workers Compensation, and by members of Perkins Coie's data privacy group. *See* Transcript of Public Hearing, January 8, 2019, Pgs. 28-29, 33, *available at* <https://oag.ca.gov/privacy/ccpa>.

transfer, and pregnancy disability leave” policies, among other notice requirements). Had the legislature intended for the Act to cover employees, surely it would have included a specific method for notifying employees that would be consistent with the employment context as few employees would be on reasonable notice of a policy implemented by an employer through its public, consumer-facing webpage.

Moreover, the Act’s anti-discrimination provisions also appear to demonstrate the legislature’s intent not to regulate records management in the employment context. That provision prohibits businesses from discriminating against consumers who exercise their rights under the Act by denying service, charging different prices, or providing a lower-quality product. *See* Cal. Civ. Code §1798.125(a)(1). Had the legislature intended the Act to regulate the collection of employees’ personal information during the employment relationship, it almost surely would have prohibited a business from discriminating in the terms or conditions of employment against consumers exercising their rights.

Finally, the Act’s protections expressly extend to consumers under the age of 16, with additional protections for minors under the age of 13. *See* Cal. Civ. Code §1798.120(d). With the exception of child labor laws, few if any laws relating to the employment relationship contain specific provisions addressing minors, especially those under age 13.

B. Applying the CCPA to employees’ personal information would create obstacles to implementation.

In addition to lacking language reflecting a legislative intent to include employees’ personal information within the scope of the CCPA, the Act confers rights on consumers that would be unworkable in the employment context. The Act confers the following new rights on consumers:

- a) the right to access personal information collected by the business, Cal. Civ. Code §1798.100(c);
- b) the right to information about the business’ collection, sale, and other disclosure of the consumer’s personal information collected by the business, Cal. Civ. Code §§1798.100(a), 1798.110(a), 1798.115(a);
- c) the right to request deletion of personal information collected by the business, Cal. Civ. Code §1798.105; and
- d) the right to opt out of the business’ sale of the consumer’s personal information, Cal. Civ. Code §1798.120.

Of these rights, the right to access has the potential to be unreasonably burdensome to employers with regard to employees' personal information. The rights to deletion and to information about collection and disclosure also would carry a significant burden if applied to employees' personal information.

Under the right of access, a business is required, within 45 days of receiving a consumer's verified request, to provide all personal information collected by the business, free of charge, during the twelve months preceding the request. This request could encompass the following categories of an employee's personal information:

- All identifiers related to the employee, including, for example, Social Security number, driver's license number, passport number, and contact information, Cal. Civ. Code §1798.140(o)(1)(A);
- Physical characteristics or description, insurance policy number, education, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information, Cal. Civ. Code §1798.140(o)(1)(B);
- "Biometric information," such as that collected through a biometric time clock, Cal. Civ. Code §1798.140(o)(1)(D);
- "Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement," which would encompass a substantial amount of the information collected by many employers through standard workplace monitoring as well as Internet activity by employees exclusively for their employers' own business purposes (as opposed to the employee's personal eCommerce activity), Cal. Civ. Code § 1798.140(o)(1)(F);
- "Geolocation data," which arguably could include information collected by employers through GPS units in company-owned vehicles as well as location information collected through applications downloaded by field employees to their company-issued mobile devices, Cal. Civ. Code §1798.140(o)(1)(G); and
- "Professional or employment-related information," which effectively would include everything in an employee's personnel file. Cal. Civ. Code § 1798.140(o)(1)(I).

Given the breadth of the Act's definition of "personal information," many employers would be challenged to compile all information falling within the scope of a request.

Further, it is easy to envision a number of circumstances where it would not be reasonable or practicable for an employer to provide an employee access to information, where for example, that information was relevant to an internal investigation or the employee's discipline or is intermingled with highly sensitive information about co-workers, such as records of counseling provided by an on-site health care professional to an employee concerning her supervisor's sexual harassment. The Act does not explicitly provide for any exceptions to the right of access in employment situations, which would leave employers to question whether to comply with the CCPA or withhold the information above. Moreover, if an employer were to attempt to limit some of the rights to access in an employment contract, that contract likely would be void under §1798.192.

Likewise, the right to information about collection and disclosure of personal information requires that a business, in response to a consumer's verified request, provide a report listing all types of personal information collected, the purposes for which the information will be used, the categories of sources for the collection, and any disclosure of that personal information. This right could create similar burdens to the right of access to compile and produce this information for each employee who makes a request. Thus, in the same way that the right to access could be unreasonably burdensome, the right to information about collection and disclosure would also be unreasonably burdensome to employers.

Employees can also ask for their personal information to be deleted. Cal. Civ. Code §1798.105. While the CCPA would permit an employer to not delete information where deletion conflicts with federal law, this exception is not broad enough to cover circumstances that may frequently arise. Cal. Civ. Code §1798.105(d)(8). For example, an employee could potentially ask for his or her browsing history to be deleted after learning of potential discipline stemming from a history of using an employer's electronic resources to view child pornography or other sexually explicit material. In most situations, nothing in the law would require an employer to keep this information, but the employer would likely need the information to maintain records of its discipline and otherwise defend against potential lawsuits. If an employee could ask an employer to delete this information, it could create a tension between an employer's business interests and the rights conferred to individuals under the CCPA.

Taken together, these points demonstrate the CCPA was not intended to confer rights on employees vis-à-vis their employers with respect to personnel records. But, as noted above, the definitions as drafted may lead to confusion and inconsistent application. Accordingly, we request that the Department issue a regulation implementing WPI's recommendation below to clarify that employees' personal information maintained by an employer exclusively for purposes of administering the employment relationship is not subject to the CCPA.

C. Proposed regulation

Because the CCPA so clearly was not intended to apply to employers' own personnel records, the Department could eliminate substantial obstacles to implementation for thousands of California businesses by promulgating a regulation concerning the definition of "personal information" which includes the following sentence:

Personal information excludes any information in the possession, custody or control of an employer concerning a prospective, current or former employee where the employer maintains, uses and discloses that information exclusively for purposes of administering its prospective, current and/or former employment relationship with the employee.

Thank you for the opportunity to respond to the Request for Information and to present WPI's views before you begin a formal rulemaking. We look forward to working with the Department on this important issue.

Respectfully Submitted,



Philip L. Gordon
Co-Chair
Privacy and Background Checks Practice Group
Littler Mendelson, PC
1900 Sixteenth Street
Suite 800
Denver, CO 80202

303.362.8103 fax



Bruce J. Sarchet
Workplace Policy Institute - California
Shareholder
Littler Mendelson, PC
500 Capitol Mall – Suite 2000
Sacramento, CA 95814

916.561.0828 fax

Message

From: Cheryl Berman [REDACTED]
Sent: 3/8/2019 8:39:15 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Privacy Regulation CCPA and Workers' Compensation
Attachments: CCPA (Final) Attny General Comment Letter - Work Comp. (3-6-19) (002) TBC with sign.pdf

Cheryl Berman, CRIS on behalf of Harry Schirer

Risk Manager

TBC LLC/The Brady Companies



This email contains confidential information intended only for the individual or entity named within the message. If the reader of this message is not the intended recipient, or the agent responsible to deliver it to the intended recipient, you are hereby notified that any review, dissemination or copying of this communication is prohibited. If this communication was received in error, please notify us by return email and delete the original message.

This email has been scanned for email related threats and delivered safely by Mimecast.
For more information please visit <http://www.mimecast.com>

March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

VIA US MAIL and EMAIL

TO WHOM IT MAY CONCERN:

The following comments are submitted on behalf of Sharp Rees Stealy, Kaiser Permanente, US Healthworks, One Call and Scripps Health.

**The Attorney General Should Exempt the Workers' Compensation System
From the California Consumer Privacy Act**

The California Consumer Privacy Act (CCPA) directs the Attorney General to adopt regulations to further the purposes of the CCPA, including "...[e]stablishing any exceptions necessary to comply with state or federal law, ... within one year of passage of this title and as needed thereafter."¹

An Exception From CCPA is Necessary to Comply With the California Constitution
and State Laws Governing the Workers' Compensation System

1) The workers' compensation system is established and regulated pursuant to the state Constitution.

