

Message

From: Saul Bercovitch [REDACTED]
Sent: 12/7/2019 12:37:45 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Proposed CCPA Regulations - Comments of the California Lawyers Association Privacy Working Group
Attachments: CCPA_proposed_regulations_CLA_privacy_working_group_comments.pdf

I've attached comments of the California Lawyers Association Privacy Working Group on the proposed CCPA regulations.

Saul Bercovitch | Director of Governmental Affairs

California Lawyers Association

[400 Capitol Mall, Suite 650 | Sacramento, CA 95814](#)

O: [REDACTED] [REDACTED]



December 6, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
Email: PrivacyRegulations@doj.ca.gov

Re: Proposed California Consumer Privacy Act Regulations

Dear Attorney General Becerra:

The California Lawyers Association (“CLA”) Privacy Working Group (“PWG”) respectfully submits these comments on the proposed California Consumer Privacy Act (“CCPA”) regulations. The PWG is a multidisciplinary group with members drawn from various sections of the California Lawyers Association, including: Antitrust, UCL and Privacy; Business Law; and Intellectual Property Law. Our members have broad-ranging expertise in areas that include consumer privacy, cybersecurity, and data protection, and extensive experience with related regulatory, transactional, and litigation matters.

The Attorney General released these proposed regulations for public comment on October 10, 2019. The regulations are intended to operationalize the CCPA and provide clarity and specificity to assist in the implementation of the law. The CCPA requires the Attorney General to adopt initial regulations on or before July 1, 2020.

The PWG applauds the Office of the Attorney General for engaging in a broad and inclusive rulemaking process, including public forums. This public comment period is important because the stakes are high. According to estimates in the Standardized Regulatory Impact Assessment for the CCPA regulations, published by the Berkeley Economic Advising and Research, LLC, the CCPA will protect over \$12 billion worth of personal information that is used for advertising in California each year. If finalized, businesses are estimated to spend between \$467 million to \$16,454 million in costs to comply with the draft regulation during the period 2020-2030. The CCPA grants new rights to consumers and imposes new obligations on businesses.

As highlighted in the CCPA Fact Sheet, published together with the proposed regulations, the CCPA and the European Union's General Data Protection Regulation ("GDPR") are separate legal frameworks with different scopes, definitions, and requirements. A business that is subject to GDPR and also processes personal information of California consumers will need to reconcile the differences between the two regimes. In addition, a business will need to examine what additional obligations apply under the CCPA that are outside of how personal information is collected, processed, sold or disclosed pursuant to the federal Gramm-Leach-Bliley Act, the California Financial Information Privacy Act, the Driver's Privacy Protection Act of 1994, the Confidentiality of Medical Information Act, the Health Insurance Portability and Accountability Act of 1996 and the Federal Policy for the Protection of Human Subjects.

We submit the following comments on the proposed regulations.

All views expressed in these comments are our own as individual members of the PWG and do not represent the views of any entity whatsoever with which we have been, are now, or will be affiliated.

Overall Concerns:

The PWG notes that the proposed regulations will not be final before the January 1, 2020 effective date of the CCPA. Once the regulations are final, it will likely take most businesses several months to fully implement processes consistent with the final regulations. Accordingly, we urge the Office of the Attorney General to take into consideration the practical impact these regulations will have on businesses as well as the desire to protect consumer rights.

Our comments below are organized by section. We underlined for ease of reading new or amended language and we struck out language we propose to have deleted (i.e., underline or ~~strike-out~~).

Article 2. Notices to Consumers

§ 999.305. Notice at Collection of Personal Information

Section 999.305(a)(2)(d) provides that a notice at collection of personal information shall: “Be accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.” This same language exists in § 999.306(a)(2)(d) (Notice of Right to Opt-Out of Sale of Personal Information), § 999.307(a)(2)(d) (Notice of Financial Incentive), and § 999.308(a)(2)(d) (Privacy Policy).

The PWG is concerned that “accessible” in the first sentence is unclear, ambiguous, and undefined. This could result in regulatory enforcement issues as well as prolonged litigation regarding interpretation and applicability, similar to other litigation we have already seen concerning website accessibility. In order to address this concern, the PWG suggests that the phrase “accessible to consumers with disabilities” be tied to the requirements of other specific provisions of law and recommends revising § 999.305(a)(2)(d) to read as follows:

§ 999.305(a)(2)(d)

Be accessible to consumers with disabilities to the extent required by the Americans with Disabilities Act, the Unruh Civil Rights Act, the California Disabled Persons Act, or any applicable regulations. At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.

We recommend that this same amendment be made to § 999.306(a)(2)(d), § 999.307(a)(2)(d), and § 999.308(a)(2)(d).

Section § 999.305(a)(3) appears to create an opt-in and consent requirement. The PWG is concerned that a new opt-in requirement not already part of CCPA will potentially lead to “click fatigue” in which consumers ignore notices because of their ubiquity. We think a better approach may be to limit the use of personal information to the purposes that were included in the notice at the time of collection or uses that are within the reasonable expectation of the consumer. We understand that the existing text of the CCPA already allows for exceptions that permit use of personal information for other purposes, as enumerated in Civil Code § 1798.145(a), including: (1) to comply with federal, state or local laws; (2) to comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities; (3) to 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 laws; (4) to exercise or defend legal claims; and (5) to collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information. As such, uses required by law or in furtherance of legal processes, such as serving subpoenas, providing required warranty or recall notices, providing notice of pending class actions, etc. would be permitted even if the notice at collection did not adequately cover these use cases. We recommend revising § 999.305(a)(3) to read as follows:

§ 999.305(a)(3)

A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection, required by law, or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business, or within a lawful manner that is compatible with the context in which the consumer provided the information. ~~If the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall use and obtain explicit consent from the consumer to use it for this new purpose.~~

Section § 999.305(b)(4) appears to require a link to a privacy policy in the notice at collection, implying the privacy policy must be a set of text that is separate from the notice at collection. The PWG suggests that if a privacy policy is provided at or before the time of collection, then a separate notice would not be required. We recommend revising § 999.305(b) to read as follows:

§ 999.305(b)

A business may 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 by providing a link to the privacy policy at or before the point of collection, or in the case of offline notices, the web address of the business's privacy policy, by URL, QR code, or similar means. If the privacy policy or a link to the privacy policy cannot be provided at or before the time of collection, a business shall provide a separate notice at collection which includes:

- (1) A list of the categories of personal information about consumers to be collected. Each category of personal information shall be written in a manner that provides consumers a meaningful understanding of the information being collected.
- (2) For each category of personal information, the business or commercial purpose(s) for which it will be used.

(3) If the business sells personal information, the link titled “Do Not Sell My Personal Information” or “Do Not Sell My Info” required by section 999.315(a), or in the case of offline notices, the web address for the webpage to which it links.

~~(4) A link to the business’s privacy policy, or in the case of offline notices, the web address of the business’s privacy policy.~~

Similar to the change noted above, we recommend revising § 999.305(a)(2)(e) as follows, to allow for other means to link to privacy policies than web addresses, such as QR codes or shortened URLs such as bit.ly:

§ 999.305(a)(2)(e)

Be visible or accessible where consumers will see it in reasonable proximity to where any personal information is collected. At a minimum, the notice may consist of a link to the portion of the privacy policy that describes the categories of information collected and the purposes of collection, though a business may also choose to provide a separate notice, so long as the notice complies with this section. For example, when a business collects consumers’ personal information online, it may conspicuously post a link to the notice on the business’s website homepage or the mobile application’s download page, or on all webpages where personal information is collected. When a business collects consumers’ personal information offline, it may, for example, include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post signage directing consumers to the web address where the notice can be found, by URL, QR code, or similar means.

§ 999.306. Notice of Right to Opt-Out of Sale of Personal Information

Similar to our comment for § 999.305, we recommend allowing businesses to provide the notice of right to opt-out as part of their privacy policy. We recommend revising § 999.306(b) to read as follows:

§ 999.306(b)(1)

A business may inform consumers as to the right to opt-out of sale of personal information by providing a link to the privacy policy, or in the case of offline notices, the web address of the business’s privacy policy, by URL, QR code, or similar means. If the privacy policy or a link to the privacy policy cannot be provided, a business shall provide a separate notice of right to opt-out. A business shall post the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the “Do Not Sell My Personal Information” or “Do Not Sell

My Info” link on the website homepage or the download or landing page of a mobile application.—The Notice shall include the information specified in subsection (c) or link to the section of the business’s privacy policy that contains the same information. For example, one of the acceptable methods to provide the notice of right to opt-out would be for the business to provide the “Do Not Sell My Personal Information” or “Do Not Sell My Info” link on the website homepage or the download, settings or landing page of a mobile application and direct the consumer to the section of the business’s privacy policy that contains the information in subsection (c). Using pop-up or pop-over windows or check boxes may also be acceptable and appropriate means for informing consumers as to the right to opt-out.

We also recommend removing § 999.306(c)(5) so it is clear to the businesses that if a link to the privacy policy was provided, a separate notice of right to opt-out is not necessary.

We encourage the Office of the Attorney General to consider other permissible means of presenting the opt-out notice in § 999.306(b)(2), particularly for offline notices, such as providing the web address to the privacy policy or using QR codes which link to the privacy policy.

Article 3. Business Practices for Handling Consumer Requests

§ 999.312. Methods for Submitting Requests to Know and Requests to Delete

The proposed regulations in § 999.312(a) set forth the requirements for businesses to provide two or more designated methods through which consumers may submit requests to know. We ask the Office of the Attorney General to consider the legislative changes under AB 1564 (Stats. 2019, ch. 759), which clarify this toll-free number requirement and would require a business which “operates exclusively online and has a direct relationship with a consumer” to only provide an email address for submitting access requests.

We recommend revising § 999.312(a) to read as follows, adding this clarification to make the draft regulations consistent with the CCPA:

§ 999.312(a)

A business shall provide two or more designated methods for submitting requests to know including, at a minimum, a toll-free telephone number, and, if the business operates a website, an interactive webform accessible through the business's website or mobile application. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.

We also recommend revising the proposed example (1) in § 999.312(c)(1) to clarify that if a business is primarily an online retailer but also has certain products or services that are provided to consumers at brick-and-mortar retail stores, the consumer may submit requests through the email address that is provided on the business's retail website.

In Example 2, the PWG proposes revising the requirement so that the businesses can consider the methods by which they interact with consumers but the number of designated methods the retail businesses must provide is no more than the two that are required for other industries to avoid any confusion on the minimum requirement.

As such, our recommended revision to § 999.312(c) reads as follows:

§ 999.312(c)

A business shall consider the methods by which it interacts with consumers when determining which methods to provide for submitting requests to know and requests to delete. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer, even if it requires a business to offer three methods for submitting requests to know. Illustrative examples follow:

(1) Example 1: If the business is primarily an online retailer, businesses can provide an email address on their retail website through which consumers can submit requests to know or requests to delete. ~~at least one method by which the consumer may submit requests should be through the business's retail website.~~

(2) Example 2: If the business operates a website but primarily interacts with customers in person at a retail location, the business may ~~shall~~ offer three methods to submit requests to know ~~consumers the following designated methods for submitting requests to know or requests to delete:~~ a toll-free telephone number, an interactive webform accessible through the

business's website, and or a form that can be submitted in person at the retail location.

We understand that the intent of § 999.312(d) may be to allow for instances where a consumer may have submitted the deletion request by mistake, especially in an electronic setting where accidents may occur at the click of a button. However, we do not believe this is a significant issue as deletion requests under the CCPA already require a process for verifying the identity of the consumer. As such, we recommend revising § 999.312(d) to indicate that the businesses can apply discretion in asking the consumers if they indeed meant to submit such deletion request but it is not a requirement. Our suggested language for § 999.312(d) reads as follows:

§ 999.312(d)

A business may ~~shall~~ use a two-step for online requests to delete where the consumer must first, clearly submit the request to delete and then second, separately confirm that they want their personal information deleted.

The PWG suggests removing proposed §999.312(f) because it is overly burdensome and unworkable as drafted. If a business has 10,000 employees, we cannot expect all 10,000 employees to be trained to handle privacy-related inquiries. Especially given that the draft regulations require a response from the business within certain number of days after receiving such requests, we ask that the regulations do not add this new requirement and keep the requirement intact as it is written in the CCPA, which is for the businesses to respond to requests that are submitted through the designated methods. In the alternative, we would propose at a minimum that the requirement is amended to read as follows:

§ 999.312(f)

If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall, to the extent feasible, either:

- (1) Treat the request as if it had been submitted in accordance with the business's designated manner, or
- (2) Provide the consumer with specific directions on how to submit the request or remedy any deficiencies with the request, if applicable.

§ 999.313. Responding to Requests to Know and Requests to Delete

Section 999.313(c)(7) allows a business that maintains a password-protected account with the consumer to comply with a request to know by utilizing a secure self-service portal for consumers to access, view, and receive a portable copy of their personal

information. The PWG proposes the below changes to make clear that the business which uses such a portal may direct the consumer to the portal for submission and processing of a consumer request.

The PWG suggests revising § 999.313(c)(7) to read as follows:

§ 999.313(c)(7)

If a business maintains a password-protected account with the consumer, it may comply with a request to know by using directing the consumer to a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 4.

Section 999.313(d)(1) requires businesses to treat a failed deletion request as an opt-out request. The CCPA treats the right to opt-out and the right to delete as two separate rights. We do not recommend conflating the two and instead recommend clarifying that if the business is unable to verify the identity of the requestor for the deletion request, the requestor must be informed how she may rectify the issue and allow an opportunity to complete verification. The PWG recommends revising § 999.313(d)(1) to read as follows:

§ 999.313(d)(1)

For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified, and shall instead treat the request as a request to opt-out of sale the information needed for verification, and allow the requestor to provide additional information to complete verification.

We understand the intent behind the proposed regulations in § 999.313(d)(3) may be to provide the businesses the flexibility to not have to search through and delete personal information from archived or backup systems if the information is not in use currently. We recommend revising the language in § 999.313(d)(3) to clarify that the requests to delete do not apply to information on archived or backup systems but if the information were accessed or used by the business, the deletion request would apply to that information. Our recommended version reads as follows:

§ 999.313(d)(3)

~~If a business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system is~~

~~next accessed or used.~~ The consumers' request to delete shall not apply to any personal information on archived or backup systems, as long as that information is not accessed or used by the business.

§ 999.315. Requests to Opt-Out

The CCPA already contains a provision which restricts the resale of personal information (see Civil Code § 1798.115(d)). We suggest removing § 999.315(f), as any third parties to whom the personal information is sold would already be restricted from reselling the personal information unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out. The proposed requirement to look back 90 days in § 999.315(f) is unnecessary and unduly burdensome.

§ 999.317. Training: Record-Keeping

In § 999.317(b), there is no clear indication of when the 24 month clock starts (i.e., from the date the business receives the request, responds to the request, etc.). The PWG recommends the Attorney General clarify when the 24 months record-keeping requirement begins. Recommended version of § 999.317(b) reads as follows:

§ 999.317(b)

A business shall maintain records of consumer requests made pursuant to the CCPA and how the business responded to said requests for at least 24 months from the date the consumer submitted any such request.

The PWG proposes a minor change to § 999.317(f) in order to provide clarity as to what record-keeping purpose it pertains. We recommend revising § 999.317(f) to read as follows:

§ 999.317(f)

Aside from this the record-keeping purpose referred to in subsection (e), a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.

Article 4. Verification of Requests

§ 999.325. Verification for Non-Accountholders

The PWG recommends adding language to § 999.325(c) to allow for electronic signatures, as follows:

§ 999.325(c)

A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. A signed declaration may be physically signed or electronically signed. Businesses shall maintain all signed declarations as part of their record-keeping obligations.

Article 5. Special Rules Regarding Minors

§ 999.330. Minors Under 13 Years of Age

The PWG recommends adding language to § 999.330.(a)(2)(a) to allow for additional electronic methods for businesses to verify user identities. Recommended changes to § 999.330(a)(2)(a) reads as follows:

§ 999.330(a)(2)(a)

Providing a consent form to be signed physically or electronically by the parent or guardian under penalty of perjury and returned to the business by postal mail, electronic mail, electronic form, facsimile, or electronic scan;

We thank you for your consideration of these comments.

Members of the Privacy Working Group that prepared these comments are identified below. Affiliations are provided for identification purposes only.