The state Constitution confers plenary power on the Legislature to enact a comprehensive worker's compensation system. Section 4 of Article XIV of the state Constitution vests the Legislature with "plenary power, unlimited by any provision of this Constitution, to create, and enforce a complete system of workers' compensation, by appropriate legislation."² This constitutional mandate gives the Legislature "complete, absolute and unqualified power to create and enact the workers' compensation system."³ California courts have interpreted this grant of

¹ Civil Code §1798.185 (a) (3)

² Cal Const. Article XIV, § 4

³ *Facundo-Guerrero v. Workers' Comp. Appeals Bd.* (2008) 163 Cal.App.4th 640, 650 [intent behind Section 4 "was to endow [the Legislature] expressly with exclusive and 'plenary' authority to determine the contours and content of our state's workers' compensation system"].



TBC LLC, 8104 Commercial St. PO Box 1780, La Mesa, CA 91942

broad power to mean that “absolutely nothing” in Section 4 “purports to limit the Legislature's authority to enact additional appropriate legislation for the protection of employees.”⁴

The constitutional grant of power has “compelled the conclusion” that Section 4 of Article XIV of the state Constitution supersedes the state Constitution’s Due Process clause with respect to legislation passed under the Legislature’s plenary powers over the workers’ compensation system.⁵ Courts have held that, even if conflicts existed between Section 4 [workers’ compensation] and other state Constitutional provisions governing Separation of Powers or Due Process, “the plenary powers conferred by Section 4 would still control.”⁶

The courts have unambiguously held that the provisions of the California Constitution governing workers’ compensation are not limited by other provisions of the state Constitution, including the Due Process and Separation of Powers clauses.

These interpretations lead to a likely conclusion that, by its own terms, the constitutional provisions governing workers’ compensation will also control over state constitutional provisions in Section 1 of Article I pertaining to the right to Privacy, so long as the Legislature has employed its “...plenary power, *unlimited by any provision of this Constitution*, to create, and enforce a complete system of workers’ compensation, by appropriate legislation.”⁷

2) Pursuant to its constitutional mandate, the Legislature has enacted a comprehensive workers’ compensation system by statute.

Section 4 of Article XIV of the state Constitution provides in part that “[a] complete system of workers’ compensation includes...full provision for vesting power, authority and jurisdiction in an administrative body with all the requisite governmental functions to determine any dispute or matter arising under such legislation.” The intent behind Section 4 “was to endow [the Legislature] expressly with exclusive and ‘plenary’ authority to determine the contours and content of our state’s workers’ compensation system.”⁸ The only limitations on the Legislature’s plenary powers are that the Legislature cannot act outside of its authority to create and to enforce a complete system of workers’ compensation or enact a provision that conflicts with federal law.⁹ The state Constitution, and the cases interpreting it, confirm that “nearly any exercise of the

⁴ *City and County of San Francisco v. Workers’ Comp. Appeals Bd. (Wiebe)* (1978) 22 Cal.3d 103, 114

⁵ *Hustedt v. Workers’ Comp. Appeals Bd.* (1981) 30 Cal.3d 329, 343 [“It is well established that adoption of [Section 4] ‘effected a repeal pro tanto’ of any state constitutional provisions which conflicted with that amendment”]; see also *Greener v. Workers’ Comp. Appeals Bd.* (1993) 6 Cal.4th 1028 [article VI of the state Constitution governing courts’ jurisdiction inapplicable to extent Legislature has exercised its powers under Section 4]

⁶ *Stevens v. Workers’ Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

⁷ (Emphasis added) Cal Const. Article XIV, § 4

⁸ *Facundo-Guerrero v. Workers’ Comp. Appeals Bd.* (2008) 163 Cal.App.4th 640, 650

⁹ *Hustedt v. Workers’ Comp. Appeals Bd.* (1981) 30 Cal.3d 329; see also, *Stevens v. Workers’ Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

Legislature's plenary powers over workers' compensation is permissible so long as the Legislature finds its action to be 'necessary to the effectiveness of the system of workers' compensation.'¹⁰

Acting under this power, the Legislature enacted the workers' compensation law to govern compensation to California workers who are injured in the course of their employment.¹¹

The underlying premise behind this statutorily created system is the "compensation bargain, [under which] the employer assumes liability for industrial personal injury or death without regard to fault in exchange for limitations on the amount of that liability. The employee is afforded relatively swift and certain payment of benefits to cure or relieve the effects of industrial injury without having to prove fault but, in exchange, gives up the wider range of damages potentially available in tort."¹² The workers' compensation law requires employers to secure the payment of workers' compensation benefits either by purchasing third-party insurance or by self-insuring with permission from the Department of Industrial Relations.¹³

In addition, where the "conditions of compensation" exist, the right to recover such compensation is the "sole and exclusive remedy" of the employee or his or her dependents against the employer when acting within the scope of his or her employment.¹⁴

3) Existing privacy protections in the workers' compensation system

There are several privacy requirements within the Labor Code directly applicable to workers' compensation. Labor Code Section 138.7 provides in part:

"A person or public or private entity not a party to a claim for workers' compensation benefits shall not obtain individually identifiable information obtained or maintained by the division on that claim. For purposes of this section, 'individually identifiable information' means any data concerning an injury or claim that is linked to a uniquely identifiable employee, employer, claims administrator, or any other person or entity."

There are limited exceptions to that rule, but it is unlawful for any person who has received individually identifiable information from the division pursuant to this section to provide that

¹⁰ *Stevens v. Workers' Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

¹¹ Division 4 (commencing with Section 3200) of the Labor Code

¹² *Charles J. Vacanti, M.D., Inc. v. State Comp. Ins. Fund* (2001) 24 Cal.4th 800, 811. See also, *Shoemaker v. Myers* (1990) 52 Cal.3d 1

¹³ Labor Code § 3700

¹⁴ Labor Code § 3602 (a)

information to any person who is not entitled to it.¹⁵ In a similar way, Labor Code Section 3762 (c) states:

“An insurer, third-party administrator retained by a self-insured employer pursuant to Section 3702.1 to administer the employer’s workers’ compensation claims, and those employees and agents specified by a self-insured employer to administer the employer’s workers’ compensation claims, are prohibited from disclosing or causing to be disclosed to an employer, any medical information, as defined in Section 56.05 of the Civil Code, about an employee who has filed a workers’ compensation claim, except as follows: (1) Medical information limited to the diagnosis of the mental or physical condition for which workers’ compensation is claimed and the treatment provided for this condition. (2) Medical information regarding the injury for which workers’ compensation is claimed that is necessary for the employer to have in order for the employer to modify the employee’s work duties.”

Insofar as electronic billing purposes are concerned, Labor Code Section 4603.4 (b) specifies that that billing standards developed by the Division of Workers’ Compensation (DWC), “...shall be consistent with existing standards under the federal Health Insurance Portability and Accountability Act of 1996.”

Labor Code Section 4610.5 (m) states that when a claims administrator is transmitting medical records pursuant to a request for independent medical review, “The confidentiality of medical records shall be maintained pursuant to applicable state and federal laws.” Confidentiality of medical information was also addressed by the Legislature in Labor Code Section 4903.6 (d):

“With the exception of a lien for services provided by a physician as defined in Section 3209.3, a lien claimant shall not be entitled to any medical information, as defined in subdivision (g) of Section 56.05 of the Civil Code, about an injured worker without prior written approval of the appeals board. Any order authorizing disclosure of medical information to a lien claimant other than a physician shall specify the information to be provided to the lien claimant and include a finding that the information is relevant to the proof of the matter for which the information is sought.”

In summary, privacy protections within the Labor Code extensively address protection of medical information.

4) Workers’ Compensation is a comprehensive statutory medical, legal and adjudicatory system that is incompatible with the provisions of the CCPA.

Each day, personal and medical information concerning hundreds of thousands of injured workers is circulated from a Medical Provider Network (MPN) or insurance claims administrator to the physician, to the physician specialist to whom an injured worker may be referred, to the Utilization Review Organization, an Independent Medical Review (IMR) service, an

¹⁵ Labor Code § 138.7

Independent Bill Review (IBR) organization, and Electronic Billing Review organization, Pharmacy Benefit Managers, Vocational Rehabilitation Counselors, Job Training and Supplemental Job Displacement Benefit entities, and more.

Additionally, MPN administrators and self-insured employers are required to report injured workers' medical information to the Office of Self-Insured Plans, Workers' Compensation Information System, Workers' Compensation Appeals Board and the Workers' Compensation Insurance Rating Bureau, all mandatory reporting requirements that would trigger disclosure notifications under the CCPA.

Because an injured worker cannot, and would clearly not wish to frustrate the adjusting of a claim by not allowing information to be disclosed to those who are integral to the workers' compensation medical treatment and benefit payment system, the disclosures nevertheless must be provided to the workers' compensation claimant or applicant. Failure to do so can result in penalties and enforcement actions from the California Department of Justice and the Department of Industrial Relations.

For example, Civil Code § 1798.115(a) of the CCPA states that the consumer has a right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer (1) the categories of personal information that the business collected about the consumer, (2) the categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold, and (3) the categories of personal information that the business disclosed about the consumer for a business purpose.

Section 1798.115(a) would likely apply to nearly all workers' compensation claims transactions. As noted above, medical records are sent to a medical provider network (MPN), medical records are sent to a utilization review organization (URO), and medical records are sent to an independent review organization (IRO). "Personal information" would clearly include payment information sent to a payment processing center falling within the definition of "service provider." A vocational evaluator would clearly need to know "professional or employment-related information" that is included within the definition of "personal information" in Civil Code Sec. 1798.140(o)(1)(I).

During the routine administration of a workers' compensation claim, especially a claim involving indemnity benefits, considerable "personal information," as defined in Civil Code Sec. 1798.140(o), must be collected so that the claim can be processed and the injured worker can be treated and compensated. For physicians and other service providers, an injured worker's personal information is collected during the payment and remittance process. In addition, the placement of insurance, including providing and disclosure claims information, is a vital function in the workers' compensation system.

By law, workers' compensation claimants are considered "consumers" for purposes of the Insurance Information and Privacy Protection Act.¹⁶ Therefore, the notice of information practices required by Insurance Code Sec. 791.04 applies to workers' compensation insurers.

Although these are just a few examples, the fact remains that each and every referral or transmittal cited above would, pursuant to the CCPA, trigger a disclosure notification to the injured worker. The sheer number of notices that would be generated pursuant to the CCPA has, in the case of one large MPN doing business in the state, been estimated to generate nearly 61 million pieces of paper for each 150,000 claims during routine claims processing operations.

Yet, every one of these transactions are already governed by a comprehensive body of *existing state law*. Moreover, because workers' compensation is the sole and exclusive remedy for all injuries and illnesses that occur within the course and scope of employment, the injured employees would not be allowed to opt out of participation as is provided for within the CCPA.

Therefore, although an injured worker cannot prevent the adjusting of a claim by refusing to allow information to be given to workers' compensation service providers, the notification disclosures nevertheless must be sent if the CCPA were to apply. Failure to do so can result in penalties and enforcement actions from the Department of Justice.

5) A regulatory exception from CCPA is needed in order to comply with the comprehensive constitutionally mandated and legislatively enacted workers' compensation system.

The workers' compensation system is a unique body of state law that is breathtaking in its scope and applicability. The workers' compensation system has its own legal and court adjudication system. Medical treatment offered within the workers' compensation system is completely separate and apart from the state's health care delivery system. Nearly every aspect of an injured worker's medical care, vocational rehabilitation, and benefit payments is governed by state law and subject to extensive oversight by the Division of Workers' Compensation within the state Department of Industrial Relations.

This petition for an exception from CCPA in order to comply with state law, as authorized pursuant to Civil Code Section 1798.185 (a) (3), is presented herein on account of the fact that these extremely complex and comprehensive transactions that take place every day concerning the medical treatment and monetary benefits of injured workers in this state are already regulated extensively by an all-inclusive statutory structure.

Importantly, the right to recover compensation and treatment under the workers' compensation system is the sole and exclusive remedy for injury or death of an employee against the employer or co-employee acting within the scope of his or her employment,¹⁷ making participation in the workers' compensation system mandatory for both employers and employees.

¹⁶ Insurance Code § 791 et seq.

¹⁷ See, Labor Code, § 3602 (a)

Thus, we respectfully submit that all aspects of the workers' compensation statutory and constitutional system should be exempted entirely from CCPA. We therefore strongly urge that the Attorney General adopt regulations to establish an exception from the CCPA for the workers' compensation system, as specifically authorized in Civil Code Section 1798.185 (a) (3):

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas: [...]

(3) *Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.*
(Emphasis added)

Workers' compensation is a heavily regulated industry, with an extensive body of statutory and constitutional laws governing it. We strongly believe that exempting workers' compensation from the CCPA is appropriate, and we respectfully urge this action be taken as it is "...*necessary to comply with state law...*"¹⁸

Suggested regulatory language is provided as follows:

Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code does not apply to medical or personal information collected by a business, medical provider network, third party administrator, insurer or other third-party entity for the purpose of providing medical treatment or administering claims pursuant to Division 4 (commencing with Section 3200) of the Labor Code.

Thank you for your consideration.

Sincerely,

A handwritten signature in blue ink, appearing to read "Harry Schirer", is written over a horizontal line.

Harry Schirer
CFO TBC LLC

¹⁸ Civil Code § 1798.185 (a) (3)

Message

From: Janet Massolo [REDACTED]
Sent: 3/8/2019 9:48:43 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: WC Exemption from CCPA
Attachments: 20190308094946842.pdf

Please see attached letter.

Gregg Brady

President

Brady Company/Central California, Inc.

13540 Blackie Road

Castroville, CA 95012



This email has been scanned for email related threats and delivered safely by Mimecast.
For more information please visit <http://www.mimecast.com>



BRADY COMPANY /
CENTRAL CALIFORNIA, INC.

March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

VIA US MAIL and EMAIL

TO WHOM IT MAY CONCERN:

The following comments are submitted on behalf of Kaiser Permanente, Washington Hospital, Santa Clara Valley Medical and Pinnacle Health.

**The Attorney General Should Exempt the Workers' Compensation System
From the California Consumer Privacy Act**

The California Consumer Privacy Act (CCPA) directs the Attorney General to adopt regulations to further the purposes of the CCPA, including "...[e]stablishing any exceptions necessary to comply with state or federal law, ... within one year of passage of this title and as needed thereafter."¹

**An Exception From CCPA is Necessary to Comply With the California Constitution
and State Laws Governing the Workers' Compensation System**

1) The workers' compensation system is established and regulated pursuant to the state Constitution.

The state Constitution confers plenary power on the Legislature to enact a comprehensive worker's compensation system. Section 4 of Article XIV of the state Constitution vests the Legislature with "plenary power, unlimited by any provision of this Constitution, to create, and enforce a complete system of workers' compensation, by appropriate legislation."² This constitutional mandate gives the Legislature "complete, absolute and unqualified power to create and enact the workers' compensation system."³ California courts have interpreted this grant of

¹ Civil Code §1798.185 (a) (3)

² Cal Const. Article XIV, § 4

³ *Facundo-Guerrero v. Workers' Comp. Appeals Bd.* (2008) 163 Cal.App.4th 640, 650 [intent behind Section 4 "was to endow [the Legislature] expressly with exclusive and 'plenary' authority to determine the contours and content of our state's workers' compensation system"].

Brady Companies/Central California, Inc. 13540 Blackie Rd, Castroville, CA 95012

BRADY COMPANY / CENTRAL CALIFORNIA, INC.

13540 Blackie Road • Castroville, CA 95012 • [REDACTED] FAX: 831/633-5913

broad power to mean that “absolutely nothing” in Section 4 “purports to limit the Legislature's authority to enact additional appropriate legislation for the protection of employees.”⁴

The constitutional grant of power has “compelled the conclusion” that Section 4 of Article XIV of the state Constitution supersedes the state Constitution’s Due Process clause with respect to legislation passed under the Legislature's plenary powers over the workers’ compensation system.⁵ Courts have held that, even if conflicts existed between Section 4 [workers’ compensation] and other state Constitutional provisions governing Separation of Powers or Due Process, “the plenary powers conferred by Section 4 would still control.”⁶

The courts have unambiguously held that the provisions of the California Constitution governing workers’ compensation are not limited by other provisions of the state Constitution, including the Due Process and Separation of Powers clauses.