Stanton Burke, Member of the California Lawyers Association

Christopher James Donewald, Member of the California Lawyers Association

Aigerim Dyussenova, Member of the California Young Lawyers Association

Jennifer S. Elkayam, Member of the Antitrust, Unfair Competition, and Privacy Law Section of the California Lawyers Association

Jared Gordon, Past co-chair of the Internet and Privacy Law Committee of the Business Law Section of the California Lawyers Association

Christian Hammerl, Past co-chair of the Internet and Privacy Law Committee of the Business Law Section of the California Lawyers Association

Thomas A. Hassing, Chair of the Internet and Privacy Law Committee of the Business Law Section of the California Lawyers Association

Irene Jan, Member of the Intellectual Property Law Section of the California Lawyers Association

Minji Kim, Member of the Antitrust, UCL and Privacy Section of the California Lawyers Association

Joshua de Larios-Heiman, Executive Committee Member of the Antitrust, UCL and Privacy Section of the California Lawyers Association

Marina A. Lewis, Member of the California Lawyers Association

Gayatri Raghunandan, Member of the California Lawyers Association

Mary Stone Ross, Executive Committee Member of the Antitrust, UCL and Privacy Section of the California Lawyers Association

Perry L. Segal, Board Representative, Law Practice Management and Technology
Section of the California Lawyers Association

Jeewon Kim Serrato, Executive Committee Member of the Antitrust, UCL and Privacy
Section of California Lawyers Association

Kieran de Terra, Executive Committee Member of the Intellectual Property Law Section
of the California Lawyers Association

Emily S. Yu, Secretary of the Intellectual Property Law Section of the California Lawyers
Association and Chair of the Technology, Internet and Privacy Interest Group

Message

From: Donnelly, Kristina [REDACTED]
Sent: 12/6/2019 10:51:35 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Ungson, Chris [REDACTED]; Johnson, Ana Maria [REDACTED]; Lyser, Shelly [REDACTED]; Fisher, Emily [REDACTED]
Subject: Public Advocates Office Comments on CCPA Draft Regulations
Attachments: PUBADV CCPA Comments_2019-12-06.pdf

Hello,

On behalf of the Public Advocates Office at the California Public Utilities Commission, please find attached comments on the draft regulations implementing the California Consumer Privacy Act. Thank you for the opportunity to comment and please don't hesitate to get in touch if you have any questions.

Best,
Kristina Donnelly

Kristina Donnelly
Regulatory Analyst
Public Advocates Office
California Public Utilities Commission
[REDACTED]
[REDACTED]



Public Advocates Office

California Public Utilities Commission

505 Van Ness Avenue

San Francisco, California 94102

Tel: 415-703-1584

<http://www.publicadvocates.cpuc.ca.gov/>

December 6, 2019

California Office of the Attorney General
Attn: Privacy Regulations Coordinator
300 South Spring Street, First Floor
Los Angeles, CA 90013

Subject: Public Advocates Office Comments on the Draft Regulations Implementing the 2018 California Consumer Privacy Act

INTRODUCTION

The Public Advocates Office at the California Public Utilities Commission (Public Advocates Office) appreciates the opportunity to submit these comments on the California Consumer Privacy Act (CCPA) draft regulations published by the California Department of Justice on October 11, 2019.¹

The Public Advocates Office is a legislatively created independent organization within the California Public Utilities Commission (CPUC) that advocates for consumers to obtain the lowest possible rates for service consistent with reliable and safe energy, water, and communications services. The Governor appoints its director.²

The CCPA applies to businesses defined broadly in scope and includes within it many types of businesses providing services regulated by the CPUC. Thus, implementation and enforcement of the CCPA will have significant impact on the consumers the Public Advocates Office represents and the businesses the CPUC regulates.

To protect the ability of consumers to fully and meaningfully exercise their rights under the CCPA, the Attorney General should adopt the changes described in this letter. The Public Advocates Office developed these recommendations to ensure that the CCPA regulations appropriately apply to the customers of communications providers, including wireline telephone, wireless telephone, and Internet Service Providers.

The below comments include recommendations on the draft regulations organized by subject matter and section, followed by recommended revisions to the draft CCPA regulations. Underlined typeface indicates proposed new language and strikethrough indicates proposed deletions.

¹ §§ 999.300 through 999.341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations.

² Pub. Util. Code § 309.5(a) and (b).

PUBLIC ADVOCATES OFFICE COMMENTS TO DRAFT CCPA REGULATIONS

Definition of Categories of Third Parties, § 999.301(e)

The definition of “categories of third parties” in subdivision (e) of § 999.301 includes Internet Service Providers (ISPs) as an example of a type of entity that does not collect personal information directly from consumers. However, according to the CCPA’s definition of “collect,”³ ISPs *do* collect personal information directly from consumers. Typical privacy policies of major ISPs provide for direct collection of consumers’ names, telephone numbers, email addresses, browsing histories and wireless app usage, or other information.⁴

As currently written, the “categories of third parties” definition implies, or could be misunderstood to imply, that the types of businesses listed—including ISPs—never collect information directly from consumers. This categorization of ISPs could potentially confuse consumers, businesses, and regulators about how and when the CCPA applies to ISPs.

RECOMMENDATION:

Section 999.301(e) should clarify that entities meeting the definition of “categories of third parties” does not necessarily mean that the entities do not, or may not, also collect personal information directly from consumers, or that they never function in direct relationship with consumers, depending on circumstances. Accordingly, the Public Advocates Office proposes the following revisions:

§ 999.301(e) “Categories of third parties” means types of entities that ~~do not~~ may collect personal information from sources other than directly from consumers, including but not limited to [list of entities as currently drafted].

³ Cal. Civ. Code 1798.140(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.

⁴ See, e.g., AT&T’s privacy policy, stating that AT&T collects information from the consumer directly as well as automatically through the use of AT&T’s networks, products, and services. (“How we collect your information” available at: https://about.att.com/csr/home/privacy/full_privacy_policy.html; accessed November 19, 2019.) The information collected directly from consumers includes, for example: names, telephone numbers, email addresses, web browsing and wireless app usage, and location of consumers’ wireless devices. (“The information we collect,” available at:

https://about.att.com/csr/home/privacy/full_privacy_policy.html; accessed November 19, 2019.)

In March, 2019, the U.S. Federal Trade Commission (FTC) issued orders to seven U.S. Internet broadband providers and related entities seeking information the agency will use to examine how broadband companies collect, retain, use, and disclose information about consumers and their devices. The orders seek information about the companies’ privacy policies, procedures, and practices. (“FTC Seeks to Examine the Privacy Practices of Broadband Providers,” available at: <https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-examine-privacy-practices-broadband-providers>; accessed November 25, 2019.)

Notice of Financial Incentive, § 999.307 and § 999.336(e)

Section 999.336(e) requires businesses to notify consumers of any financial incentive or price or service difference, and § 999.307 outlines the notification requirements. Section §999.307(a)(2)e. and (a)(3) requires a business to make the notice of financial incentive “available online or other physical location where consumers will see it before opting in,” or to provide a link to the notice in the relevant section of the business’s privacy policy. However, the draft regulations do not expressly require businesses to make the notice of financial incentive generally available for public review without requiring consumers to first create an account, enter an email address, or sign up for services. In order to make fully informed choices, consumers need an opportunity to review and compare businesses’ financial incentives before providing any personal information. Ensuring open access to the notice of financial incentive would also facilitate efficient review and enforcement of the CCPA notice requirements for oversight agencies.

RECOMMENDATION:

To support meaningful consumer choice and facilitate enforcement of the CCPA, the Public Advocates Office proposes adding a subpart (4) to § 999.307(a), as follows:

§ 999.307(a)(4) Whether made available in an online or other physical location, the notice shall be readily locatable and accessible for review by any party wishing to read the notice, without requiring the party to establish an account, create a log-in, or otherwise request or receive services from the business.

Privacy Policy and Consumers’ Rights, §999.308

Section 999.308(b)(4)a requires a business’s privacy policy to inform consumers of their right to not be subject to discriminatory treatment for exercising any privacy rights under the CCPA. This right to non-discrimination does not prohibit businesses from offering financial incentives to consumers, or price or service differences, based on the value of the consumers’ information, as the CCPA and draft regulations provide at Civ. Code § 1798.125 and § 999.336(b), respectively. However, subpart (b)(4) of § 999.308 does not require businesses to make any reference to financial incentives with their privacy policy’s explanation of the right to non-discrimination. This omission may lead consumers to misunderstand the scope of this right.

RECOMMENDATIONS:

For improved clarity, internal consistency of the regulations, and consistency with Civ. Code § 1798.125, the Public Advocates Office recommends the addition of a new sub-subpart b. to § 999.308(b)(4), as follows:

§ 999.308(b)(4)b. Explain that the business may offer financial or service incentives to consumers only when justified by the value of the consumer’s information and upon notice to the consumer as required under §999.307, with opportunity to opt-out of the incentive. If the privacy

policy is online, provide a link to the notice of financial incentive (if any).

Given the complexity of information that the draft CCPA regulations require in a privacy policy, inclusion of a template or suggested sample language describing consumers' rights could promote consistency and make it easier for businesses to comply with the requirements of § 999.308(b).⁵

Responding to Requests to Know and Requests to Delete, §§ 999.313-314

Basis for denial of access to information. Subpart (c)(5) of § 999.313 states that when a business denies a consumer's verified request to access their information because of a conflict with federal or state law, or an exception to the CCPA, the business must "explain the basis for the denial." However, the meaning of "explain" is unclear and allows for potentially vague, incomplete responses. Applying the language used later in the section in subpart (d)(6) (concerning requests to delete information), requiring that the explanation for denial include the statutory and regulatory basis for denial, resolves this issue.

RECOMMENDATION:

To ensure that consumers receive full and adequate notice of the legal basis for denial of verified requests to access their information, the Public Advocates Office recommends the following revision of § 999.313(c)(5) (in relevant part):

§ 999.313(c)(5) If a business denies a consumer's verified request to know specific pieces of personal information...because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial, including any statutory and regulatory exception therefor.⁶

Direction to service providers to delete information. The CCPA requires businesses to direct their service providers to delete consumers' personal information pursuant to a verified request,⁷ but the draft regulations do not include the steps a business must take to comply with a consumer's request to delete, as listed in § 999.313(d)(2). Similarly, the regulations do not include a provision explaining how service providers should respond to a request to delete received from businesses to which they provide services.

⁵ See further discussion of templates at pg. 9 of these comments.

⁶ The statutory and regulatory provision(s) provided to consumers as the basis for denial of access to information would, accordingly, be included with the business's records as required by § 999.317(c).

⁷ Cal. Civ. Code § 1798.105(c) states that "a business that receives a verifiable consumer request from a consumer to delete the consumer's personal information...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*" (emphasis added).

RECOMMENDATION:

To maintain consistency with the statute, protect consumers, and support businesses' compliance with the CCPA, the Public Advocates Office proposes a new sub-subpart d. to §999.313(d)(2) as follows:

§999.313(d)(2) d. Notifying any service providers to delete the consumer's personal information from their records.

In addition, the Public Advocates Office recommends a new subdivision after §999.314(d) (requirements for service providers responding to consumer requests to know or delete information), specifying what actions service providers must take in response to requests from businesses to delete consumers' personal information, as follows:

§ 999.314(e) If a service provider receives a verified request to delete a consumer's personal information from a business on whose behalf the service provider collects, maintains, or sells personal information, the service provider shall comply with the request in accordance with the provisions of § 999.313(d)(2) and any applicable statutory or regulatory requirements for protection and deletion of personal information. The service provider shall follow applicable internal procedures and contract provisions for deletion of consumer personal information it maintains on behalf of the business, provided that the procedures or contract provisions are otherwise consistent with the requirements of this title and the CCPA.

Deleting personal information from archives or backup systems. When a business stores a consumer's personal information in archives or backup systems, the draft regulations allow for indefinite delay in compliance with the consumer's request to delete "until the archived or backup system is next accessed or used."⁸ This provision undermines the purpose of consumers' right to delete their information under the CCPA, and potentially requires businesses to establish new recordkeeping systems and protocols to ensure that the consumer's information is actually deleted, if and when the archive or backup is accessed.

RECOMMENDATION:

Consumers should be afforded a reasonable timeframe in which businesses will fulfill requests for deletion, regardless of how or where the information is stored. Alternatively, a business should be required to notify the consumer at a regular interval (e.g., 30 days) that the personal information is still archived, until the business can fulfill the consumer's request and delete the information from its archives or backup systems. Accordingly, the Public Advocates Office proposes the following revisions to §999.313(d)(3):

§999.313(d)(3) If a business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete for up to 90 days

⁸§999.313(d)(3)

from receipt of the request, with respect to data stored on the archived or backup system, provided that the business complies with the requirements of §999.313(a) with notice to the consumer that the information is stored in an archive or backup system and will be deleted within 90 days.

(4) If the business maintains archives or backup systems that are not in electronic format and/or consist of physical records stored in a third-party facility, or the business's archives are not readily searchable due to unforeseen circumstances, the business shall:

- a. inform the consumer of the anticipated delay and provide a new estimated date for location and deletion or destruction of the information, and
- b. provide written notice to the consumer of the status of the consumer's request at least once every 30 days from the date of the consumer's initial request until the request is fulfilled, or until the business confirms that the consumer's information has already been destroyed.

Definition of 'Household' and Verification of Requests to Access or Delete Household Information, §§ 999.301(h), 999.318, and 999.323-.326

The Public Advocates Office recognizes the difficulty of establishing factors for safe and appropriate verification of requests by household members to access or delete information pertaining to accounts used by multiple members of a household. However, the definition of household at § 999.301(h) as "a person or group of people occupying a single dwelling" is too narrow to allow businesses to respond reasonably to requests for access or deletion of household information. People sharing a 'family' wireless plan, for example, frequently do not occupy a single dwelling. Furthermore, aggregating household information to protect privacy may not be appropriate for small households or wireless family plans shared by only two or three people.

RECOMMENDATION:

Individuals receiving communications services through a family wireless plan or shared internet services account, but who do not reside together, may or may not have privacy and information access needs that differ from occupants of a single dwelling. To allow business to more accurately assess and apply verification factors in Article 4 when responding to requests to access or delete household information, the Public Advocates Office recommends revising the definition of 'household' to include members of shared communications services accounts or plans who may not occupy a single dwelling.

Discriminatory Practices and Coercive Financial Incentives, § 999.336 and Cal. Civ. Code § 1798.125(b)(4)

The CCPA prohibits financial incentives that are discriminatory; e.g., charging a fee, denying service, providing a different level or quality of service, or using discounts based solely on a consumer's choice to exercise rights under the CCPA.⁹ Nevertheless, businesses may offer

⁹ Cal. Civ. Code § 1798.125(a)(1); draft CCPA regulations, § 999.336(a).

“financial incentives” to consumers in exchange for permission to access and use consumers’ information, if the incentives are “reasonably related to the value of the consumer’s data” and designed based on a “reasonable and good faith method for calculating the value of the consumer’s data.”¹⁰ Some entities that meet the CCPA’s definition of a business, however, such as utility companies, may be the sole providers (or one of very few providers) of essential services within their territory. Where consumers have very few or no alternatives for obtaining essential services—whether electricity, gas, water, telephone (wireline and wireless), or internet access¹¹—financial incentives may create undue pressure to opt-in to obtain the benefit of the incentive, and are much more likely to have a coercive effect, especially for lower income consumers. The CCPA expressly prohibits coercive financial incentives.¹² For this reason, businesses that provide the services of a public utility, as defined in Public Utilities Code § 216 and including communications services, should be restricted from offering financial incentives in exchange for consumer opt-in.¹³ As of 2017, approximately half of California households were already “wireless only.”¹⁴ During the October 2018 wildfires, approximately 80 percent of all 9-1-1 calls came from cellular devices.¹⁵

RECOMMENDATION:

To protect consumers from financial incentives that may have a coercive effect, particularly on lower income consumers, and to ensure consistency with other state law regulating utility services and rates, the Public Advocates Office recommends adding the following subdivision (g) to § 999.336:

§ 999.336(g) A business that provides services as a public utility, as defined by Public Utilities Code § 216, including wireless and internet communications services, to consumers in any area of the state where the business or utility service is either: (1) subject to oversight by the California Public Utilities Commission (CPUC), or (2) the only provider of equivalent utility services to consumers in any part of the business’s service area, shall be restricted from offering financial incentives for consumer opt-in as described in this section, unless the business has filed an application with and obtained

¹⁰ Cal. Civ. Code §§ 1798.125(a)(2), 1798.125(b)(1).