These interpretations lead to a likely conclusion that, by its own terms, the constitutional provisions governing workers’ compensation will also control over state constitutional provisions in Section 1 of Article I pertaining to the right to Privacy, so long as the Legislature has employed its “...plenary power, *unlimited by any provision of this Constitution*, to create, and enforce a complete system of workers’ compensation, by appropriate legislation.”⁷

2) Pursuant to its constitutional mandate, the Legislature has enacted a comprehensive workers’ compensation system by statute.

Section 4 of Article XIV of the state Constitution provides in part that “[a] complete system of workers’ compensation includes...full provision for vesting power, authority and jurisdiction in an administrative body with all the requisite governmental functions to determine any dispute or matter arising under such legislation.” The intent behind Section 4 “was to endow [the Legislature] expressly with exclusive and ‘plenary’ authority to determine the contours and content of our state's workers' compensation system.”⁸ The only limitations on the Legislature’s plenary powers are that the Legislature cannot act outside of its authority to create and to enforce a complete system of workers’ compensation or enact a provision that conflicts with federal law.⁹ The state Constitution, and the cases interpreting it, confirm that “nearly any exercise of the

⁴ *City and County of San Francisco v. Workers' Comp. Appeals Bd. (Wiebe)* (1978) 22 Cal.3d 103, 114

⁵ *Hustedt v. Workers' Comp. Appeals Bd.* (1981) 30 Cal.3d 329, 343 [“It is well established that adoption of [Section 4] ‘effected a repeal pro tanto’ of any state constitutional provisions which conflicted with that amendment”]; see also *Greener v. Workers' Comp. Appeals Bd.* (1993) 6 Cal.4th 1028 [article VI of the state Constitution governing courts' jurisdiction inapplicable to extent Legislature has exercised its powers under Section 4]

⁶ *Stevens v. Workers' Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

⁷ (Emphasis added) Cal Const. Article XIV, § 4

⁸ *Facundo-Guerrero v. Workers' Comp. Appeals Bd.* (2008) 163 Cal.App.4th 640, 650

⁹ *Hustedt v. Workers' Comp. Appeals Bd.* (1981) 30 Cal.3d 329; see also, *Stevens v. Workers' Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

Legislature's plenary powers over workers' compensation is permissible so long as the Legislature finds its action to be 'necessary to the effectiveness of the system of workers' compensation.' ”¹⁰

Acting under this power, the Legislature enacted the workers' compensation law to govern compensation to California workers who are injured in the course of their employment.¹¹

The underlying premise behind this statutorily created system is the “compensation bargain, [under which] the employer assumes liability for industrial personal injury or death without regard to fault in exchange for limitations on the amount of that liability. The employee is afforded relatively swift and certain payment of benefits to cure or relieve the effects of industrial injury without having to prove fault but, in exchange, gives up the wider range of damages potentially available in tort.”¹² The workers' compensation law requires employers to secure the payment of workers' compensation benefits either by purchasing third-party insurance or by self-insuring with permission from the Department of Industrial Relations.¹³

In addition, where the “conditions of compensation” exist, the right to recover such compensation is the “sole and exclusive remedy” of the employee or his or her dependents against the employer when acting within the scope of his or her employment.¹⁴

3) Existing privacy protections in the workers' compensation system

There are several privacy requirements within the Labor Code directly applicable to workers' compensation. Labor Code Section 138.7 provides in part:

“A person or public or private entity not a party to a claim for workers' compensation benefits shall not obtain individually identifiable information obtained or maintained by the division on that claim. For purposes of this section, ‘individually identifiable information’ means any data concerning an injury or claim that is linked to a uniquely identifiable employee, employer, claims administrator, or any other person or entity.”

There are limited exceptions to that rule, but it is unlawful for any person who has received individually identifiable information from the division pursuant to this section to provide that

¹⁰ *Stevens v. Workers' Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

¹¹ Division 4 (commencing with Section 3200) of the Labor Code

¹² *Charles J. Vacanti, M.D., Inc. v. State Comp. Ins. Fund* (2001) 24 Cal.4th 800, 811. See also, *Shoemaker v. Myers* (1990) 52 Cal.3d 1

¹³ Labor Code § 3700

¹⁴ Labor Code § 3602 (a)

information to any person who is not entitled to it.¹⁵ In a similar way, Labor Code Section 3762 (c) states:

“An insurer, third-party administrator retained by a self-insured employer pursuant to Section 3702.1 to administer the employer’s workers’ compensation claims, and those employees and agents specified by a self-insured employer to administer the employer’s workers’ compensation claims, are prohibited from disclosing or causing to be disclosed to an employer, any medical information, as defined in Section 56.05 of the Civil Code, about an employee who has filed a workers’ compensation claim, except as follows: (1) Medical information limited to the diagnosis of the mental or physical condition for which workers’ compensation is claimed and the treatment provided for this condition. (2) Medical information regarding the injury for which workers’ compensation is claimed that is necessary for the employer to have in order for the employer to modify the employee’s work duties.”

Insofar as electronic billing purposes are concerned, Labor Code Section 4603.4 (b) specifies that that billing standards developed by the Division of Workers’ Compensation (DWC), “...shall be consistent with existing standards under the federal Health Insurance Portability and Accountability Act of 1996.”

Labor Code Section 4610.5 (m) states that when a claims administrator is transmitting medical records pursuant to a request for independent medical review, “The confidentiality of medical records shall be maintained pursuant to applicable state and federal laws.” Confidentiality of medical information was also addressed by the Legislature in Labor Code Section 4903.6 (d):

“With the exception of a lien for services provided by a physician as defined in Section 3209.3, a lien claimant shall not be entitled to any medical information, as defined in subdivision (g) of Section 56.05 of the Civil Code, about an injured worker without prior written approval of the appeals board. Any order authorizing disclosure of medical information to a lien claimant other than a physician shall specify the information to be provided to the lien claimant and include a finding that the information is relevant to the proof of the matter for which the information is sought.”

In summary, privacy protections within the Labor Code extensively address protection of medical information.

4) Workers’ Compensation is a comprehensive statutory medical, legal and adjudicatory system that is incompatible with the provisions of the CCPA.

Each day, personal and medical information concerning hundreds of thousands of injured workers is circulated from a Medical Provider Network (MPN) or insurance claims administrator to the physician, to the physician specialist to whom an injured worker may be referred, to the Utilization Review Organization, an Independent Medical Review (IMR) service, an

¹⁵ Labor Code § 138.7

Independent Bill Review (IBR) organization, and Electronic Billing Review organization, Pharmacy Benefit Managers, Vocational Rehabilitation Counselors, Job Training and Supplemental Job Displacement Benefit entities, and more.

Additionally, MPN administrators and self-insured employers are required to report injured workers' medical information to the Office of Self-Insured Plans, Workers' Compensation Information System, Workers' Compensation Appeals Board and the Workers' Compensation Insurance Rating Bureau, all mandatory reporting requirements that would trigger disclosure notifications under the CCPA.

Because an injured worker cannot, and would clearly not wish to frustrate the adjusting of a claim by not allowing information to be disclosed to those who are integral to the workers' compensation medical treatment and benefit payment system, the disclosures nevertheless must be provided to the workers' compensation claimant or applicant. Failure to do so can result in penalties and enforcement actions from the California Department of Justice and the Department of Industrial Relations.

For example, Civil Code § 1798.115(a) of the CCPA states that the consumer has a right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer (1) the categories of personal information that the business collected about the consumer, (2) the categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold, and (3) the categories of personal information that the business disclosed about the consumer for a business purpose.

Section 1798.115(a) would likely apply to nearly all workers' compensation claims transactions. As noted above, medical records are sent to a medical provider network (MPN), medical records are sent to a utilization review organization (URO), and medical records are sent to an independent review organization (IRO). "Personal information" would clearly include payment information sent to a payment processing center falling within the definition of "service provider." A vocational evaluator would clearly need to know "professional or employment-related information" that is included within the definition of "personal information" in Civil Code Sec. 1798.140(o)(1)(I).