¹¹ Wireless and internet services are properly considered essential because these services are critical for public safety and emergency communications. In a 2018 CPUC rulemaking proceeding, the Director of California Office of Emergency Services (CalOES) stated that “it goes without saying that the communications network is foundational to public safety. ...When you are responding to an emergency, communications are your lifeline.” CPUC Rulemaking 18-03-011, “Order Instituting Rulemaking Regarding Emergency Disaster Relief Program” (“Disaster Relief OIR”); November 1, 2018 Workshop, Reporter’s Transcript (RT) at 12:25-27.

¹² Cal. Civ. Code § 1798(b)(4).

¹³ Pub. Util. Code § 701 gives the CPUC broad statutory authority to regulate utilities. Most utility providers, with the exception of broadband and (potentially) wireless services, are already prohibited under Pub. Util. Code § 453 from discrimination in provision of service and would have to obtain permission from the CPUC before adopting a financial incentive offered to ratepayers and customers.

¹⁴ National Center for Health Statistics, National Health Interview Survey Early Release Program, U.S. Department of Health and Human Services, Centers for Disease Control and Prevention, data released in December 2017.

¹⁵ See CalOES report included in Disaster Relief OIR, November 1, 2018 Workshop (RT at 15:12-22).

approval from the CPUC to offer the incentive. The requirements of this subdivision (g) shall apply to the extent consistent with the CPUC's jurisdictional authority as provided by statute.

Issues Not Addressed in the Draft Regulations

Personal Information Collected Prior to the Implementation of the CCPA

The draft CCPA regulations provide for notice to consumers about their privacy rights “at or before” the moment when their data are collected. However, the requirements for notice to a business’s existing customers are unclear.

RECOMMENDATIONS:

The regulations should ensure that businesses provide updated privacy policy information to all existing customers, at a minimum; ideally notice should be provided to all individuals whose personal information is retained by the business, whether current customers or not.

Enforcement Gaps in the CCPA

The draft regulations lack implementation guidance for the CCPA enforcement provisions in Civ. Code §§ 1798.150 and 1798.155. Section 1798.155(b) refers to a 30-day notification of alleged noncompliance, but does not specify who should notify the business, or how the notice must be provided. Consumers have no clear process for addressing violations of their privacy rights under §1798.155.

Without further regulatory guidance as to notice and enforcement procedures, consumers’ rights to know, delete, and opt-out will be mainly conceptual. Businesses are unlikely to perceive the commercial risks of noncompliance with the CCPA as high enough to justify the costs of compliance.

RECOMMENDATIONS:

The Public Advocates Office recommends inclusion of a new Article to the draft regulations to address enforcement. This Article should include sections covering the following issues:

- Clarification of the 30-day notice requirement in §1798.155: who sends it, and whether a consumer should provide proof of service and a copy of the notice to the Attorney General (or appropriate division).
- Description of a process or processes by which consumers can file complaints with the Attorney General or appropriate division when a business has failed to timely and adequately respond to the consumer’s notice of alleged violation. Electronic and paper options should be available.
- Requirement that businesses include information about the above complaint processes in their privacy policies.

- Requirement that whenever a business responds to a consumer's notice of violation with a written statement that the violations have been cured and no further violations shall occur,¹⁶ the business should provide a copy of the statement to the Department of Justice's Privacy Unit.

By the effective date of the CCPA regulations, the Attorney General should also implement a customer complaints portal and internal processes to resolve consumer complaints as provided above.

Standardized Language and Templates

To facilitate businesses' compliance with the CCPA and make it easier for consumers to understand their rights, the Public Advocates Office recommends inclusion of sample language or templates either within the regulations, or in easily accessible supplemental materials on the Attorney General's website (as well as links to the materials on the Secretary of State's Business Portal website, or any state resources frequently accessed by businesses and consumers).

RECOMMENDATIONS:

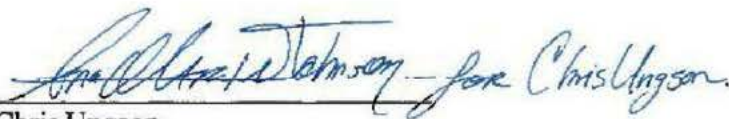
Examples of standardized or sample language may include:

- Descriptions of consumers' rights in privacy policies, as required under §999.308(b).
- A standard form or template for reporting the metrics required under §999.317(g).
- Sample notices of violation for use by consumers.

CONCLUSION

The Public Advocates Office appreciates this opportunity to provide comments on the draft regulations implementing the CCPA. These recommendations are important to ensure the regulations meaningfully and effectively implement the protections afforded to consumers under the CCPA. The effort to develop the regulations with robust public input and participation is critical. If you have any questions about the above proposals, please contact Kristina Donnelly, at [REDACTED] or Emily Fisher, at [REDACTED].

Sincerely,


Chris Ungson
Deputy Director
Public Advocates Office

¹⁶ Civ. Code § 1798.150(b).

Message

From: John Kabateck [REDACTED]
Sent: 12/6/2019 8:42:36 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Public Comment Letter re: CCPA - Small Business Data Privacy Coalition
Attachments: Small_Biz_Letter_AG_12.6.19.pdf

ATtN: Privacy Regulations Coordinator, California Office of the Attorney General

Attached please find the public comment letter submitted on behalf of the Small Business Data Privacy Coalition, as comments to the draft California Consumer Privacy Act (CCPA) regulations issued by the California Office of the Attorney General in October of this year. This letter is signed by eleven of the leading small and small ethnic business organizations from across California. Thank you and the Attorney General for your consideration of these comments during your process of evaluating these regulations. If you should have any questions, feel free to contact me at [REDACTED] or at [REDACTED].

John Kabateck
California State Director
National Federation of Independent Business



Connected Commerce
Council



SMALL
BUSINESS
CALIFORNIA



CALIFORNIA SMALL BUSINESS ASSOCIATION



November 29, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

To Whom It May Concern:

On behalf of the Small Business Data Privacy Committee and the tens of thousands of businesses we represent, we appreciate the opportunity to provide comments to the draft California Consumer Privacy Act (CCPA) regulations issued by your office in October of this year.

As written, the law and draft regulations create confusion for business and consumers, impose costs that are too high, and layer additional requirements beyond what is already in the CCPA, all of which heighten the difficulty for small and medium size business to develop in good faith a compliance regiment in a very narrow window of time given the complexity of the CCPA. It is our understanding that the finalized regulations will not be released before the spring of 2020, with an enforcement date of July 1, 2020. That only provides for a few months for small and medium size businesses once the final regulations are made public.

We appreciate your work to reconcile the CCPA and the many "clean-up" bills that were passed to clarify the original bill, but California business owners are similarly struggling to understand their compliance requirements. With less than a month to go, business owners are largely unsure of where to allocate resources, what kind of consultants are needed in order to ensure compliance, and what software is needed to upgrade their systems.

Speeding towards January 1, businesses are being required to fundamentally change their operations to become compliant with a law very few can understand, at very high cost. As determined by the economic impact assessment prepared for your office, implementation of CCPA, as passed by the Legislature, will cost California businesses \$55 billion, equivalent to 1.8% of the state's Gross Domestic Product, in just initial compliance costs. And the estimated cost of \$50,000 for small business to hire a lawyer, engage a technology business, buy software, and maintain records and respond to requests is more than many small and medium size businesses can afford.

We are concerned that the regulations exceed the requirements in the CCPA. Rather than facilitating and encouraging compliance, we believe the current regulations will lead to more confusion and noncompliance. The regulations appear to require business to comply with heightened notice requirements, establish enhanced privacy policies, and produce more information to consumers upon

request for personal information. Additionally, the regulations impose new requirements for responding to consumer requests without considering the time necessary to verify the request. This is exemplified by the new requirement to calculate the value of consumer data. Forcing businesses to calculate the value of consumer data is beyond what is written in statute. Further there are too many variables that go into this calculation making any value created subjective and unreliable.

The regulations also fail to provide enough direction around establishment of an opt-out policy. Small and medium-size businesses subject to the CCPA need more clarification of the opt-out and opt-in requirements in order to present consumers with a legally sufficient and effective means of establishing their privacy preference.

We are concerned about the broad definition of personal information and the requirement that a business identify all personal information reasonably capable of being linked to a consumer. Many businesses voiced concern about the possibility that consumer requests will create privacy issues by requiring a business to connect disparate pieces of information to respond to the consumer request. This policy seems inconsistent with the purpose of protecting privacy, potentially actionable from a security standpoint and incredibly time-consuming for a business trying to meet consumer needs. Also, the regulations are still confusing regarding household information. We are mandated to protect individual privacy but required to release household information without a means of verifying the identity of the requestor.

The regulations further introduce a process for businesses to give notices in person and gives individuals the ability to submit requests in person. This additional requirement is concerning for small business owners who might have not the bandwidth or expertise to comply with this process. The issues here are expounded by the requirement that business compile and post annual metrics from the previous year. Not only is this an onerous requirement but risks unfairly portraying small businesses in an unfavorable light despite good faith efforts to comply. This would especially be the case for small businesses who are being forced into fundamental changes of their business while under an expediated timeline.

We are also concerned that the new private right of action will lead to a cottage industry of phony complaints, much like the scams associated with the Americans with Disabilities Act (ADA). The misuse of the ADA took nearly a decade to reform and drove many small business owners into financial trouble. Here, the statutory damages that will arise from even a small data breach will be staggering – forcing many businesses to settle rather than fighting a costly legal battle over the reasonableness of their data security procedures. Worse, recovery of damages does not require plaintiffs to prove that they were actually damaged by the breach.

We are concerned that the regulations and the passage of AB 25 provide a temporary solution for handling information relating to employees. While some of the CCPA requirements were deferred, other provisions of the CCPA will take effect in January. The regulations attempt to clarify the requirements imposed on a business but have left many unsure about whether to continue to keep employees' files for the purpose of determining compensation, reviewing performance, handling possible violations of business policy or keeping records of leave and other operational matters. Much of the employee information in question is contained in company software. Given the uncertainty around a one year "fix" and the need to comply with remaining requirements, business will need to decide how to modify their current procedures or simply replace their current system. This uncertainty makes compliance more complicated and costly.

For many small and medium-size businesses, digital advertising has become the great equalizer in competing with larger entities that have a national footprint or a big traditional advertising budget. Our members are unclear about whether digital advertising will still be an effective means of reaching customers. Small and medium-size businesses have limited resources. We are not interested in accumulating personal information, we are simply trying to connect with our customers or potential customers. The proposed rules will likely make customer acquisition more expensive for small businesses by significantly limiting the availability and effectiveness of targeted advertising. Clarity around permissible interactive engagement would help us to understand how we can operate within the limitations of the law.

We strongly support efforts to protect consumer privacy. But in doing so, we also must ensure that the rules governing these protections are laid out in a way that allows businesses to reasonably and successfully comply with the law. Protecting consumers privacy is an important and laudable goal – but not a goal to be pursued at any cost. Rather, we believe the goal should be to pursue sensible, cost-effective privacy rules. Consumers count on us to protect their privacy; however, they also rely on us to maintain a functioning economy as well as ensure their access to internet services. We trust that as your office finalizes the regulations, you will ensure that all these goals can be achieved.

Sincerely,

Coalition members:

California Asian Pacific Chamber of Commerce
California Hispanic Chambers of Commerce
California Restaurant Association
California Small Business Association
Coalition of Small & Disabled Veteran Businesses
Connected Commerce Council
Latin Business Association
Los Angeles Business Federation
National Federation of Independent Business, CA
Small Business California
Valley Industry & Commerce Association

Message

From: Alex Berger [REDACTED]
Sent: 12/6/2019 12:15:03 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Public Comments of MIC, SVIA & ROHVA re CCPA Regulations
Attachments: 2019-1206 MIC SVIA ROHVA Public Comment re CCPA regulations.pdf

Attached, please find written comments of the Motorcycle Industry Council, the Specialty Vehicle Institute of America, and the Recreational Off-Highway Vehicle Association, relevant to the proposed rulemaking action for the California Consumer Privacy Act.

Sincerely,

Alex Berger

--

Alexander B. Berger
General Counsel
Motorcycle Industry Council

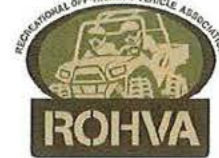
Office
Mobile
Email



The information contained in this e-mail, including any attachments, is confidential and intended solely for the named recipient(s) and may be subject to protection under federal and state laws. If you are not the intended recipient, please inform the sender immediately by reply e-mail that the message was sent in error and delete the message. Thank you.



**MOTORCYCLE
INDUSTRY
COUNCIL**



December 5, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

via email: PrivacyRegulations@doj.ca.gov

Re: Public Comments to §§ 999.300 through 999.341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations (CCR) concerning the California Consumer Privacy Act (CCPA)

Dear Attorney General Becerra:

We are pleased to offer comments regarding the CCPA on behalf of the Motorcycle Industry Council (MIC), the Specialty Vehicle Institute of America (SVIA) and the Recreational Off-Highway Vehicle Association (ROHVA). MIC, SVIA and ROHVA collectively represent more than 700 motor vehicle manufacturers, dealers, aftermarket and allied trades.

As we read the CCPA's exemption for motor vehicles, our manufacturers of motorcycles, all-terrain vehicles (ATVs) and recreational off-highway vehicles (ROVs) are exempt from provisions granting consumers the right to opt out vehicle information or ownership information retained or shared between a new motor vehicle dealer and the vehicle's manufacturer, if the information is shared for the purpose of effectuating or in anticipation of effectuating a vehicle repair covered by a vehicle warranty or a recall.¹

Vehicles manufactured by MIC, SVIA and ROHVA should be treated the same as automobiles under the CCPA. The data provided by purchasers of motorcycles, ATVs and ROVs is substantially the same as data provided by automobile consumers. As in the automotive industry, that data is critical for dealers and manufacturers to notify customers of critical updates such as warranty and recall information. We are asking you to confirm the above interpretation and to ensure regulatory parity under the CCPA between automobiles and other motor vehicles such as motorcycles, ATVs and ROVs.

Thank you for the opportunity to clarify this critical issue on behalf of MIC, SVIA and ROHVA's members.

Sincerely,

Erik Pritchard
MIC President & CEO
SVIA President & CEO
ROHVA President & CEO

¹ See AB-1146, California Consumer Privacy Act of 2018: Exemptions: Vehicle Information, at https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1146.

2 Jenner, Suite 150, Irvine, CA 92618 / [REDACTED]

Message

From: Townley, Katie [REDACTED]
Sent: 12/6/2019 11:52:20 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Hutnik, Alysa [REDACTED]; Myers, Lauren [REDACTED]
Subject: QuinStreet, Inc. Comments to Proposed CCPA Regulations
Attachments: QuinStreet, Inc. Comments to Proposed CCPA Regulations.pdf

On behalf of QuinStreet, Inc., we are pleased to submit these comments in response to the proposed California Consumer Privacy Act regulations.

Please do not hesitate to contact us if you have any questions.

Katie

KATIE TOWNLEY

Senior Associate

Kelley Drye & Warren LLP
Washington Harbour
3050 K Street NW, Suite 400
Washington, DC 20007
Tel: [REDACTED]

WWW.KELLEYDRYE.COM

[REDACTED]



The Washington Post

This message is subject to Kelley Drye & Warren LLP's email communication policy.

[KDW-Disclaimer](#)

December 6, 2019

Via Online Submission – PrivacyRegulations@doj.ca.gov

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: Proposed California Consumer Privacy Act Regulations

QuinStreet, Inc. (“QuinStreet”) is pleased to submit these comments in response to the proposed California Consumer Privacy Act (“CCPA”) regulations (the “Regulations”). QuinStreet supports the CCPA; we believe consumers are entitled to know who has their data, where they got it, and where it goes.

With over 200 engineers and dozens of legal, compliance, and content personnel, QuinStreet has the resources to devote to CCPA compliance, regardless of what the final Regulations say. At the same time, based upon our 20 years of experience in online marketing, we believe portions of the Regulations may inadvertently impose burdens on online publishers, intermediaries, and advertisers that will not bring corresponding benefits to consumers (or regulators).

In particular, QuinStreet believes Sections 999.305(d), 999.315(c), 999.315(f), 999.316, and 999.317(g), as written, may have unintended adverse consequences that the Attorney General should consider. We have included, as Appendix A, specific changes to the Regulations to address the concerns identified in these comments.

QuinStreet provides these comments in light of its role as a leading provider of consumer “search and compare” performance marketing services. In that role, QuinStreet leverages proprietary technologies to receive and share consumer data to match consumers with products and services that may meet their needs. QuinStreet, a publicly-traded company (NASDAQ: QNST), is based in California, generates over \$500 million in revenue annually, and employs over 600 people.