During the routine administration of a workers' compensation claim, especially a claim involving indemnity benefits, considerable "personal information," as defined in Civil Code Sec. 1798.140(o), must be collected so that the claim can be processed and the injured worker can be treated and compensated. For physicians and other service providers, an injured worker's personal information is collected during the payment and remittance process. In addition, the placement of insurance, including providing and disclosure claims information, is a vital function in the workers' compensation system.

By law, workers' compensation claimants are considered "consumers" for purposes of the Insurance Information and Privacy Protection Act.¹⁶ Therefore, the notice of information practices required by Insurance Code Sec. 791.04 applies to workers' compensation insurers.

Although these are just a few examples, the fact remains that each and every referral or transmittal cited above would, pursuant to the CCPA, trigger a disclosure notification to the injured worker. The sheer number of notices that would be generated pursuant to the CCPA has, in the case of one large MPN doing business in the state, been estimated to generate nearly 61 million pieces of paper for each 150,000 claims during routine claims processing operations.

Yet, every one of these transactions are already governed by a comprehensive body of *existing state law*. Moreover, because workers' compensation is the sole and exclusive remedy for all injuries and illnesses that occur within the course and scope of employment, the injured employees would not be allowed to opt out of participation as is provided for within the CCPA.

Therefore, although an injured worker cannot prevent the adjusting of a claim by refusing to allow information to be given to workers' compensation service providers, the notification disclosures nevertheless must be sent if the CCPA were to apply. Failure to do so can result in penalties and enforcement actions from the Department of Justice.

5) A regulatory exception from CCPA is needed in order to comply with the comprehensive constitutionally mandated and legislatively enacted workers' compensation system.

The workers' compensation system is a unique body of state law that is breathtaking in its scope and applicability. The workers' compensation system has its own legal and court adjudication system. Medical treatment offered within the workers' compensation system is completely separate and apart from the state's health care delivery system. Nearly every aspect of an injured worker's medical care, vocational rehabilitation, and benefit payments is governed by state law and subject to extensive oversight by the Division of Workers' Compensation within the state Department of Industrial Relations.

This petition for an exception from CCPA in order to comply with state law, as authorized pursuant to Civil Code Section 1798.185 (a) (3), is presented herein on account of the fact that these extremely complex and comprehensive transactions that take place every day concerning the medical treatment and monetary benefits of injured workers in this state are already regulated extensively by an all-inclusive statutory structure.

Importantly, the right to recover compensation and treatment under the workers' compensation system is the sole and exclusive remedy for injury or death of an employee against the employer or co-employee acting within the scope of his or her employment,¹⁷ making participation in the workers' compensation system mandatory for both employers and employees.

¹⁶ Insurance Code § 791 et seq.

¹⁷ See, Labor Code, § 3602 (a)

Thus, we respectfully submit that all aspects of the workers' compensation statutory and constitutional system should be exempted entirely from CCPA. We therefore strongly urge that the Attorney General adopt regulations to establish an exception from the CCPA for the workers' compensation system, as specifically authorized in Civil Code Section 1798.185 (a) (3):

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas: [...]

(3) *Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.* (Emphasis added)

Workers' compensation is a heavily regulated industry, with an extensive body of statutory and constitutional laws governing it. We strongly believe that exempting workers' compensation from the CCPA is appropriate, and we respectfully urge this action be taken as it is "...*necessary to comply with state law...*"¹⁸

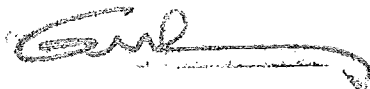
Suggested regulatory language is provided as follows:

Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code does not apply to medical or personal information collected by a business, medical provider network, third party administrator, insurer or other third-party entity for the purpose of providing medical treatment or administering claims pursuant to Division 4 (commencing with Section 3200) of the Labor Code.

Thank you for your consideration.

Sincerely,

Brady Company/Central California, Inc.



Gregg Brady
President

¹⁸ Civil Code § 1798.185 (a) (3)

Message

From: Janet Massolo [REDACTED]
Sent: 3/8/2019 9:01:28 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: WC Exemption from the CCPA
Attachments: 20190308085916153.pdf

Please see attached letter.

Gregg Brady,

President

Brady Company/Central California, Inc.

13540 Blackie Road

Castroville, CA 95012



This email has been scanned for email related threats and delivered safely by Mimecast.
For more information please visit <http://www.mimecast.com>



BRADY COMPANY /
CENTRAL CALIFORNIA, INC.

March 6, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

VIA US MAIL and EMAIL

TO WHOM IT MAY CONCERN:

The following comments are submitted on behalf of (list workers' compensation medical and ancillary service providers here.)

**The Attorney General Should Exempt the Workers' Compensation System
From the California Consumer Privacy Act**

The California Consumer Privacy Act (CCPA) directs the Attorney General to adopt regulations to further the purposes of the CCPA, including "...[e]stablishing any exceptions necessary to comply with state or federal law, ... within one year of passage of this title and as needed thereafter."¹

**An Exception From CCPA is Necessary to Comply With the California Constitution
and State Laws Governing the Workers' Compensation System**

1) The workers' compensation system is established and regulated pursuant to the state Constitution.

The state Constitution confers plenary power on the Legislature to enact a comprehensive worker's compensation system. Section 4 of Article XIV of the state Constitution vests the Legislature with "plenary power, unlimited by any provision of this Constitution, to create, and enforce a complete system of workers' compensation, by appropriate legislation."² This constitutional mandate gives the Legislature "complete, absolute and unqualified power to create and enact the workers' compensation system."³ California courts have interpreted this grant of

¹ Civil Code §1798.185 (a) (3)

² Cal Const. Article XIV, § 4

³ *Facundo-Guerrero v. Workers' Comp. Appeals Bd.* (2008) 163 Cal.App.4th 640, 650 [intent behind Section 4 "was to endow [the Legislature] expressly with exclusive and 'plenary' authority to determine the contours and content of our state's workers' compensation system"].

broad power to mean that “absolutely nothing” in Section 4 “purports to limit the Legislature's authority to enact additional appropriate legislation for the protection of employees.”⁴

The constitutional grant of power has “compelled the conclusion” that Section 4 of Article XIV of the state Constitution supersedes the state Constitution’s Due Process clause with respect to legislation passed under the Legislature's plenary powers over the workers’ compensation system.⁵ Courts have held that, even if conflicts existed between Section 4 [workers’ compensation] and other state Constitutional provisions governing Separation of Powers or Due Process, “the plenary powers conferred by Section 4 would still control.”⁶

The courts have unambiguously held that the provisions of the California Constitution governing workers’ compensation are not limited by other provisions of the state Constitution, including the Due Process and Separation of Powers clauses.

These interpretations lead to a likely conclusion that, by its own terms, the constitutional provisions governing workers’ compensation will also control over state constitutional provisions in Section 1 of Article I pertaining to the right to Privacy, so long as the Legislature has employed its “...plenary power, *unlimited by any provision of this Constitution*, to create, and enforce a complete system of workers’ compensation, by appropriate legislation.”⁷

2) Pursuant to its constitutional mandate, the Legislature has enacted a comprehensive workers’ compensation system by statute.