I. A Brief Overview of Online Advertising

Every website has an owner (a “Publisher”). In order to generate content (e.g., pay writers, buy graphics, host the site, etc.), the Publisher needs income. The quest for income is generally referred to as “monetization.”

At one level, online monetization mirrors the offline world (e.g., in newspapers, billboards and TV). In each case, Publishers lease space on their property to an Advertiser. The internet consists of millions of Publishers, many of which are individuals or small businesses.¹ Given that number of properties and advertisers, Intermediaries (e.g., advertising agencies) grew to manage campaigns, purchase media, and maintain compliance with advertiser and public standards.

¹ Some of the best content on the internet, especially for consumers, come from small sites that are passionate about a single topic (e.g., auto insurance or airline rewards programs).

Using technology, contracts, and business processes at scale, Intermediaries manage the millions of queries and responses consumers and businesses exchange in real-time every day.

A. Performance Marketing

Historically, Advertisers had difficulty tracking whether consumers who saw their offline ads became customers. Advertisers would prefer to only pay Publishers when their visitors (consumers) become the Advertiser's customers. In the online world this match between consumer intent and business results is generally referred to as "performance marketing." Intermediaries in the online world, such as QuinStreet, manage this data-driven approach to marketing, including the compliance responsibilities that result from witnessing consumer intent and advertiser results.

B. Consumer Expectations

Performance marketing also aligns with 21st century consumer expectations. Consumers increasingly begin their searches for products and services online. Consumers expect that search engines and other websites will enable their "search and compare" behavior. Consumers have also come to understand that providing websites with their data can lead to a more tailored – and thereby beneficial – search experience.²

Not all consumers have the same expectations (and comfort level) with the depth and scope of online data sharing. We appreciate that one of the goals of the CCPA is to increase transparency for consumers (and regulators). Our comments below are intended to align with those goals without saddling the vast, long tail of small Publishers and Advertisers with burdens that they will struggle to meet.³

II. Third-Party Sale Verification

Section 999.305(d) of the Regulations could place a substantial burden on certain businesses that collect consumers' personal information, without providing corresponding benefits to consumers. Specifically, in online advertising (including performance marketing), a consumer often submits personal information on Website A (i.e., a Publisher). That information may then be transferred to Business B (e.g., an Agency or Aggregator (an "Intermediary")) before it is delivered to Advertiser C. As written, the Regulation would require Business B to comply with the following obligations:

1. Provide direct notice to the consumer that (i) Business B will sell the consumer's personal information, and (ii) the consumer has a right to opt out of such sale; or

² It is hard to get a good travel quote (let alone a flight or hotel room) if you are not willing to reveal where and when you are traveling.

³ From the tenor of many of the comments at the recent public hearings, it is not clear that the majority of companies that do business online understand what they will need to do come January 1, 2020.

2. Obtain a signed attestation from the Publisher that describes how the Publisher gave compliant notice of its sale practices and the consumer's opt-out rights at collection, as well as an example of that notice.

We respectfully submit that the real-time nature of much online advertising makes real-time confirmation (section 999.305(d)(2)) impracticable for most Intermediaries. Accordingly, we begin our comment with a focus on post-sale certification (section 999.305(d)(2)), and how we believe it can be achieved without undue burden.

A. Intermediaries Should Be Able to Rely on Existing Contractual and Other Mechanisms to Comply with Section 999.305(d)(2)

Section 999.305(d)(2) would require that Intermediaries obtain “signed attestations” and a copy of the notice provided to consumers from each Publisher. The Initial Statement of Reasons (“ISOR”) suggests that this process should “not be overly burdensome” to businesses.⁴ In that spirit, QuinStreet respectfully requests that the Attorney General confirm that existing contractual and compliance-oriented mechanisms may be used to satisfy the requirements of Section 999.305(d).

Businesses like QuinStreet have invested millions of dollars in technology, personnel, and business processes to ensure consumer information is gathered and transferred in accordance with the consumer's expectations (and in compliance with applicable law). These business processes include contractual provisions (e.g., representations, warranties, and covenants), as well as initial due diligence, periodic auditing, and consumer complaint monitoring. This approach is consistent with Federal Trade Commission guidance, which recommends flexible and resource-conscious – yet effective – steps for “supply chain” management.⁵ This approach is also consistent with other consumer protection laws and regulations, including interpretation of California's Unfair and Deceptive Practices Act.⁶

Making such materials available to consumers upon request⁷ would also be unmanageable from a recordkeeping perspective and prevent businesses from responding to consumers in a timely manner. QuinStreet and other Intermediaries receive personal information from tens of thousands of consumers and hundreds of Publishers daily. Maintaining notices from each Publisher would be extremely burdensome in and of itself. Attempting to identify and provide the relevant notice in response to each consumer's request would only impose additional burdens on businesses, especially small businesses, which represent the majority of Publishers.

⁴ Initial Statement of Reasons, Proposed Adoption of California Consumer Privacy Act Regulations, 43 (2019) (*hereinafter* “ISOR”).

⁵ See Andrew Smith, *Companies Must Manage Lead Generators Responsibly*, Law360 (Sept. 25, 2019), available at <https://www.law360.com/articles/1202654/companies-must-manage-lead-generators-responsibly>. Existing federal and state consumer protection laws and regulations also require the disclosure of Intermediaries, including in connection with telemarketing, electronic signatures, and otherwise.

⁶ See Cal. Bus. & Prof. Code §§ 17200 *et seq.*

⁷ See Cal. Code Regs. tit. 11, § 999.305(d)(2)(b) (proposed Oct. 11, 2019).

Intermediaries will in any event, pursuant to their existing contracts, have their counterparties represent, warrant, and covenant that each party is in compliance with the CCPA (as with all other laws). Allowing Intermediaries to use their existing diligence, contractual, and monitoring processes to confirm CCPA compliance provides the same benefit to the consumer as seeking individual signed attestations for each transaction, but with significantly less administrative effort for the business or risk of opportunity loss for the consumer.

Accordingly, QuinStreet respectfully requests that the Attorney General confirm that businesses may rely on existing business processes (e.g., contractual provisions) to comply with Section 999.305(d). We have included in Appendix A suggested language to this effect.

B. Compliance with Section 999.305(d)(1) Would Not Provide Consumers with Meaningful Notice

The ISOR states that the Attorney General’s office believes Section 999.305(d) “will provide consumers with more effective notification of the business’s collection practices than any alternative” and will “[ensure] that consumers have an opportunity to opt-out of the sale of their personal information before it is sold by those businesses.”⁸ QuinStreet respectfully disagrees.

Requiring that the Intermediary contact the consumer directly prior to sharing the consumer’s personal information would render the information sharing process inefficient and burdensome. Businesses like QuinStreet connect consumers with better pricing and/or services within seconds. Section 999.305(d)(1) would encumber the consumer’s online experience without adding value, slowing down service to consumers. At best, it adds to “notice fatigue”⁹; at worst, it is impractical.

The consumer already begins their “search and compare” journey with a notice from the Publisher. The Regulation as written would result in the consumer receiving an additional notice from each Intermediary with which the Publisher shared their personal information. With each notice the consumer receives, the likelihood that they take the time to read and understand it decreases, rendering the notice insignificant and an inefficient use of consumer time and business resources.

Further, in a number of “search and compare” scenarios, subsequent notice is either redundant or impossible. For example, many Intermediaries do not have a direct relationship with the consumer, but nonetheless provide an integral role in fulfilling a consumer’s request.¹⁰ In these scenarios, the consumer has agreed to the Publisher engaging in this practice, and has typically been notified about other entities with whom the Publisher may share their personal

⁸ ISOR, at 9–10.

⁹ The concept of “notice fatigue” suggests that consumers encounter so many privacy notices and policies that such messaging becomes meaningless to them. *See, e.g.,* Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* 1, 42 (2014), available at https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

¹⁰ These Intermediaries may, for example, match a consumer with insurance options, based on the consumer’s needs and the insurance providers’ offerings.

information.¹¹ Adding a “Do you really, *really* want the help you just asked for?” step would not add value. In light of these considerations, QuinStreet respectfully requests that the Attorney General reconsider whether including Section 999.305(d)(1) in the Regulations is appropriate.

III. Opt-Out Requests

Section 999.315 of the Regulations discusses a business’s obligations with regard to consumer requests to opt out of the sale of their personal information. QuinStreet’s comments on subsections (c) and (f) are as follows:

A. Section 999.315(c): Requiring that Businesses Treat “Do Not Track” Requests or Settings as Opt-Out Requests Is Unnecessary and Will Complicate an Otherwise Clear and Straightforward Process

1. The “Do Not Sell” Hyperlink/Button Is the Most Effective Way for Consumers to Opt Out

Section 999.315(c) of the Regulations would require that businesses “treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information as a valid request.” Proposed Section 999.315(c)’s requirement is unnecessary, as the CCPA already contemplates the ideal method for indicating a request to opt out – **a prominent and easily-accessible link on the business’s website**.

The CCPA requires that businesses that sell personal information include a “clear and conspicuous link on the business’s Internet homepage, titled ‘Do Not Sell My Personal Information’” for a consumer to request to opt out of the sale of their personal information.¹² The Regulations also will include a uniform “opt-out button,” ensuring that consumers understand how to effect this right across all online services subject to the CCPA.

Attempting to use the Regulations to mandate acceptance of a flawed privacy setting seems suboptimal. For example, the current Do Not Track browser plugin is largely ineffective in preventing browsers from collecting browsing information from consumers.¹³ Businesses could not agree on a common standard to govern how the plugin would work, so the once-promising

¹¹ In fact, in many instances, the consumer has provided prior express written consent, pursuant to the Telephone Consumer Protection Act and its implementing regulations, 47 U.S.C. § 227 and 47 C.F.R. § 64.1200, to the first-party business sharing the consumer’s personal information with its partners so that those partners can contact the consumer with information about products or services she desires.

¹² Cal. Civ. Code § 1798.135(a)(1). A “homepage” is defined as “the introductory page of an internet website and any internet web page where personal information is collected.” *Id.* § 1798.140(l).

¹³ See, e.g., Chris Hoffman, *RIP “Do Not Track,” the Privacy Standard Everyone Ignored*, How-To Geek (Feb. 7, 2019), available at <https://www.howtogeek.com/fyi/rip-do-not-track-the-privacy-standard-everyone-ignored/>; Glenn Fleishman, *How the Tragic Death of Do Not Track Ruined the Web for Everyone*, Fast Company (Mar. 17, 2019), available at <https://www.fastcompany.com/90308068/how-the-tragic-death-of-do-not-track-ruined-the-web-for-everyone>.

feature is now essentially defunct.¹⁴ Further, browsers do not respond to consumer requests in a way that meets consumer expectations.¹⁵

The lack of industry consensus regarding what the “Do Not Track” plugin means has rendered consumers’ attempts to use the plugin fruitless and the promises of the plugin misleading. As a result, Section 999.315(c) of the Regulations would frustrate the Legislature’s directions to the Attorney General to establish rules “necessary to ensure that the notices and information that businesses are required to provide . . . are provided in a manner that may be easily understood by the average consumer.”¹⁶

The CCPA and its Regulations provide a great opportunity to create a workable consumer data notice and compliance regime. Encumbering the CCPA with the legacy of the failed Do Not Track concept would be unfortunate. The CCPA hyperlink/button is a much more effective means to ensure that consumers understand how to opt out of a sale, and should remain the sole option for consumers to exercise their rights under Civil Code section 1798.120.¹⁷

2. The Proposed Requirement Is Overly Broad and Will Be Burdensome for Businesses

The Regulations would require that a business “treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism” as a valid opt-out request. This language is overly broad and will create burdens for businesses without aiding consumers in effecting their opt-out rights.

For example, it would require businesses to invest substantial resources to continually update and maintain programs that recognize any and all “user-enabled privacy controls.” Most businesses (especially small businesses, which constitute the majority of online Publishers) do not have the resources to monitor each and every technological development intended to give a consumer control over their online browsing preferences.

The ISOR suggests that this provision is intended to ensure innovation in developing options for consumers to make opt-out requests.¹⁸ Limiting the opt-out request to the approved

¹⁴ See W3C Working Group, *Tracking Preference Expression (DNT)*, W3C (Jan. 17, 2019), available at <https://w3c.github.io/dnt/drafts/tracking-dnt.html> (noting that there was not “sufficient deployment of [the DNT extensions] to justify further advancement [of the plugin], nor [were there] indications of planned support among user agents, third parties, and the ecosystem at large”).

¹⁵ See Kashmir Hill, ‘Do Not Track,’ the Privacy Tool Used by Millions of People, Doesn’t Do Anything, *Gizmodo* (Oct. 15, 2018), available at <https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324>.

¹⁶ Cal. Civ. Code § 1798.185(a)(6).

¹⁷ QuinStreet also notes that this provision is at odds with the “Do Not Track” language in the California Online Privacy Protection Act (“CalOPPA”). CalOPPA requires that operators of commercial websites or online services disclose in their privacy policies *how* they honor or comply with browser “do not track” signals or other mechanisms. It does not require that they automatically comply with such mechanisms. See Cal. Bus. & Prof. Code § 22575(b)(5).

¹⁸ ISOR, at 24.

hyperlink/button does not, however, preclude the Attorney General from updating the regulations to later identify other mechanisms that ultimately prove effective. Without assurance that all “user-enabled privacy controls” are effective and easy-to-understand, however, the “Do Not Sell” hyperlink/button should remain the sole option for a consumer to opt out of a sale.

B. Section 999.315(f): Requiring Businesses to Notify Third Parties Not to Further Sell Personal Information Does Not Reflect the Legislative Intent of the CCPA (and May Not Reflect Consumer Preferences)

Section 999.315(f) of the Regulations would require a business that receives an opt-out request to (i) notify any third parties to whom it has sold the consumer’s personal information within the 90 days prior to receipt of such request and (ii) instruct such third parties not to sell the consumer’s information.

There is no statutory basis for Section 999.315(f)’s requirement. The CCPA states that “[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.”¹⁹ The statute does not require the business to inform the third parties with whom it shared such data of the opt-out request. In contrast, the statute explicitly provides that when a consumer makes a deletion request, a business must direct its service providers to delete the consumer’s personal information from its records.²⁰ This difference demonstrates the Legislature’s intent to not require that businesses communicate opt-out requests to service providers or third parties.

Further, requiring businesses to pass opt-out signals to third parties may not reflect consumer preferences. For example, a consumer may visit a campground website because they are visiting that campground for vacation. As disclosed in its privacy policy, that site may then share the consumer’s personal information with camping supply retailers that use such information to deliver relevant advertising to the consumer. Although the consumer may later exercise their opt-out right with respect to the campground website, taking that action does not mean the consumer no longer wants to receive relevant advertising about camping supplies. The consumer still enjoys camping, after all.²¹ And, the consumer can already opt-out of receiving camping supply advertising directly.²²

Finally, mandating that a business later restrict a recipient from selling personal information would interfere with the basis of the bargain upon which the personal information was shared

¹⁹ Cal. Civ. Code § 1798.120(d).

²⁰ *Id.* § 1798.105(c).

²¹ Moreover, in the online environment, the reality is the “third-party advertising” the consumer receives will largely consist of (i) email and (ii) display ads in subsequent online sessions. With respect to email, the consumer already has well-established (and commercialized) unsubscribe options. With respect to display advertising the elimination of the camping supply ad will just result in the consumer seeing a different ad, not no ad at all.

²² For example, by unsubscribing from the supplier’s email list. The consumer may also indicate (to the ad server) that they no longer want to see display/click ads for camping supplies.

initially. In light of these considerations, QuinStreet respectfully requests that the Attorney General remove subsection (f).

IV. Re-Opt-In Requests

Section 999.316 of the Regulations would require that businesses employ a two-step opt-in process to confirm that a consumer who previously opted out of the sale of their personal information wants to opt back into such sale. This two-step process is burdensome to both consumers and businesses, and it may lead businesses to simply refuse the consumer's request to re-opt in.

Publishers give consumers the opportunity to provide their personal information for the purpose of connecting the consumers with related products and services. These Intermediaries connect consumers with essential products and services, such as home and auto insurance, on which consumers rely. These connections are made in real-time.

Requiring a two-step verification process makes real-time connections difficult-to-impracticable. It is a non-trivial challenge to segment consumers that (x) have opted out of a sale and (y) now want to opt in again, but (z) have not yet provided confirmation. The simplest solution to this challenge would be to permanently bar opted-out consumers from seeing relevant advertising (even if such advertising represents the optimal product and service that meets their needs).²³ To prevent these unintended consequences, QuinStreet respectfully requests that the Attorney General allow flexibility in the re-opt-in process, as proposed in Appendix A.