Section 4 of Article XIV of the state Constitution provides in part that “[a] complete system of workers’ compensation includes...full provision for vesting power, authority and jurisdiction in an administrative body with all the requisite governmental functions to determine any dispute or matter arising under such legislation.” The intent behind Section 4 “was to endow [the Legislature] expressly with exclusive and ‘plenary’ authority to determine the contours and content of our state's workers' compensation system.”⁸ The only limitations on the Legislature’s plenary powers are that the Legislature cannot act outside of its authority to create and to enforce a complete system of workers’ compensation or enact a provision that conflicts with federal law.⁹ The state Constitution, and the cases interpreting it, confirm that “nearly any exercise of the

⁴ *City and County of San Francisco v. Workers' Comp. Appeals Bd. (Wiebe)* (1978) 22 Cal.3d 103, 114

⁵ *Hustedt v. Workers' Comp. Appeals Bd.* (1981) 30 Cal.3d 329, 343 [“It is well established that adoption of [Section 4] ‘effected a repeal pro tanto’ of any state constitutional provisions which conflicted with that amendment”]; see also *Greener v. Workers' Comp. Appeals Bd.* (1993) 6 Cal.4th 1028 [article VI of the state Constitution governing courts' jurisdiction inapplicable to extent Legislature has exercised its powers under Section 4]

⁶ *Stevens v. Workers' Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

⁷ (Emphasis added) Cal Const. Article XIV, § 4

⁸ *Facundo-Guerrero v. Workers' Comp. Appeals Bd.* (2008) 163 Cal.App.4th 640, 650

⁹ *Hustedt v. Workers' Comp. Appeals Bd.* (1981) 30 Cal.3d 329; see also, *Stevens v. Workers' Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

Legislature's plenary powers over workers' compensation is permissible so long as the Legislature finds its action to be 'necessary to the effectiveness of the system of workers' compensation.' ”¹⁰

Acting under this power, the Legislature enacted the workers' compensation law to govern compensation to California workers who are injured in the course of their employment.¹¹

The underlying premise behind this statutorily created system is the “compensation bargain, [under which] the employer assumes liability for industrial personal injury or death without regard to fault in exchange for limitations on the amount of that liability. The employee is afforded relatively swift and certain payment of benefits to cure or relieve the effects of industrial injury without having to prove fault but, in exchange, gives up the wider range of damages potentially available in tort.”¹² The workers' compensation law requires employers to secure the payment of workers' compensation benefits either by purchasing third-party insurance or by self-insuring with permission from the Department of Industrial Relations.¹³

In addition, where the “conditions of compensation” exist, the right to recover such compensation is the “sole and exclusive remedy” of the employee or his or her dependents against the employer when acting within the scope of his or her employment.¹⁴

3) Existing privacy protections in the workers' compensation system

There are several privacy requirements within the Labor Code directly applicable to workers' compensation. Labor Code Section 138.7 provides in part:

“A person or public or private entity not a party to a claim for workers' compensation benefits shall not obtain individually identifiable information obtained or maintained by the division on that claim. For purposes of this section, ‘individually identifiable information’ means any data concerning an injury or claim that is linked to a uniquely identifiable employee, employer, claims administrator, or any other person or entity.”

There are limited exceptions to that rule, but it is unlawful for any person who has received individually identifiable information from the division pursuant to this section to provide that

¹⁰ *Stevens v. Workers' Comp. Appeals Bd.* (2015) 241 Cal.App.4th 1074

¹¹ Division 4 (commencing with Section 3200) of the Labor Code

¹² *Charles J. Vacanti, M.D., Inc. v. State Comp. Ins. Fund* (2001) 24 Cal.4th 800, 811. See also, *Shoemaker v. Myers* (1990) 52 Cal.3d 1

¹³ Labor Code § 3700

¹⁴ Labor Code § 3602 (a)

information to any person who is not entitled to it.¹⁵ In a similar way, Labor Code Section 3762 (c) states:

“An insurer, third-party administrator retained by a self-insured employer pursuant to Section 3702.1 to administer the employer’s workers’ compensation claims, and those employees and agents specified by a self-insured employer to administer the employer’s workers’ compensation claims, are prohibited from disclosing or causing to be disclosed to an employer, any medical information, as defined in Section 56.05 of the Civil Code, about an employee who has filed a workers’ compensation claim, except as follows: (1) Medical information limited to the diagnosis of the mental or physical condition for which workers’ compensation is claimed and the treatment provided for this condition. (2) Medical information regarding the injury for which workers’ compensation is claimed that is necessary for the employer to have in order for the employer to modify the employee’s work duties.”

Insofar as electronic billing purposes are concerned, Labor Code Section 4603.4 (b) specifies that that billing standards developed by the Division of Workers’ Compensation (DWC), “...shall be consistent with existing standards under the federal Health Insurance Portability and Accountability Act of 1996.”

Labor Code Section 4610.5 (m) states that when a claims administrator is transmitting medical records pursuant to a request for independent medical review, “The confidentiality of medical records shall be maintained pursuant to applicable state and federal laws.” Confidentiality of medical information was also addressed by the Legislature in Labor Code Section 4903.6 (d):

“With the exception of a lien for services provided by a physician as defined in Section 3209.3, a lien claimant shall not be entitled to any medical information, as defined in subdivision (g) of Section 56.05 of the Civil Code, about an injured worker without prior written approval of the appeals board. Any order authorizing disclosure of medical information to a lien claimant other than a physician shall specify the information to be provided to the lien claimant and include a finding that the information is relevant to the proof of the matter for which the information is sought.”

In summary, privacy protections within the Labor Code extensively address protection of medical information.

4) Workers’ Compensation is a comprehensive statutory medical, legal and adjudicatory system that is incompatible with the provisions of the CCPA.

Each day, personal and medical information concerning hundreds of thousands of injured workers is circulated from a Medical Provider Network (MPN) or insurance claims administrator to the physician, to the physician specialist to whom an injured worker may be referred, to the Utilization Review Organization, an Independent Medical Review (IMR) service, an

¹⁵ Labor Code § 138.7

Independent Bill Review (IBR) organization, and Electronic Billing Review organization, Pharmacy Benefit Managers, Vocational Rehabilitation Counselors, Job Training and Supplemental Job Displacement Benefit entities, and more.

Additionally, MPN administrators and self-insured employers are required to report injured workers' medical information to the Office of Self-Insured Plans, Workers' Compensation Information System, Workers' Compensation Appeals Board and the Workers' Compensation Insurance Rating Bureau, all mandatory reporting requirements that would trigger disclosure notifications under the CCPA.

Because an injured worker cannot, and would clearly not wish to frustrate the adjusting of a claim by not allowing information to be disclosed to those who are integral to the workers' compensation medical treatment and benefit payment system, the disclosures nevertheless must be provided to the workers' compensation claimant or applicant. Failure to do so can result in penalties and enforcement actions from the California Department of Justice and the Department of Industrial Relations.

For example, Civil Code § 1798.115(a) of the CCPA states that the consumer has a right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer (1) the categories of personal information that the business collected about the consumer, (2) the categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold, and (3) the categories of personal information that the business disclosed about the consumer for a business purpose.

Section 1798.115(a) would likely apply to nearly all workers' compensation claims transactions. As noted above, medical records are sent to a medical provider network (MPN), medical records are sent to a utilization review organization (URO), and medical records are sent to an independent review organization (IRO). "Personal information" would clearly include payment information sent to a payment processing center falling within the definition of "service provider." A vocational evaluator would clearly need to know "professional or employment-related information" that is included within the definition of "personal information" in Civil Code Sec. 1798.140(o)(1)(I).

During the routine administration of a workers' compensation claim, especially a claim involving indemnity benefits, considerable "personal information," as defined in Civil Code Sec. 1798.140(o), must be collected so that the claim can be processed and the injured worker can be treated and compensated. For physicians and other service providers, an injured worker's personal information is collected during the payment and remittance process. In addition, the placement of insurance, including providing and disclosure claims information, is a vital function in the workers' compensation system.

By law, workers' compensation claimants are considered "consumers" for purposes of the Insurance Information and Privacy Protection Act.¹⁶ Therefore, the notice of information practices required by Insurance Code Sec. 791.04 applies to workers' compensation insurers.

Although these are just a few examples, the fact remains that each and every referral or transmittal cited above would, pursuant to the CCPA, trigger a disclosure notification to the injured worker. The sheer number of notices that would be generated pursuant to the CCPA has, in the case of one large MPN doing business in the state, been estimated to generate nearly 61 million pieces of paper for each 150,000 claims during routine claims processing operations.

Yet, every one of these transactions are already governed by a comprehensive body of *existing state law*. Moreover, because workers' compensation is the sole and exclusive remedy for all injuries and illnesses that occur within the course and scope of employment, the injured employees would not be allowed to opt out of participation as is provided for within the CCPA.

Therefore, although an injured worker cannot prevent the adjusting of a claim by refusing to allow information to be given to workers' compensation service providers, the notification disclosures nevertheless must be sent if the CCPA were to apply. Failure to do so can result in penalties and enforcement actions from the Department of Justice.

5) A regulatory exception from CCPA is needed in order to comply with the comprehensive constitutionally mandated and legislatively enacted workers' compensation system.