V. Compliance Metrics Tracking and Disclosure Requirements for Certain Businesses

Section 999.317(g) of the Regulations would require that certain businesses retain and disclose statistical data regarding the consumer requests received and complied with, and the timing associated with such requests. This requirement adds burdens to businesses without providing benefits to consumers (or regulators).

Whether a business has complied in whole or in part or denied Consumer A's request may be irrelevant to how the business will respond to Consumer B's request. Further, such information may discourage a consumer from making a valid request if the metrics indicate, for example, that the business has denied a large number of requests – even if those denials were valid.

The statute already requires businesses to respond to verifiable consumer requests within 45 days.²⁴ We are not aware of other instances in which parties are obligated to post publicly how much they beat a deadline by, without regard to the complexity of the case. Moreover, the more

²³ The income from matching any one consumer to any one advertiser is trivial. The cost of confirming an opt-in is significant and effectively impracticable in many cases in real-time. Accordingly, many intermediaries may simply opt consumers out permanently.

²⁴ *Id.* § 1798.130(a)(2).

interesting data for most businesses is how many problems they avoided in the first place, not how fast they were in solving the ones created.²⁵

Businesses will retain this data (or could develop it in response to an Attorney General request). A large intermediary operating at scale, like QuinStreet, will probably have it at hand in any event. But, saddling thousands of small Publishers with an obligation to track, post and update information that is likely of little value to consumers seems suboptimal.

Accordingly, QuinStreet respectfully requests that the Attorney General remove Section 999.317(g) from the Regulations or, at a minimum, remove subsection (2), which obligates businesses to make this information publicly available.


* * *

We appreciate the opportunity to submit these comments. Please do not hesitate to contact us if you have any questions.

Respectfully submitted,

Marissa Levinson

Marissa Levinson
Vice President and Associate General Counsel
QuinStreet, Inc.
950 Tower Lane
Foster City, CA 94404

Counsel:
Alysa Hutnik
Katherine Townley
Lauren Myers
Kelley Drye & Warren LLP
3050 K Street, NW, Suite 400
Washington, DC 20007


²⁵ Metrics for problem avoidance also are hard to come by; just ask any business legal or compliance department.

Appendix A: Proposed Regulatory Changes

This Appendix A provides the revisions to the sections of the Regulations discussed in the comments above. Language that QuinStreet proposes to delete is ~~struck through~~, and proposed additions are double underlined.

§ 999.305. Notice at Collection of Personal Information

...

- (d) A business that does not collect information directly from consumers does not need to provide a notice at collection to the consumer, but before it can sell a consumer's personal information, it shall do ~~either~~ one of the following:
- (1) Contact the consumer directly to provide notice that the business sells personal information about the consumer and provide the consumer with a notice of right to opt-out in accordance with section 999.306; or
 - (2) Contact the source of the personal information to:
 - a. Confirm that the source provided a notice at collection to the consumer in accordance with subsections (a) and (b); and
 - b. Obtain signed attestations from the source describing how the source gave the notice at collection and including an example of the notice. Attestations shall be retained by the business for at least two years and made available to the consumer upon request; or
 - (3) Confirm through contract terms with the source of the personal information that the consumer was provided with a notice of his or her right to opt-out in accordance with section 999.306, and implement reasonable due diligence and monitoring processes to confirm compliance with such contract terms.

§ 999.315. Requests to Opt-Out

...

(c) ~~If a business collects personal information from consumers online, the business shall treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.~~

...

(f) ~~A business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the consumer's request that the consumer has exercised their right to opt-out and instruct them not to further sell the information. The business shall notify the consumer when this has been completed.~~

...

§ 999.316. Requests to Opt-In After Opting Out of the Sale of Personal Information

- (a) ~~Requests to opt-in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in~~ require a consumer to expressly agree to the subsequent sale of his or her personal information. Express agreement includes, but is not limited to, clicking a previously un-clicked checkbox or providing a verbal "yes."
- (b) A business may inform a consumer who has opted-out when a transaction requires the sale of their personal information as a condition of completing the transaction, along with instructions on how the consumer can opt-in.

§ 999.317. Training; Record-Keeping

...

~~(g) — A business that alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers, shall:~~

~~(1) — Compile the following metrics for the previous calendar year:~~

~~a. — The number of requests to know that the business received, complied with in whole or in part, and denied;~~

~~b. — The number of requests to delete that the business received, complied with in whole or in part, and denied;~~

~~c. — The number of requests to opt out that the business received, complied with in whole or in part, and denied; and~~

~~d. — The median number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt out.~~

~~(2) — Disclose the information compiled in subsection (g)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy.~~

~~(3) — Establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.~~

###

Message

From: Shane Wiley [REDACTED]
Sent: 12/6/2019 6:49:37 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Recommended Clarifications to and Questions about the CCPA Regulation Draft
Attachments: Cuebiq Submission to CCPA Regulation.docx

Privacy Regulations Coordinator,

Thank you to the entire California Attorney's General office team that worked on managing the public review process of both CCPA and now the draft Regulation. We have a few recommendations for clarification to the Regulation primarily with regard to the limited flexibility of use for the key user opt-out action under "Do Not Sell My Personal Information". We have a single question as to the intersection, if any, between a user's direction to share information between two parties and the application, if any, of a user's opt-out to the sale of their Personal Information. If you have any questions about our comments or question, please don't hesitate to reach out to use for further details.

[Document Attached]

Thank you,
Shane Wiley
Chief Privacy Officer
Cuebiq



[Like](#) | [Follow](#) | [Connect](#)

This email is reserved exclusively for sending and receiving messages inherent working activities, and is not intended nor authorized for personal use. Therefore, any outgoing messages or incoming response messages will be treated as company messages and will be subject to the corporate IT policy and may possibly to be read by persons other than by the subscriber of the box. Confidential information may be contained in this message. If you are not the address indicated in this message, please do not copy or deliver this message to anyone. In such case, you should notify the sender immediately and delete the original message.

To: Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

From: Shane Wiley
Chief Privacy Officer @ Cuebiq, Inc.
15 W 27th St., 10th Floor
New York, NY 10001
[REDACTED]

Re: Recommended Clarifications to and Questions about the CCPA Regulation Draft

Thank you to the entire California Attorney's General office team that worked on managing the public review process of both CCPA and now the draft Regulation. We have a few recommendations for clarification to the Regulation primarily with regard to the limited flexibility of use for the key user opt-out action under "Do Not Sell My Personal Information". We have a single question as to the intersection, if any, between a user's direction to share information between two parties and the application, if any, of a user's opt-out to the sale of their Personal Information. If you have any questions about our comments or question, please don't hesitate to reach out to use for further details.

Recommendations on Clarifications to the CCPA Regulation draft

Reference: 999.305 (a)(3):

A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.

Note: The introduction of a new **prospective** use of information should conform to the same initial standard of notice but should be paired with a reminder that the user can exercise their right to opt-out at the same time of the notice. Only the introduction of a new retrospective use should require explicit consent as this is a change to practices outlined at the time the personal information was collected from the user.

Recommended Language: If the business intends to use a consumer's **previous collected** personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall...

Reference: 999.305 (b)(3):

If the business sells personal information, the link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info" required by section 999.315(a), or in the case of offline notices, the web address for the webpage to which it links.

Note: It would be helpful for consumers and businesses alike to leverage existing mechanisms for user's to exercise their right to "opt-out" of data collection or data sales. We recommend that an allowance for leveraging existing "opt-out" links and mechanisms if their equivalence is explained in the Privacy Policy. For example, "Your privacy right to opt-out, or to direct us to "Do Not Sell My Personal Information", is provided here or anywhere else on this site where you see the term "Opt-Out". This term "opt-out" is the universal standard so would both meet consumer needs (high degree of understanding of what this means among users) and would lower the engineering and operational overhead of introducing new links within existing technical environments. This would also provide a mechanism for layered additional prescriptive language that may emerge from our state privacy laws.

Recommended Language: If a business sells personal information, the link titled "Do Not Sell My Personal Information", "Do Not Sell My Info", **or a well understood proxy, such as "Opt Out", that is clearly explained in the Privacy Policy**, required by section...

Reference: 999.306.

Notice of Right to Opt-Out of Sale of Personal Information

Note: Similar request as the previous request to allow existing links for "Opt Out", if well explain as equivalent in the Privacy Policy, to suffice for links labeled "Do Not Sell My Personal Information". Please take note of the heavy use of the term "Opt-Out" already leveraged in the Regulation as a proof point of its equivalence.

Recommended Language: **(a)(2)e.** The use of well understood terms of proxy, such as "Opt Out" may suffice in the place of "Do Not Sell My Personal Information" if the equivalence is explained in the Privacy Policy.

Note: In section (e) it would be helpful to provide a button with the term "Opt Out" to support the equivalence concept and provide a more universal platform of user understanding and scalability across individual state privacy laws.



Reference: 999.308.

Privacy Policy

Note: **(b)(3)c.** For consistency throughout the Regulation, it's recommended to add a new element of this section to highlight the requirement to list equivalent terms that may be used as a proxy for "Do Not Collect My Personal Information".

Proposed Language: Provide an explanation of any commonly recognized privacy right terms you may be using, such as "Opt-Out", in your privacy policy as a fully equivalent path to "Do Not Collect My Personal Information".

Note: (b)(5)b. Authorized Agent - It's recommended that the regulation also request existing authorized agents be listed so users understand the full scope of their technical options to exercise their privacy rights under CCPA such as if DNT or Mobile Operating Systems opt-outs are honored as equivalent to "Do Not Collect My Personal Information" and if so, how to configure them properly to be recognized as intended by the company.

Proposed Language: a. Explain how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf **or provide a list of authorized agents you already support with instructions on how those may be accessed.**

Reference: 999.312.(e)

Methods for Submitting Requests to Know and Requests to Delete

Note: As many business operate solely as mobile applications it would be helpful to insert this as a key example in the scope of covered areas in the regulation. We would recommend that you also add the concept of "physical interaction" such that the "online only" perspective of the statute is more easily understood.

Proposed Language: If a business does not interact directly with consumers **in the physical world** in its ordinary course of business, at least one method by which a consumer may submit requests to know or requests to delete shall be online, such as through the business's website or a link posted on the business's website.

Reference: 999.315.(h)

Requests to Opt-Out

Note: In some cases, as with mobile devices, it may be necessary for a user to provide even their opt-out in a validatable manner such that their opt-out is not impacted another individual unfairly and outside of their direct request. It would be helpful if this element of the Regulation could be updated to support validation for opt-out, especially on mobile devices

Proposed Language:

(h) A request to opt-out need not be a verifiable consumer request. If a business, however, has a

good-faith, reasonable, and documented belief that a request to opt-out is fraudulent **or pathway to request opt-out is easily attackable in a fraudulent manner**, the business may deny the request **or request further verification that the request is originating with the user the Personal Information was collected from**. The business shall inform the requesting party **if further verification is requested or** that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent.

-also-

Add "to opt-out, " in 999.323. General Rules Regarding Verification

(a) A business shall establish, document, and comply with a reasonable method for verifying that the person making a request **to opt-out**, to know or a request to delete is the consumer about whom the business has collected information.

Questions Not Addressed by Current Regulation Draft

Reference: CCPA 1798.140.(t)(2)(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.

Question: When prior direction (consent) has been received from a user to disclose their Personal Information with another party -and- a separate tool for a user to retract consent is provided in the same interface in which they provided that direction (consent) does a company need to apply a user's selection of "Do Not Sell My Personal Information" to that specific Personal Information that is being shared under the direction of the user?

Reasoning: Our assumption is that the independent opt-in consent directing a company to share the user's Personal Information with another party removes this sharing under the definition of "Sale" and therefore is not subject to the application of "Do Not Sell My Personal Information" but only if a separate tool is provided to the user for them to retract that initial direction (consent).

CCPA_45DAY_01526

Message

From: Thresher, Chip (Refinitiv) [REDACTED]
Sent: 12/6/2019 9:34:22 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Refinitiv Comments
Attachments: Refinitiv Comments to AG.pdf

I respectfully submit Refinitiv's comments regarding the proposed adoption of sections §§ 999.300 through 999.341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations (CCR) concerning the California Consumer Privacy Act (CCPA).

Chip Thresher
Head of Industry and Government Affairs, Americas
REFINITIV

Phone: [REDACTED]
Mobile [REDACTED]

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Via Email to: PrivacyRegulations@doj.ca.gov

Dear Attorney General Becerra,

Refinitiv writes to provide comments regarding the proposed adoption of sections §§ 999.300 through 999.341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations (CCR) concerning the California Consumer Privacy Act (CCPA).

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 and the proposed regulations 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 practice 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 down in the UN Global Compact. They 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 prevention often necessitate the processing of personal information as defined under §1798.140. For these activities, the personal information processed is aggregated largely from publicly available sources and often provided by third party data providers, like Refinitiv, that maintain databases and provide services to support these efforts. Generally, Refinitiv and similar third parties 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.

We have deep concerns about section 999.305(d) of the proposed regulations, which applies to businesses that collect personal information about consumers from sources other than consumers themselves. The regulation requires that before selling that information: they must (1) contact the consumer directly to provide notice that the business sells personal information about the consumer, and provide the consumer with a notice of right to opt-out of those sales; or (2) obtain signed attestations from the sources of the personal information, describing how the sources gave the notice at collection and providing an example of the notice. This obligation is untenable, especially regarding businesses such as Refinitiv where the personal information collected is often obtained from lawful, publicly available sources such as widely distributed media. There is generally no contact information available to us or to the sources collected from, providing no reasonable way to provide any sort of direct notice or attestation to that effect.

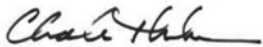
Another area we are deeply concerned with is section 999.315(f) of the proposed regulations, which requires a business that has received a consumer's opt-out request to provide notice of that request to all third parties to whom it has sold the consumer's personal information in the 90 days preceding the request, and instruct those third parties to refrain from further selling the consumer's personal information. This provision would create an environment where a business would be forced to breach existing contracts by limiting the rights granted in contacts with other third parties.

Any final rulemaking should revise or remove the provisions outlined above and should make it clear that organizations like Refinitiv, as a third party, should be permitted to collect, process, and sell personal information for business purposes and not be required to honor a consumer's request to opt-out of having Refinitiv share such personal information for the sole purpose of fighting financial crime. 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 issues such as third party responsibilities and use of publicly available information.

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 and Industry Affairs, Americas
Refinitiv

Message

From: Christopher Mohr [REDACTED]
Sent: 12/6/2019 9:29:36 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Sara DePaul [REDACTED]; Christopher Mohr [REDACTED]
Subject: Regulatory Comments Attached
Attachments: SIIA Comments re CCPA regs 6 DEC FNL FILED.pdf

Greetings:

Attached please find the comments of the Software and Information Industry Association on the proposed regulations.

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
Direct: [REDACTED]
Mobile: [REDACTED]

December 6, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, California 90013
Via Email: PrivacyRegulations@doj.ca.gov

Re: SIIA Comments on the Proposed Text of the CCPA Regulations

On behalf of the Software & Information Industry Association (SIIA), thank you for the opportunity to submit comments regarding the proposed text for the regulations implementing the California Consumer Privacy Act Regulations (CCPA). SIIA and our member companies support the CCPA's intention to provide consumers with more awareness, control, and choice over the dissemination of their personal information. We thank the Office of the Attorney General for its leadership and diligence in developing proposed regulations that are measured, sensible, and provide industry with needed guidance on how to implement the CCPA.

As background, SIIA is the principal trade association of the software and digital content industry. We represent over 800 companies that develop and market software and digital content for business, education, consumers, the Internet, and entertainment. Our members include software publishers, financial trading and investment services, and specialized and business-to-business publishers. A number of our member companies also provide services to children online and to schools to develop and deliver software applications, digital instructional content, online learning services, and related technologies. These members, often referred to as "edtech companies," work to support teachers and instruction, improve student learning, carry out various administrative operations, and improve school productivity.

The proposed regulations are particularly useful where they clarify the CCPA's legislative intent to provide consumers with meaningful notice, choice, and control over the collection and use of their personal information. For example, the proposed regulations provide a critical clarification regarding the obligations of service providers in section 999.314(a), by making it clear that a person or entity qualifies as a "service provider" if it "provides services to a person or organization that is not a business, and would otherwise meet the requirements of a 'service provider'" under the CCPA.

With this clarification, businesses that provide services to schools or other government agencies will be subject to the CCPA's service provider requirements. This includes edtech companies, which provide services critical to modern learning

in the classroom. For edtech companies, this proposed clarification appropriately alleviates the conflicting compliance obligations imposed by existing student privacy laws, including California's Student Online Personal Information Protection Act (SOPIPA). For more information on the compliance conflicts created by the CCPA on edtech companies without this clarification, please see our [December 26, 2018 letter to the Attorney General](#).

Nevertheless, we have a number of concerns with the proposed regulations, which we are grateful for the opportunity to bring to your attention. As a general matter, we are concerned about the constitutional issues raised by the statute and the proposed regulations. More specifically, we note that the proposed regulations run afoul of First Amendment principles in three important respects:

- First, the underlying statute has fatal constitutional defects that we urge the Attorney General to remedy in this proceeding. The CCPA unconstitutionally regulates information in the public domain including information sourced from research databases, directories, registries, news articles, books, unrestricted social media feeds, and any number of other general interest, media, or business-to-business publications available to the general public. The Attorney General has an opportunity to correct this constitutional defect using his authority granted by Cal Civ. Code 1798-185(a)(3) to promulgate regulations to "[e]stablish[] any exceptions necessary to comply with state or federal law. . . ." **To comply with federal constitutional law, we respectfully urge the Attorney General to use this statutory authority to draft an exemption for all publicly available information, whether made available by a government agency or a non-government source.**
- Second, section 999.305(d), which sets forth requirements for businesses that do not collect information directly from consumers, increases the burdens imposed by an already problematic statute in a particularly overbroad way. **To cure this constitutional infirmity, we recommend that the Attorney General strike section 999.305(d) from the proposed regulations.**
- Third, the proposed regulations do not adopt the CCPA's amended treatment of information contained in public records, which the legislature enacted pursuant to AB 874 in order to resolve significant First Amendment defects with respect to the CCPA's regulation of information in the public domain. **To account for this legislative change, which the Governor signed into law after the proposed regulations were released, the Attorney General should amend the definitions at section 999.301(d) and (e) to strike or clarify references to public records and government entities that could run afoul of the exemption for public records set forth in AB 874.**

Finally, our members have practical, operational concerns with several sections of the proposed regulations that impose unintentional compliance outcomes and difficulties without meaningfully advancing the CCPA's intention to expand

consumer choice and control. Our focus here is on sections 999.313(c)(4), .314(d), .315(c) and (f), and .316(a). As explained in more detail in Section II, below, we generally recommend line-item edits to these proposed provisions to clarify that they do not require overly burdensome compliance requirements.

I. The First Amendment and Privacy Regulation

A. The CCPA's Regulation of Public Domain Information Constitutes a First Amendment Violation that The Attorney General Can Cure by Exempting Information From Non-Government Sources

SIIA's members amass public domain information to provide research tools for a variety of socially valuable uses, such as law enforcement investigations, investigative journalism, identity verification, scientific and medical research, corporate due diligence, and finding missing witnesses, among other uses. The collection and publication of public domain information is protected by the First Amendment, which requires statutes and regulations to be carefully tailored so that they do not infringe freedom of speech guarantees. Such guarantees extend to a private company that, for example, creates databases of publicly available factual information. *See IMS Health v. Ayotte*, 564, U.S. 552, 570 (2011) ("the creation and dissemination of information are speech within the meaning of the First Amendment"), citing *Bartnicki v. Vopper*, 532 U.S. 514, 527 (2001) ("If the acts of disclosing and publishing information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct.") (other citations omitted).

During California's 2018-19 legislative session, SIIA shared with legislators a [memorandum from its outside counsel](#) regarding First Amendment problems raised by the CCPA as originally enacted. The memo detailed the way in which the statute was vague, overbroad, and content-discriminatory by regulating information in the public domain. In response to those First Amendment concerns, Rep. Irwin introduced AB 874, which unanimously passed both houses and was signed into law on October 11, 2019 – a day after the Attorney General released the proposed regulations.¹

¹ *See* Senate Judiciary Committee, [Bill Analysis](#) at 5-6 (recognizing "very real concerns" raised by the Mayer Brown memorandum); Assembly Committee on Privacy and Consumer Protection, [Bill Analysis](#) at 5 ("The concern that this bill seeks to address is that the CCPA's limitations on the use of publicly available information are vague and could run afoul of the First Amendment, which protects the right of individuals to disseminate information.").

AB 874 amended the provision specifying the “publicly available information” exempted from the definition of “personal information.”² Following the enactment of AB 874, the relevant portion of the CCPA exempting “publicly available information” states:

“Personal information” does not include publicly available information. For purposes of this paragraph, “publicly available” means 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.

Cal. Civ. Code 1748.140(o)(2).

AB 874 cures the CCPA’s First Amendment defect with respect to public domain information derived from public records. But the amended CCPA (and by extension the proposed regulations as currently drafted) still contain fatal First Amendment flaws because they regulate public domain information derived from widely available non-government sources, such as professional contact, credential and licensing details, biographical data, and other information drawn from registries, directories, websites, and news and social media channels.

However, the CCPA gives the Attorney General the authority to establish exemptions necessary to “comply with state or federal law.” *See* Cal. Civ. Code. 1798.185(a)(3). **SILA, therefore, respectfully urges the Attorney General to use that authority to promulgate a regulation that places the scope of the CCPA’s regulations within the bounds of the First Amendment. This can be done by expressly excluding from the regulation’s scope public domain information that is widely available from non-government sources.**

Unfortunately, in some instances, the proposed regulations take the existing constitutional problems with the CCPA and make them worse. In the absence of legislative action, these constitutional problems require regulatory adjustment even if the Attorney General uses his authority to exempt widely distributed media to cure the larger First Amendment issues created by the CCPA. We turn to these problems in the following subsections.

² AB 874, Bill History, available at https://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=201920200AB874.

B. The Attorney General Should Strike Section 999.305(d) in its Entirety In Order to Conform with the First Amendment

As proposed, section 999.305(d) of the regulations requires that a business that does not collect “information directly from consumers” must, *before* disseminating personal information, fulfill one of two conditions. First, the business may contact consumers directly and inform them that the business has personal information about them and provide them with a notice of their right to opt-out of the sale of their personal information. *See* Section 999.305(d)(1). Alternatively, the business must contact the source of the information to confirm that the source provided the consumers with a notice as required by the CCPA *and* obtain signed attestations from the “source of the consumer information” describing how the source gave the notice required by CCPA at the time of collection and including an example of the notice.” Failure to satisfy one of these two proposed requirements makes publication of the information unlawful, whether the CCPA would have otherwise permitted its dissemination or not.

SIIA’s members have a constitutional right to publish directories, registries and other important works that contain public domain information, whether that information comes from public records or publicly available non-government sources. For example, some of SIIA’s members sell online databases that index millions of articles covering subjects ranging from science and medicine to law and finance. These kinds of databases contain the author’s names and other information about the authors sourced from works published by different publishing houses.

The proposed regulation makes the publication and sale of the above information illegal – and exposes publishers to massive potential liability – in all circumstances unless they comply with section 999.305(d) by either contacting all of these authors to give a privacy notice required by the CCPA or obtain attestations that such notice was provided from the original source of the articles. This neither advances a compelling privacy interest, nor does it comport with our First Amendment guarantees to freedom of speech. Indeed, proposed section 999.305(d) goes even further than the statute, rendering *all* publication illegal, even if the CCPA’s substantive requirements would have otherwise permitted it. Section 999.305(d) exacerbates the CCPA’s First Amendment infirmities.

Finally, the conditions imposed by proposed section 999.305(d) will in many cases be impossible to satisfy. Take, for example, the situation in which a publishing house from which a library of journals is acquired has been absorbed or gone out of business or when the author of a work that is thirty or fifty years old cannot be found. This problem repeats itself across a variety of media, including directories of films, literary agents, or newspaper articles. If section 999.305(d) is promulgated as proposed, the State will, in effect, ban the publication of information in these

circumstances despite an obvious lack of tailoring to a colorable privacy interest. Although the State may in certain circumstances punish the publication of some information after its release, the state may not curtail First Amendment speech by a blanket ban on publication. **Section 999.305(d) should be stricken in its entirety.**

C. The Attorney General Should Revise the Definitions for “Categories of Sources” and “Categories of Third Parties” to Conform with AB 874 and the First Amendment.

The Attorney General’s proposed regulations were released to the public one day before AB 874 was signed into law by the Governor. Once AB 874 became law, information derived from lawfully made available records was exempted from the CCPA’s scope and, by extension, from any resulting regulations. While on balance, this does not affect the vast majority of the proposed regulations, it does call into question two definitions that could be interpreted to capture public record information that the legislature expressly excluded from the CCPA’s scope.

First, “Categories of sources” in section 999.301(d) is defined to include “government entities from which public records are obtained” as a type of entity “from which a business collects personal information about consumers.” As a result of AB 874, however, information derived from public records is not regulated by the CCPA. It is inappropriate both under the strictures of AB 874 and the First Amendment concerns that prompted it, for the proposed regulations to capture public record information by including government entities that publish such records in this definition. **We respectfully request that the Attorney General strike the reference to “government entities from which public records are obtained” from this definition.**

Second, the proposed regulation defines “Categories of third parties” to include “government entities” as a type of entity that does “not collect personal information directly from consumers.” **To avoid any confusion that this definition results in the proposed regulations drawing in government entities with respect to public records, it should either be stricken or clarified to conform to AB 874.**

We note that both of these definitions include the qualifier “personal information,” which technically constrains the extension of those definitions to account for the amended CCPA’s exemption of public records information. Nevertheless, both definitions can be interpreted to work around this exemption to draw in government entities with respect to public records for the proposed obligations elsewhere in the proposed regulations. This result is likely not intentional, but underlies why our recommendations to strike and/or clarify these aspects of the two defined terms is important to bring the proposed regulations

within the ambit of AB 874 and the First Amendment concerns it was passed to address.

II. The Attorney General Should Revise Several Proposed Provisions to Avoid Unintentional and Overly Burdensome Compliance Outcomes

Setting the above-described constitutional concerns aside, SIIA generally supports the proposed regulations, which update, establish, and govern the CCPA's standards. We have concerns with five proposed provisions, however, because they create overly burdensome operational problems for businesses and service providers subject to the CCPA. Those proposed provisions are: Sections 999.313(c)(4), .314(d), .315(c) and (f), and .316(a). Our comments below explain the compliance issues presented by these provisions and suggest revisions or clarifications that the Attorney General can make to avoid unintentional but burdensome compliance outcomes.

A. The Attorney General Should Clarify Proposed Provision 999.313(c)(4) To Meet Consumer Expectations for Data Portability

Proposed provision 999.313(c) clarifies the parameters for how a business must respond to a request to know from a consumer, including obligations for disclosures when a business cannot verify an individual and prohibitions on disclosing sensitive data. The latter point is addressed by proposed provision 999.313(c)(4), which outright bans a business from disclosing "a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers."

We agree that this provision is generally sensible given the sensitivity of the data, particularly if the business has not been able to verify the identity of the person making the request to know. We also note that it is sensible to outright prohibit the disclosure of passwords and security questions and answers. However, this prohibition is unlikely to align with some consumer's expectations. For example, medical, tax, and other forms that contain government identifiers may be sought by consumers to port such forms from one provider to use for another purpose (including to port to another provider). **Taking into account consumer expectations and that the CCPA does not expressly prohibit such disclosure, we recommend modifying the proposed provision to allow, subject to a verified request, an entity to consider the context and intent of the consumer's request, including portability, when determining whether to provide such data.**

A. The Attorney General Should Revised Proposed Provision 999.314(d) to either remove or clarify the word "maintains" and to clarify the meaning of "feasible"

Proposed section 999.315(d) clarifies the obligations of a service provider that receives a request from a consumer to know or delete personal information. The proposed provision requires a service provider in receipt of such requests to explain the basis for a denial, if one is made, and to inform requesting consumers that they should submit the request directly to the business that controls the data at issue. In addition, the service provider must, *when feasible*, provide the consumer with the contact information for the business. The obligations under this section are triggered when the service provider receives a qualifying consumer request regarding personal information that the provider “collects, *maintains*, or sells on behalf of the business it services.” (emphasis added)

The provision attempts to balance obligations between the service provider and the business while ensuring that consumers receive sufficient information to resubmit requests to know or delete to the appropriate entity (i.e. the business). We are concerned, however, that inclusion of the word “maintains” is vague and may capture situations in which a service provider “maintains” data on behalf of a business but does not have a right to access the data. A common example would be a cloud service provider, which likely maintains personal information on behalf of businesses that it is contractually obligated not to access. In these circumstances, it would be contractually impossible for the service provider to access the data to respond to a request to know or delete in order to assess a reason for the denial or to redirect the consumer to the appropriate business to which to submit the request.

To address these situations (and avoid forcing service providers to access data in contravention of contractual obligations), we recommend that the Attorney General revise this proposed section to clarify that service providers who “maintain” personal information on behalf of a business but do not have a right to access the data are not subject to this provision. This can be done by either striking the word “maintains” from this provision or by clarifying that the term is not intended to reach situations where personal information is maintained without a right of access by a service provider. The latter fix can be achieved by revising 999.314(d) to state:

- If a service provider receives a request to know or a request to delete from a consumer regarding personal information that the service provider collects, ***maintains with a right to access***, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial.

In addition, the proposed provision requires a service provider to give the requesting consumer the contact information for the relevant business when it is feasible to do so, but the proposal leaves it unclear when it may be infeasible to do so. For instance, would a feasibility determination rest on whether a service provider

would have to deploy significant resources to identify the business? Or would a feasibility determination come down to a technical ability to identify the business? What if the business is prohibited by a court order or a legal obligation from identifying the business? **To help businesses make these determinations, we respectfully suggest that the Attorney General revise this provision to clarify the meaning of feasibility and to ensure that businesses can rely on an infeasibility determination when identifying a business requires them to deploy significant and disproportionate resources or they are otherwise legally barred from doing so.**

B. The Attorney General Should Strike Proposed Section 999.315(c)

Proposed section 999.315(c) addresses consumer requests to opt-out of the sale of their personal information by obligating businesses that collect such information online to treat user-enabled privacy controls as a valid request to opt-out for the browser or device from which the request is sent, or from the consumer (if known). It is unclear if this provision is intended as a *de facto* amendment to the California Online Privacy Protection Act to export that law's Do Not Track requirements into the CCPA, or if it is merely intended to incentivize the development of new technological solutions to facilitate these requests. We respectfully suggest that if it is the former, it would be helpful for the Attorney General, at a minimum, to explicitly reference the Do Not Track to facilitate compliance. But even with this fix, large scale operational concerns remain that render this proposed provision harmful to consumer choice and unduly disruptive to business without a concomitant benefit to consumers.

This is because the proposed provision creates several unintended policy outcomes. First, it weakens rather than strengthens consumer choice and control by creating a legal assumption that the browser-based user-enabled privacy controls, like do not track, are equivalent to an opt-out. Second, because the proposed regulations do not require businesses to verify the identity of a consumer making an opt-out request, it will be incredibly difficult, if not impossible, for businesses to ascertain the identity of a consumer for purposes of operationalizing these requests as an opt-out request. The proposed provision's requirements for business to exercise the opt-out at the browser or device level do not help because it will result in overinclusive opt-outs. Take, for instance, a large company that uses a single IP address across the devices used by its thousands of employees. Under proposed provision section 999.315(c), business will have to opt-out all information associated with the IP address of that company if even one personal within the company utilizes a user-enabled privacy control.

These outcomes are unduly and wrongly disruptive to businesses subject to this regulation. Worse, these outcomes vitiate consumer control and choice, a key

tenant of the CCPA. **To avoid this, the Attorney General should strike this provision.**

C. The Attorney General Should Clarify Section 999.315(f)

Proposed section 999.315(f) seeks to ensure that consumer opt-outs are fulfilled downstream by requiring businesses to notify all third parties to whom they have sold the information within 90 days prior to the receipt of the consumer request to opt-out. Businesses are required to instruct third parties to not further sell the information, and to inform the consumer when this obligation has been fulfilled. We have several concerns with this provision.