The workers' compensation system is a unique body of state law that is breathtaking in its scope and applicability. The workers' compensation system has its own legal and court adjudication system. Medical treatment offered within the workers' compensation system is completely separate and apart from the state's health care delivery system. Nearly every aspect of an injured worker's medical care, vocational rehabilitation, and benefit payments is governed by state law and subject to extensive oversight by the Division of Workers' Compensation within the state Department of Industrial Relations.

This petition for an exception from CCPA in order to comply with state law, as authorized pursuant to Civil Code Section 1798.185 (a) (3), is presented herein on account of the fact that these extremely complex and comprehensive transactions that take place every day concerning the medical treatment and monetary benefits of injured workers in this state are already regulated extensively by an all-inclusive statutory structure.

Importantly, the right to recover compensation and treatment under the workers' compensation system is the sole and exclusive remedy for injury or death of an employee against the employer or co-employee acting within the scope of his or her employment,¹⁷ making participation in the workers' compensation system mandatory for both employers and employees.

¹⁶ Insurance Code § 791 et seq.

¹⁷ See, Labor Code, § 3602 (a)

Thus, we respectfully submit that all aspects of the workers' compensation statutory and constitutional system should be exempted entirely from CCPA. We therefore strongly urge that the Attorney General adopt regulations to establish an exception from the CCPA for the workers' compensation system, as specifically authorized in Civil Code Section 1798.185 (a) (3):

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas: [...]

(3) *Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.* (Emphasis added)

Workers' compensation is a heavily regulated industry, with an extensive body of statutory and constitutional laws governing it. We strongly believe that exempting workers' compensation from the CCPA is appropriate, and we respectfully urge this action be taken as it is "...*necessary to comply with state law...*"¹⁸

Suggested regulatory language is provided as follows:

Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code does not apply to medical or personal information collected by a business, medical provider network, third party administrator, insurer or other third-party entity for the purpose of providing medical treatment or administering claims pursuant to Division 4 (commencing with Section 3200) of the Labor Code.

Thank you for your consideration.

Sincerely,

Brady Company/Central California, Inc.



Gregg Brady
President

¹⁸ Civil Code § 1798.185 (a) (3)

Andrew J. Avsec
[REDACTED]

BRINKS
GILSON
& LIONE

March 7, 2019

VIA FEDEX

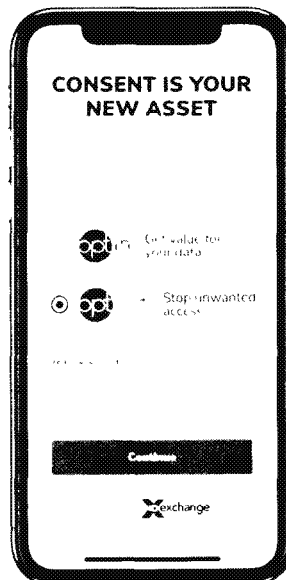
Mr. Xavier Becerra, Esq.
State of California
Office of the Attorney General
1300 I Street
Sacramento, CA 95814-2919

Re: OPT OUT and Design Trademark (U.S. Reg. No. 5,299,154)

Dear Mr. Becerra:

We represent ID Exchange Pty Ltd ("ID Exchange") in trademark matters.

ID Exchange was established in 2012 to develop privacy enhancing technologies (PETs) and digital rights management solutions to assist consumers to protect and mobilize their data for their benefit. Their technologies and represented platforms will provide consumers with the means to control and manage their personal data using methods such as unified instruments of consent management controls, which take the form of OPT IN and OPT OUT logos that represent different software functionality. A representative image is provided below:



A verified Opt Out® request via ID Exchange will instruct the data holder to de-identify the user's Personally Identifiable Information (PII). This notification asks for the deletion of your name, address, email, gender, date of birth, contact number and any other PII data as stipulated under Privacy legislation.

State of California
March 7, 2019
Page 2

Often for this to be accepted by the data holder it must be compliant with data-collection "consent" regulation and the terms of the data holders Privacy Policy to which the user agreed unless the user's jurisdictional law finds the collection was not obtained in an appropriate manner.

ID Exchange is the owner of U.S. Federal Trademark Registration No. 5,299,154 for the trademark OPT OUT and Design trademark depicted below for software related to privacy management.



A copy of the federal Certificate of Registration and the full list of goods and services covered by the registration is provided at Exhibit A.

It recently came to ID Exchange's attention that the California Consumer Privacy Act of 2018 (CCPA) contains a provision requiring the development of a uniform Opt Out logo. Section 1798.185(a)(4)(C) states that the Attorney General shall solicit comments on "[t]he development and use of a recognizable and uniform opt out logo or button by all businesses to promote consumer awareness of the opportunity to opt out of the sale of personal information." ID Exchange is concerned that Section 1798.185(a)(4)(C) may encourage the development of a logo or button that infringes upon its trademark rights in its Opt Out mark.

ID Exchange's solution is complementary to government efforts to protect privacy. Indeed, ID Exchange is engaged with the Australian Federal government and corresponding regulator as a stakeholder and working group participant due to the forming of the new Consumer Data Right Bill (CDR) which was recently submitted to Parliament and now before the Senate, to deliver technologies aligned to emerging policy, privacy and data sharing legislation.

ID Exchange is greatly encouraged that the technology, intellectual property, and policy that ID Exchange has been developing over several years may be used to help and possibly accelerate the achievement of the CCPA's legislative objectives to the benefit of all Californians. ID Exchange is hoping to open a dialog on how its investment, knowledge and IP assets may be of benefit to assisting or collaborating with others pertaining to the rollout of such legislation.

Please contact me at your earliest convenience to discuss.

Sincerely,

A handwritten signature in black ink, appearing to read "Andrew J. Avsec", is written over a horizontal line.

Andrew J. Avsec
Enclosures

cc: California Department of Justice, ATTN: Privacy Regulations Coordinator,
(Via Email privacyregulations@doj.ca.gov)

EXHIBIT A

United States of America

United States Patent and Trademark Office



Reg. No. 5,299,154

Registered Oct. 03, 2017

Int. Cl.: 9, 42, 45

Service Mark

Trademark

Principal Register

Cloud Insurance Pty Ltd (AUSTRALIA proprietary limited company (p/l or pty. ltd.))
Level 2, 50 Bridge Street
Stone&chalk Fintech Incubator-amp Centre
Sydney, AUSTRALIA NSW2000

CLASS 9: Computer application software for computers, tablet computers, hand held computers, portable media players, and mobile devices, namely, data synchronization software, security software, password management and protection software, biometric identification, matching and authentication software, automatic notification software, data access permissions, revocations, and notifications software, database maintenance software, information storage compliance software, trust assessment software, data scrubbing and de-identification software for protection and control of users' information; Computer software for computers, tablet computers, hand held computers, portable media players, medical and mobile devices, namely, data synchronization software, security software, password management and protection software, biometric identification, matching and authentication software, automatic notification software, data access permissions, revocations, and notification software, electronic consent receipts software, database maintenance software, information storage compliance software, trust assessment software, data scrubbing software, data risk automation software for protection and control of users' information

CLASS 42: Software as a service (SAAS) services featuring software for data synchronization, security, password management and protection, biometric identification, credential matching and authentication, email account scanning, assessment of data holders to inform identity verification, authentication, and validation processes; Software as a service (SAAS) services featuring software for providing an authorized e-proxy scheme, namely, an e-proxy scheme to determine data holder access to information; Software as a service (SAAS) services featuring software for providing searching of target data holders, selection of target data holders, data access permissions, revocations and notifications, storage and maintenance of information in databases and document management systems, assuring compliance with legislation and regulations applying to personal information, data scrubbing and de-identification; Providing temporary use of a web-based software application for data synchronization, security, password management and protection, biometric identification, matching and authentication, email account scanning, assessment of data holders to inform identity verification, authentication, and validation processes, authorized e-proxy scheme to determine data holder access to information, searching of target data holders, selection of target data holders, data access permissions, revocations and notifications, storage, consent receipts and maintenance of information in databases and document management systems, assuring compliance with legislation and regulations applying to personal information, data scrubbing; Computer software design; Computer software development

CLASS 45: Identification verification services, namely, providing authentication of personal



Joseph Matol

Performing the Functions and Duties of the
Under Secretary of Commerce for
Intellectual Property and Director of the
United States Patent and Trademark Office

identification information; Digital identity access rights management for protecting data and information from unauthorized access; Personal information access rights management for protecting data and information from unauthorized access; Online privacy management, namely, authentication, assurance, validation, and revocation of digital certificates and consent receipts providing user authentication services in bilateral e-commerce transactions, open data flows, data synchronization, security, password management and protection, biometric identification, matching, and authentication

The color(s) blue and white are claimed as a feature of the mark.