First, the proposed provision imposes a significant and unfair compliance risk on businesses by requiring downstream notifications while mandating opt-outs without requiring verifiable consumer requests. Because businesses must honor an opt-out request even when they cannot verify a consumer's identity, it will be difficult in many situations to execute a meaningful downstream opt-out consistent with the obligations imposed by this proposed provision. **This risk can be alleviated by modifying the proposed provision to clarify that businesses are only obligated to follow its strictures when the consumer making the opt-out request can be identified.**

Second, the proposed provision requires businesses to notify "third parties" and instruct them to not further sell the personal information. The CCPA, however, defines third parties to mean persons with whom the business does not have a written contract. In other words, third parties in the CCPA context are not subject to the instructions of the business. It is unclear, therefore, how a business's instruction to a third party could be considered mandatory. Additionally, this ignores the "use" contexts of data that consumers will want to preserve even when opting-out with respect to one use. For example, a consumer's opt-out to stop the sale of information for marketing purposes does not mean the consumer wants their information to be removed for other non-marketing uses. For example, many sole proprietorships have built a web presence across the internet in the form of positive reviews, a positive financial history and other reputational benefits. Such information is personally identifiable as it can be traced back to a specific individual. The sole proprietor may wish to have their contact information removed from marketing lists but that does not mean they want their online reputation to disappear. **These unintended outcomes can be alleviated by modifying the proposed provision to refer to "service providers" instead of "third parties" and to clarify that the downstream notification obligations are limited to the same or similar use contexts that generated the opt-out.**

D. The Attorney General Should Revise Section 999.316(a) to Require a Single Opt-In

Proposed section 999.316(a) requires a double opt-in when a consumer is requesting to opt-in to the sale of information after exercising their opt-out right. While we agree that opt-in is the appropriate standard, we are concerned that the double opt-in may override consumer choice by signaling that they are doing something wrong by exercising an opt-in. A consumer should be free to exercise their opt-in without barriers designed to signal that their choice is wrong or risky, when that is not the case. **We, therefore, respectfully suggest that the Attorney General revise this provision to require a single affirmative opt-in consent for consumers who wish to opt-in to the sale of their information following an opt-out.**

III. Conclusion

We thank the Attorney General for this opportunity to provide our comments and suggested edits, and for considering our concerns as you work toward finalizing these proposed regulations. If you have any questions or concerns regarding our comments, please contact us at your convenience.

Respectfully submitted,



Christopher A. Mohr, Vice President for Intellectual Property and General Counsel
Sara C. DePaul, Senior Director, Technology Policy
 Software & Information Industry Association
 1090 Vermont Avenue NW, 6th Floor
 Washington D.C. 20005
www.siaa.net

Message

From: Brandon Dennison [REDACTED]
Sent: 12/5/2019 10:03:28 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: SchoolsFirst Federal Credit Union - Proposed CCPA Regulations Comment Letter
Attachments: Proposed CCPA Regulations Comment Letter.pdf

Good Afternoon,

Attached are the SchoolsFirst Federal Credit Union's comments on the Department of Justice's notice of proposed rulemaking concerning the California Consumer Privacy Act. We thank you for the opportunity to comment.

Best Regards,

Brandon Dennison, CUCE
Compliance Specialist
Operations Compliance
SchoolsFirst Federal Credit Union
[REDACTED]



November 26, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: Proposed California Consumer Privacy Act Regulations

Dear Privacy Regulations Coordinator:

I am writing on behalf of SchoolsFirst Federal Credit Union (SchoolsFirst FCU), which serves school employees and their family members in California. We have more than 900,000 Members and over \$16 billion in assets. SchoolsFirst FCU appreciates the opportunity to comment on your Notice of Proposed Rulemaking on Proposed California Consumer Privacy Act ("CCPA" or "the Act") Regulations. We have outlined our feedback and recommendations below.

CCPA Applicability

Section 3, Title 1.81.5 of the CCPA outlines the applicability of the Act and its definition of "business." It includes "(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 satisfies one or more of the qualifying thresholds."

We request that the Attorney General clarify that the CCPA does not apply to not-for-profit organizations, such as credit unions, since they are not specifically included in the definition of "business" and do not meet the criteria provided of being "organized or operated for the profit or financial benefit of its shareholders or other owners."

Unlike for-profit businesses, credit unions are not-for-profit financial cooperatives that are structured to operate on behalf of our Members, and not for their profit. Not-for-profit organizations would be heavily burdened in offsetting the large financial impact of the operational costs to meet the requirements of the CCPA and implementing Regulations.

Definition of "Sell, Selling, Sale, or Sold"

As outlined in the Act, "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." We believe that the term "*other valuable consideration*" is ambiguous and subject to interpretation. We are requesting a more succinct definition to provide clarification and ensure businesses are clear on what would fall under this classification.

Model Forms and Disclosures

The federal Gramm-Leach Bliley Act and the California Financial Information Privacy Act provide model forms for businesses to utilize for accuracy and consistency of what the laws and regulations require. However, the proposed CCPA Regulations currently do not include such forms. We recommend model forms and disclosures be included in the final Regulations and made available to businesses to ensure compliance with the requirements set forth.

CCPA Effective Date

The CCPA is effective January 1, 2020. However, the proposed implementing regulations were not issued until October 11, 2019. Given how general the statute is and the many questions and concerns that have been raised, the CCPA effective date should be extended.

Covered business should be given adequate time to understand the requirements of the statute and the final regulations prior to designing and implementing comprehensive compliance solutions. SchoolsFirst requests that the Attorney General delay the effective date to one year after the final implementing regulations are issued. This will eliminate the uncertainty surrounding how to comply with the Act.

CCPA and the Regulations

As proposed, the requirements of the CCPA currently reside in two areas; in the CCPA and the implementing Regulations. Businesses must utilize both sources to ensure they are complying accordingly. The information included in the Regulations provide the clarification needed in order to comply with the requirements of the Act.

We request that the Regulations include the necessary CCPA content to ensure businesses are following the requirements without the need to use two sources and to minimize the risk of not capturing all the necessary information to execute the Act as proposed. We thank you for the opportunity to comment on the proposed Regulations. We believe that our feedback and recommendations will allow us the flexibility to better assist and serve the needs of our Members.

Sincerely,



Bill Cheney,
President/CEO
SchoolsFirst Federal Credit Union

Cc: Credit Union National Association (CUNA)
California/Nevada Credit Union League (CCUL)

Message

From: MacGregor, Melissa [REDACTED]
Sent: 12/6/2019 12:30:35 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Chamberlain, Kim [REDACTED]; [REDACTED]; [REDACTED]
Subject: SIFMA Comment CCPA Rules 12-6-19
Attachments: SIFMA Comment CCPA Rules 12-6-19.pdf

Please see the attached letter filed in response to the request for comments on the proposed rules to be promulgated under the Consumer Privacy Act.

Thank you.

Melissa MacGregor
Managing Director and Associate General Counsel
1099 New York Avenue, NW
Washington, DC 20001
Office: [REDACTED]
Fax: [REDACTED]
www.sifma.org



December 6, 2019

VIA EMAIL TO: privacyregulations@doj.ca.gov
The Honorable Xavier Becerra
Attorney General, State of California
1300 I Street
Sacramento, CA 95814

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: Proposed California Consumer Privacy Act Regulations

Dear Attorney General Becerra,

The Securities Industry and Financial Markets Association (SIFMA)¹ appreciates this opportunity to comment on the proposed California Consumer Privacy Act (CCPA) regulations.

I. Executive Summary

In promulgating regulations under the CCPA, it is important that the Attorney General's office endeavor to create clear and consistent rules that businesses can meaningfully rely on in their efforts to comply with the CCPA and provide consumers with additional clarity about the collection, use, and sharing of their personal information. To that end, SIFMA requests that the Attorney General's office delay enforcement of the CCPA until January 1, 2022, to allow for businesses to appropriately implement the complex systems of accepting, verifying, and responding to consumers' requests in accordance with the regulations' requirements.

¹ SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate for legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

In addition, SIFMA recommends that the regulations seek to enhance the clarity of ambiguous language in the CCPA in order to ensure the efforts to increase privacy do not come at the cost of the security of consumer personal data. Within the regulations, SIFMA requests that any requirements related to the disclosure of information take into account dual goals of enhancing clarity for consumers and protecting businesses' free speech interests in the use of data for internal business purposes. In addition, the regulations should seek to provide businesses with flexible options for complying with consumer requests in a way that satisfies both the consumers' interest in protecting their personal information and the business's legitimate business interests. We describe our specific concerns and recommendations in more detail in the sections that follow.

II. Enforcement of the regulations should be delayed until January 1, 2022.

The CCPA states that the Attorney General should "adopt regulations" by July 1, 2020, but does not mandate an effective date for those regulations; instead it states that the earliest date that such enforcement could be brought is "six months after the publication of the final regulations [...] or July 1, 2020, whichever is sooner."² The Attorney General thus has discretion to delay enforcement of the regulations until a later date. California Government Code sets forth a default timeline establishing when regulations become effective.³ The default rule states that it does not apply if the "effective date is specifically provided by the statute" or if a "later date is prescribed" in the regulation.⁴ As the CCPA does not specifically provide an effective date, the California Attorney General has the authority to provide such a date in the regulations. We encourage the Attorney General to delay that enforcement until January 1, 2022, which would allow for a two-year grace period beyond the CCPA's January 2020 effective date and would provide companies an additional eighteen months to prepare for compliance, after the July 1, 2020 enforcement date. This would be somewhat less than the amount of time that the European Union provided companies to prepare for the EU's General Data Protection Regulation ("GDPR"), which developed from a well-established body of EU data protection law, but it would at least provide businesses with a reasonable opportunity to read the final regulations and develop systems in reliance upon clear guidance. The alternative has forced companies to try to anticipate what the final regulations might require even though the regulations will, at best, be issued days before the CCPA's effective date.

The CCPA itself provided an 18-month period between its passage and its effective date in recognition of the complexity of implementing the statute's numerous requirements. The draft regulations are similarly extensive and detailed in ways that could not reasonably be anticipated from the text of the CCPA. Implementation of many of the provisions in the draft regulations will require businesses to revise back-end processes. For example, the regulations necessitate the redrafting of many disclosures, notices, and

² CCPA, CA Civil Code § 1798.185(a).

³ Cal. Gov't. § 11343.4.

⁴ Cal. Gov't. § 11343.4(b).

communications. According to the draft regulations, those redrafted disclosures must include details about data collection and use that will require extensive development work to determine and convey meaningfully to consumers.

In addition, once the regulations are final, businesses will be required to revise, and possibly redraft, and implement additional content training with an expanded target audience and will need to establish channels for distributing information to consumers and accepting access and deletion requests. Attempting to rush this development work could introduce substantial anti-consumer risks, including security, fraud, and identity theft risks. Time is needed to establish and implement procedures for appropriately receiving and verifying requests, and additional personnel may need to be trained in accepting requests and documenting this verification process. If not done properly, this could lead to significant risk that consumer information is released to an unauthorized person who makes an invalid request. Testing and validation of processes is needed before these channels are opened to the public to mitigate the risk of fraud and identity theft. To reduce risk, this testing and validation should not be rushed.

While businesses are establishing robust verification procedures to meet the statutory text's effective date of January 1, 2020, they may need additional time to rework those procedures to comply with provisions in the regulations, such as § 999.325, which requires verifying identity with a high degree of certainty, including by obtaining and maintaining a record of a declaration signed under penalty of perjury, in lieu of—or possibly in addition to—comparable processes already planned. These new processes will take time to implement properly. To allow for that implementation, the Attorney General should either specify a later enforcement date in the regulation text, or, at a minimum, exercise its enforcement discretion by allowing for a grace period that would hold any enforcement actions until at least two years after the effective date of the CCPA and should withhold enforcement for any violations that occur before January 1, 2022.

III. The draft regulations should promote the goal of protecting consumers' personal information.

SIFMA and its members are strongly committed to the protection of consumer data, privacy, and security, and its members have operated for years under the well-established protections of the Gramm-Leach-Bliley Act Safeguards Rules. While the industry recognizes that the goal of the CCPA is to provide greater transparency to consumers, no regulations should be issued that would promote transparency at the expense of harming the security of consumer data. The CCPA, Civil Code § 1798.185(a)(7) requires that, when establishing rules and procedures to facilitate consumers' ability to obtain information, the Attorney General take into account security concerns and available technology. Several of the proposed regulations, as drafted, do not properly account for the security risks that they create. These proposed regulations should be revised or struck as described below.

- a. The regulations should not require detailed disclosure of the process used to verify consumer requests or the reasons that requests appear fraudulent

The proposed regulations require detailed disclosure of the process a business uses to verify consumer requests for access to or deletion of personal information, including any information the consumer must provide to verify the request.⁵ This requirement compromises the security of consumer information by requiring businesses to disclose to potential bad actors the methods that they can use to maneuver through the verification process and fraudulently obtain personal information about another consumer. If businesses are allowed to employ risk-based verification measures as needed, businesses will be better able to protect consumers' privacy and avoid such security incidents.

Similarly, the proposed regulations require that businesses who believe that requests to opt out of sales are fraudulent can deny the request but must inform the requesting party with an explanation of why it believes the request is fraudulent.⁶ Providing such an explanation places consumers' personal information at risk for two reasons. First, the group to whom the information provided—parties that have submitted requests that appear fraudulent—is likely to contain a high proportion of bad actors seeking to use deception to gain access to consumers' personal information without the consumers' authorization. Second, the information that the regulations require businesses to provide—an explanation of why the business believes the request is fraudulent—will only serve to educate the potential bad actor on how to create a more convincing request and defraud the verification system in the future.

These requirements should be struck from the final regulation entirely or the regulations should clarify that description of the process of verification and the determination that a request is fraudulent should be limited to a high-level summary.

- b. Process for deletion of personal information

With regard to the procedures for accepting and executing requests for deletion of personal information, the regulations provide detailed requirements that are not mandated by the text of the CCPA and could hurt businesses' ability to protect consumer information. Section 999.312(d) of the proposed regulations requires a two-step process for deletion requests. It should be eliminated to allow businesses to make risk-based determinations about deletion requests that would better protect consumer information. Similarly, § 999.313(d)(2) of the proposed regulations limit the methods of deletion that businesses may use to comply with consumer requests. This should be deleted to allow businesses to implement additional measures to address deletion requests that would better meet the consumer protection goals of the statute.

⁵ Proposed CCPA Regulations §§ 999.308(b)(1)c, 999.308(b)(2)c, and 999.313(a).

⁶ *Id.* § 999.315(h).

Section 999.312(d) of the proposed regulations requires a two-step process for deletion but does not clearly describe what that process should entail. This provision should be deleted or clarified so that no “re-authentication” is necessary for consumers who have already authenticated their identity. If a two-step requirement is included in the regulations, the proposed regulation should state that businesses are not required to authenticate a consumers’ identity twice. Instead businesses are required to confirm a second time whether consumers would really like their personal information deleted before deleting the information. The lack of clarity in the current provision could result in both over-deletion—because identity was authenticated twice, but the consumer did not have the opportunity to confirm that they wanted their information deleted before it was erased—and under-deletion—because businesses could not determine a workable method for the double authentication process. Both over- and under- deletion could create a risk to consumers’ personal information, either by businesses erasing information that is unrecoverable against the consumers’ wishes or by businesses maintaining information that consumers wanted erased that could be involved in future security incidents. Clarifying this requirement would result in more consistent application and better compliance with the consumers’ wishes about the handling of their personal information.

In addition, the proposed regulations limit businesses to three prescribed options for handling deletion.⁷ Limiting businesses to three options for deletion of information goes well beyond the CCPA requirement that businesses comply with consumer requests to have their personal information deleted. It imposes the three options without consideration of cost or other potential measures that businesses could employ. In addition, it prevents businesses from employing risk-based measures to determine the most appropriate method of deletion on a case-by-case basis. For these reasons, this provision should be deleted.

Finally, the proposed regulations require that information be deleted from archived or backup systems.⁸ For financial institutions, such deletion would affect the ability of the business to maintain the necessary systems in a manner that complies with FDIC/FFIEC/SEC requirements for business continuity planning. In addition to such conflict with existing federal requirements, the deletion could create great risk for consumers. This requirement should be eliminated.

c. The regulations should clearly identify when it is too risky to disclose information in response to a data subject request.

The proposed regulations state that businesses “shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer’s account with the business, or the security of the business’s systems or networks.”⁹ The terms “substantial” and “unreasonable” create ambiguity that

⁷ *Id.* § 999.313(d)(2).

⁸ *Id.* § 999.313(d)(3).

⁹ *Id.* § 999.313(c)(3).

suggests that, if a business determines that there is an articulable security risk from the provision of certain information, it would still be allowed to provide that information if the business's perception of the risk is insubstantial or reasonable. This ambiguity could lead to second guessing of business decisions and could cause businesses to disclose information in response to requests that could potentially place more consumers' privacy at risk.