PRIORITY CLAIMED UNDER SEC. 44(D) ON AUSTRALIA APPLICATION NO. 1765066, FILED 04-15-2016, REG. NO. 1765066, DATED 11-10-2016, EXPIRES 04-15-2026

The mark consists of the word "optout" and a blue circle around the letters "opt" written in white followed by the letter "out" written in blue.

SER. NO. 87-074,976, FILED 06-17-2016

REQUIREMENTS TO MAINTAIN YOUR FEDERAL TRADEMARK REGISTRATION

WARNING: YOUR REGISTRATION WILL BE CANCELLED IF YOU DO NOT FILE THE DOCUMENTS BELOW DURING THE SPECIFIED TIME PERIODS.

Requirements in the First Ten Years*

What and When to File:

- **First Filing Deadline:** You must file a Declaration of Use (or Excusable Nonuse) between the 5th and 6th years after the registration date. See 15 U.S.C. §§1058, 1141k. If the declaration is accepted, the registration will continue in force for the remainder of the ten-year period, calculated from the registration date, unless cancelled by an order of the Commissioner for Trademarks or a federal court.
- **Second Filing Deadline:** You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between the 9th and 10th years after the registration date.* See 15 U.S.C. §1059.

Requirements in Successive Ten-Year Periods*

What and When to File:

- You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between every 9th and 10th-year period, calculated from the registration date.*

Grace Period Filings*

The above documents will be accepted as timely if filed within six months after the deadlines listed above with the payment of an additional fee.

***ATTENTION MADRID PROTOCOL REGISTRANTS:** The holder of an international registration with an extension of protection to the United States under the Madrid Protocol must timely file the Declarations of Use (or Excusable Nonuse) referenced above directly with the United States Patent and Trademark Office (USPTO). The time periods for filing are based on the U.S. registration date (not the international registration date). The deadlines and grace periods for the Declarations of Use (or Excusable Nonuse) are identical to those for nationally issued registrations. See 15 U.S.C. §§1058, 1141k. However, owners of international registrations do not file renewal applications at the USPTO. Instead, the holder must file a renewal of the underlying international registration at the International Bureau of the World Intellectual Property Organization, under Article 7 of the Madrid Protocol, before the expiration of each ten-year term of protection, calculated from the date of the international registration. See 15 U.S.C. §1141j. For more information and renewal forms for the international registration, see <http://www.wipo.int/madrid/en/>.

NOTE: Fees and requirements for maintaining registrations are subject to change. Please check the USPTO website for further information. With the exception of renewal applications for registered extensions of protection, you can file the registration maintenance documents referenced above online at <http://www.uspto.gov>.

NOTE: A courtesy e-mail reminder of USPTO maintenance filing deadlines will be sent to trademark owners/holders who authorize e-mail communication and maintain a current e-mail address with the USPTO. To ensure that e-mail is authorized and your address is current, please use the Trademark Electronic Application System (TEAS) Correspondence Address and Change of Owner Address Forms available at <http://www.uspto.gov>.

realEX

Ex

224

Page 1 of 1

ORIGIN ID CHIA (312) 321-4200
ANDREW AVSEC
BRINKS GILSON & LIONE
455 NORTH CITYFRONT PLAZA DRIVE
NBC TOWER, SUITE 3600
CHICAGO, IL 60611
UNITED STATES US

SHIP DATE 07MAR19
ACTWGT 0.50 LB
CAD 112085477WSX13200

BILL SENDER

TO **XAVIER BECCERRA**
OFFICE OF THE ATTORNEY GENERAL
1300 I ST

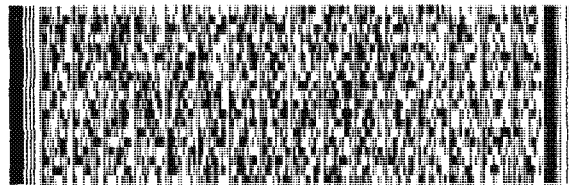
SACRAMENTO CA 95814

(312) 840-3260

REF 15933 00006 01043

INV
PO

DEPT



FedEx
Express



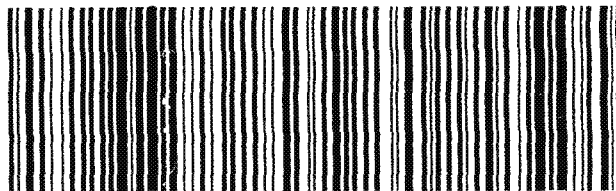
REL#
3785346

FRI - 08 MAR 10:30A
PRIORITY OVERNIGHT

TRK#
0201 7859 0214 0790

XH BLUA

95814
CA-US SMF



PS|Ship - FedEx Label

◀ Insert shipping
document here

Message

From: Robert Rutkowski [REDACTED]
Sent: 3/19/2019 3:19:36 PM
To: PIUWebform [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=PIUWebform0e5]
Subject: [WEB FORM] GENERAL COMMENT OR QUESTION

Below is the result of the feedback form.
It was submitted by [REDACTED]

===== DOJ USE ONLY =====
NEW_TYPE:
===== DOJ USE ONLY =====

TYPE: PL
First Name: Robert
Middle Initial:
Last Name: Rutkowski
[REDACTED]

Comment Or Question Message: Attorney General Xavier Becerra
Attorney General's Office
California Department of Justice
Attn: Public Inquiry Unit
P.O. Box 944255
Sacramento, CA 94244-2550
<https://oag.ca.gov/contact/general-comment-question-or-complaint-form>

Re: Comment on CCPA regulations

Dear Attorney General:

The California Consumer Privacy Act (CCPA) requires the California Attorney General to take input from the public on regulations to implement the law, which does not go into effect until 2020.

The Electronic Frontier Foundation has filed comments on two issues: first, how to verify consumer requests to companies for access to personal information, and for deletion of that information; and second, how to make the process of opting out of the sale of data easy, using the framework already in place for the Do Not Track (DNT) system.

Verification of Requests

When it comes to verifying requests that users make of businesses to access their own data, carefully balance the interest of the consumer in obtaining their own personal information without undue delay or difficulty, with their interest in avoiding theft of their private data by people who might make fraudulent CCPA requests for data.

If a consumer already has a password-protected account, mandate use of that password to verify the account. Further, the business must ensure that the requester really knows the password, and didn't just steal a laptop with an open app, by requiring the requester to log out of the account and present the password again. Also encourage, but not require, two-factor authentication as a form of verification in cases where doing so poses no risk to the user.

If a consumer does not have a password, the company must be as certain as is reasonably possible that the requester is the subject of the personal information being requested.

Opting out of Sales

I also encourage you rely on the existing Do Not Track (DNT) system when issuing rules about consumer requests to opt-out of data sales. The DNT system combines a technology (a browsing header that announces

the user prefers not to be tracked online) with a policy framework (how companies should respond to that signal).

The DNT header is already widely supported by most major web browsers, including Google Chrome, Mozilla Firefox, and Opera. EFF proposes that the Attorney General require any business that interacts with consumers directly over the Internet to treat a browser's DNT request as a request to opt-out of data collection.

Yours sincerely,
Robert E. Rutkowski

cc:
Representative Steny Hoyer
House Majority Leader
Legislative Correspondence Team
1705 Longworth House Office Building
Washington DC 20515
[REDACTED]
Fax: (202) 225-4300
<https://www.majorityleader.gov/content/email-whip>

[REDACTED]

Re: EFF's comments: <https://www.eff.org/document/eff-consumer-data-privacy-comment-california-attorney-general>

Affirm Information Accurate: Yes

[REDACTED]

Referrer: <https://oag.ca.gov/consumers>

[End of comment or complaint information]