We would recommend either (1) striking the terms "substantial" and "unreasonable" (so that the provision reads: "A business shall not provide a consumer with specific pieces of personal information if the disclosure creates an articulable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks."); or (2) replacing the word "and" before unreasonable with "or" (so that the provision reads: "A business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, or unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks.").

IV. The regulations should clarify ambiguous provisions in CCPA.

In an effort to provide maximum transparency and foster smoother and more consistent implementation of the CCPA across businesses, the regulations should clarify certain points of ambiguous text in the CCPA.

First, the regulations should specify that the AB 1355 amendment to Civil Code § 1798.145 (which exempts personal information transferred in the course of certain business communications or transactions, where the consumer is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, non-profit, or government agency) applies in the case of persons engaged in transactions in the role of institutional investors, trustees, partners, employees, beneficiaries, or other natural persons associated with financial accounts that are held in the names of institutions, partnerships, businesses, trusts, and estates. Currently, the CCPA's line between natural persons and estates, trusts, sole proprietorships, partnerships, etc. is ambiguous. The federal Gramm-Leach-Bliley Act as well as several other federal statutes established a clear line that transactions are properly considered consumer transactions when they are "for personal, family, or household purposes." See, e.g., 15 U.S.C. §§ 1692a(5), 2301(1), 6809(9). That same approach is respected in California law, Civil Code § 1791(a)(defining "Consumer goods" as a product ". . . used, bought, or leased for use primarily for personal, family, or household purposes . . ."). The CCPA should reflect this clear, commonsense division between a natural person acting as a consumer and a natural person acting as part of business. Accordingly, all financial information about natural persons gathered by a financial institution for "personal, family, or household purposes" is within Civil Code § 1798.145(e), and all personal information that is gathered by a financial institution for reasons other than "personal, family, or household purposes" should be within the ambit of the AB 1355 amendments for business interactions.

Second, the regulations should provide a non-exhaustive list of situations in which requests from a consumer could be considered manifestly unfounded or excessive, allowing businesses to charge a reasonable fee or refuse to act on the request, under Civil Code § 1798.145. Such examples should include requests that would require the business to expend a disproportionate amount of time, effort, and cost to ascertain the information that the consumer has requested or to provide the information to the consumer in a format that does not inadvertently reveal the personal information of another consumer in the process. In particular, the regulations should clarify that businesses are allowed to charge a reasonable fee or refuse to act on requests for hard copies or unstructured data. Providing clarity on this point would further the goal of protecting reasonable requests and would help protect consumer information from incidental exposure by a business.

Third, the regulations should define revenue, within the definition of “business” in the CCPA, Civil Code § 1798.140, as limited to revenue that is sourced from California. Such a clarification would be consistent with the Impact Assessment that was released along with the proposed regulations, which is calculated based on California Gross State Product and is not based on revenue from other states or international jurisdictions. Companies with small California operations but substantial operations in other areas would not be likely to process material amounts of personal information about California residents.

Fourth, the regulations should exclude from the definition of “sale” that is provided in Civil Code § 1798.140 all of the items that are subject to the general exceptions in 15 U.S.C. § 6802(e), such as disclosures of data related to servicing private label accounts, securitizations, transfers of servicing rights, provision of information to insurance rate advisory organizations, and in connection with the sale, merger, transfer, or exchange of the relevant financial institution. These exceptions are vital to the functioning of the secondary market activity that provides capital for consumer financial products and services and are subject to extensive federal oversight. It will only serve to confuse consumers if these secondary market activities are included within the definition of “sale” because the functioning of these markets can be incredibly complex and is far removed from the privacy interests that the CCPA seeks to protect.

Fifth, the regulations should clarify the definition of personal information for the purposes of data subject access requests (“DSARs”). The CCPA, as amended, defines “personal information” as information that “identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” However, the amended CCPA explicitly excludes from the definition of “personal information” any consumer information that is “deidentified.” The CCPA defines “deidentified” information as that which “cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer,” with the definition of consumer limited only to natural persons – and not a device. Because device identifier information can only reasonably be linked to a device, it should be excluded from the universe of personal information that businesses are required to provide or delete in response to DSARs. The inclusion of “device” identified information rests on the implicit presumption that devices are

surrogates for persons, but many devices are shared devices. Treating data from a shared device as data from a personal device could harm other unknowing users of that device. This is even more concerning because the users of shared devices are often those who do not have the economic means to own their own devices and may be the least familiar with the privacy and security challenges of using a shared device. Eliminating device identifier information from the universe of DSAR information would protect these shared-device using consumers and enable businesses to feel confident that they are providing information to the correct consumer without infringing on the rights of other individuals. For example, the device or browser in a public library may be used by several different consumers. If one of those consumers requested the “personal information” from a business that was connected to that device identifier, it would return information on several different consumers, which would not serve the purpose of providing consumers with more clarity about how their personal information is being used and indeed could compromise the privacy and security of the other users of that shared device.

V. The regulations should require disclosures that would provide consumers with a meaningful, comprehensible explanation of how their personal information is used and how they can exercise their rights with regard to their personal information without imposing a disproportionate burden on businesses seeking to comply with the regulations.

Several of the proposed regulations impose requirements for what must be disclosed to consumers, both in the privacy policy and in responses to consumer requests, which go above and beyond the requirements spelled out in the text of the CCPA. Many of these requirements will result in disclosures that are longer and more overwhelming and confusing to consumers. These verbose disclosures would frustrate the CCPA's goal of providing consumers with clarity about how their personal information is used and how they can exercise their rights with regard to their personal information. The proposed regulations should be modified to require only the disclosures necessary to provide consumers with meaningful information without otherwise compromising the security of the process or disproportionately burdening businesses who are trying to provide clarity to consumers.

a. Disclosures regarding the collection, use, and sharing of personal information

Sections 999.305(b)(2), 999.308(b)(1)d.2, 999.313(c)(10) address the detail with which businesses must describe the collection, use, and sharing of personal information. Those provisions require that the business specify the categories of information collected from a list provided in the CCPA, along with, for each separate data category, the sources from which the information was collected, the business purposes for which the information is used, the categories of third parties to whom the personal information may be disclosed, and the business purposes for which the information is disclosed. When listing these categories, businesses are instructed to select from eleven categories of personal information, a proposed minimum of three source types, and seven third party types, along with several possible uses of personal information. This information is too dense and detailed to include in a privacy

notice and could result in many dozens or of different combinations of this information, resulting in many additional pages of a privacy notice. This provision would be a large administrative burden on all businesses, and a mechanism by which businesses could be subject to large monetary penalties based on an error in judgment or record keeping, without meaningfully adding to consumers' understanding of how their personal information is used in shared. Rather it could cut against that understanding and cause more confusion.

The text of the CCPA does not require this information be provided in such a detailed fashion. Instead, the text of the CCPA can be interpreted to state that information on the categories of sources, business purposes, and third parties can be provided in the aggregate. The language of the regulations should be adjusted to be consistent with this understanding of the CCPA, which would provide for a disclosure that was much more accessible to consumers, easy to understand, and shorter, resulting in more consumers reading and comprehending from the disclosure how the business collects and uses their information. For example, the CCPA states that businesses should “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” but does not state that the purpose must be laid out for each category of personal information.¹⁰ Indeed, pairing purposes of use with the categories of personal information could result in more confusion and lengthy disclosures, especially where certain categories of personal information may be used for more than one business purpose. Such disclosures would be at odds with the proposed regulation’s requirement in § 999.305(a)(2) that notice be “designed and presented to the consumer in a way that is easy to read and understandable to an average consumer.”

b. Disclosures regarding the business or commercial purpose

Both the CCPA and the regulations require that businesses disclose the business or commercial purpose for collecting or selling personal information.¹¹ The regulations should clarify that the potential business purposes for collection of the information could go beyond the seven options outlined in the CCPA definitions.¹² Consistent with the U.S. Supreme Court’s decision in *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011), companies have a commercial free speech interest in their use of data. To balance the free speech interest and the resulting heightened judicial scrutiny, the regulations must use the least restrictive means of accomplishing their goal. Businesses may have legitimate interests in collecting personal information for internal uses that go beyond the seven uses provided in the CCPA definitions. The restriction of those internal uses of data to a limited set of use options does not further the government’s interest in preventing the sale of data.

¹⁰ CCPA, CA Civil Code § 1798.100(b).

¹¹ *Id.* § 1798.110(c)(3); Proposed Regulations § 999.305(b)(2).

¹² CCPA, CA Civil Code § 1798.140(d).

c. Disclosure of the right to request deletion of personal information

Section 999.308(b)(2)(a) of the proposed regulations requires that businesses explain that consumers have a right to request the deletion of their personal information that the business collects or maintains. This language is broader than the CCPA requirement, which states that consumers have the right to request that businesses delete personal information that “the business has collected from the consumer.”¹³ The regulation language should be revised to comply with the CCPA as follows: “Explain that the consumer has a right to request the deletion of their personal information collected by the business from the consumer.”

d. Disclosures in response to consumer requests

Once consumers seek to exercise their rights, the proposed regulations require that businesses provide extremely detailed, personalized information. In response to access requests, businesses providing information must do so in an individualized form,¹⁴ and businesses who do not provide specific pieces of information must explain the basis for that denial.¹⁵ Similarly, in response to deletion requests, the proposed regulations require businesses that delete information to disclose the manner in which they deleted data from among the three options provided in the draft regulations¹⁶ and businesses that do not delete all or some information to inform the consumer of the basis for the business’s denial of the deletion request, including any statutory and regulatory exceptions.¹⁷

The requirement to provide such detailed, individualized information in response to subject requests imposes a significant administrative burden and cost on businesses and conflicts with federal and state laws. We recommend that these provisions be deleted or changed to allow for a more general statement of denial or disclosure of information.

e. Disclosures regarding financial incentives

The proposed regulations also require much more detailed disclosures than the CCPA text contemplates with regard to financial incentives.¹⁸ The CCPA text requires that businesses not discriminate against consumers for exercising their rights under the CCPA, and it states that businesses may offer financial incentives but must notify consumers of the incentives. As a threshold matter, the definition of “financial incentive” in the proposed regulations is overbroad and includes programs, benefits, or offerings for the “disclosure, deletion or sale” of personal information. This definition extends beyond the language in CCPA and should be aligned more closely with the definition of financial incentive in the CCPA. In

¹³ *Id.* § 1798.105(a).

¹⁴ *Id.* § 999.313(c)(9).

¹⁵ *Id.* § 999.313(c)(5).

¹⁶ *Id.* § 999.313(d)(4).

¹⁷ *Id.* § 999.313(d)(6)a.

¹⁸ *Id.* § 1798.125.

addition, where financial incentives do exist, the proposed regulations impose significant additional obligations, including requiring that businesses offering financial incentives disclose detailed information about how they determine the value of the consumers' information and how they justify the incentive.¹⁹

Disclosure of such information could result in the revelation of trade secrets, pricing strategies, or other confidential business information that could result in a host of detrimental competitive impacts. The CCPA, Civil Code § 1798.185(a)(3), states that the Attorney General must adopt regulations that establish, among other things, "exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights." The current proposed draft regulations do not address the protection of trade secrets or intellectual property rights. This oversight should be resolved in future drafts, and provisions like this one, which conflict with those rights, should be removed.

Such a requirement could cause an unconstitutional regulatory taking of trade secrets by forcing their disclosure. Moreover, as this measure was not contemplated by the CCPA text and there has been no study of the costs or implications of such disclosures, this provision should be struck from the proposed regulations.

f. Disclosures regarding CCPA-related metrics

Finally, sections 999.308(b)(8) and 999.317(g)(1) require that businesses that buy, receive, sell, or share personal information of four million or more consumers annually for commercial purposes, compile and share CCPA-related metrics in the annual privacy notice. This obligation is not related to any CCPA provision which would authorize it but instead appears to be original to the regulations. Moreover, the four million trigger has no basis in anything in the CCPA and is not tied to any study of the costs associated with the compilations of these statistics. These provisions are thus arbitrary and beyond the regulatory authority of the Attorney General and would impose a significant administrative burden and cost on businesses. We recommend striking both sections from the proposed regulations.

VI. The regulations should propose workable methods for opting out of the sales of personal information.

a. Treatment of browser settings as opt-out

The proposed regulations, in Section 999.315(c), require that businesses that sell personal information should treat any "user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request" to opt out of the sale of their personal information. While SIFMA supports

¹⁹ *Id.* § 1798.125.

the requirement that businesses honor a consumer's request to opt out of sales, this method for opting out does not offer a reasonable approach. First, it is not clear that any browsers currently have a setting that allows consumers to select that they would like to opt out of the sales of their personal information. Instead, various internet browsers have introduced plug-ins that purport to allow consumers to signal their intention that websites not track their information. Browser plug-ins and privacy settings are not consistent across browsers and are difficult to connect to a known consumer. Indeed, a consumer that opts-out with one browser may then use a different device without an opt-out, leaving the company with conflicting and ambiguous indications of intent. For this reason, businesses have found implementation of browser settings like "Do Not Track" difficult and have instead asked consumers to indicate this directly.

The CCPA already provides a clear method for consumers to make that wish known by requiring that any business that sells information post a clear "Do Not Sell My Personal Information" in several key locations. Any user that wants to opt out of such sales will be notified and have the opportunity to do so. They will not, therefore, be deprived of the opportunity to exercise this choice by removing the requirement in § 999.315(c) and the corresponding provision in § 999.315(g), which states that browser settings should be interpreted as direct consumer requests and not requests through authorized agents. For clarity and consistency, these provisions, which were not contemplated by the text of the CCPA, should be removed.

b. Treatment of unverified deletion requests as opt-out

Similarly, Section 999.313(d)(1), which requires businesses that cannot verify the identity of a consumer making a deletion request to treat such requests as requests to opt out from the sale of personal information could have the negative consequence of opting out consumers who do not wish to opt out of sales. The verification process is in place to confirm that the right consumer's personal information is affected. If the consumer cannot be verified, the business cannot reasonably be expected to know which consumer should be opted out of the sale of information. This could lead to businesses opting out the wrong consumer and infringing on the rights of consumers who choose not to opt out from sale, but would prefer to continue to receive the benefits that may come from opting in to the sale of information, such as receiving more relevant advertising. For this reason, this provision should be struck, as it denies consumers meaningful choice about how their information is used and shared.

VII. The regulations should allow for reasonable methods for businesses to inform consumers of uses of information and should not require explicit consent for uses that are compatible with the legitimate interest of the business and are reasonably foreseeable to the consumer.

a. Notice provided at or before collection

The proposed regulations require that businesses do not collect personal information from consumers unless they give the consumer notice of the collection at or before the point of collection.²⁰ This language overlooks many scenarios in which subsequent notice may be permissible and where delivery of the notice at or before collection is impracticable and would delay meeting the consumer's needs. For example, where a consumer requests and authorizes the collection on a voice call, it may not be possible to provide the consumer with the notice at that time. In such situations, the regulations should allow for collection of personal information with subsequent deliver of the notice where the consumer authorizes such collection.

b. Consent for secondary use of data

In addition, the proposed regulations require business to obtain explicit consent from consumers if the business uses the consumers' personal information for a purpose that was not previously disclosed in the notice that the business provided to consumers at or before the point of collection.²¹ This requirement is inconsistent with the text of the CCPA which states that consent for collection and use should be opt out. The language of the regulations should be modified to replace the explicit consent requirement with a requirement to provide consumers with notification of the secondary use of the data. Moreover, such notice should only be required for uses that are incompatible with the business purpose initially disclosed for which the personal information was collected or is not reasonably related to the product or service that the business provides. In such cases, where the new use is not reasonably foreseeable to the consumer, the collection should be allowed after the consumer receives a secondary notice of collection stating the new purposes for collection.

VIII. The regulations should allow for reasonable use of aggregate information by service providers.

The proposed regulations go beyond the provisions in the text of the CCPA that limit how service providers can use the information they receive. The regulations require that service providers do not use personal information that they receive from businesses or from a consumer's direct interaction with the service provider to provide services to any other person or entity.²² The proposed regulations allow for

²⁰ *Id.* § 999.305(a)(5).

²¹ *Id.* § 999.305(a)(3).

²² *Id.* § 999.314(c).

service providers to combine personal information from multiple businesses for use on behalf of those businesses, but only “to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.”²³ The proposed regulations therefore limit the use of aggregate information by service providers.

This provision is incongruent with the law itself. The CCPA definition of “personal information,” in Civil Code § 1798.140(o), explicitly states that “aggregate consumer information” is not “personal information.” We recommend striking the restriction against service providers’ ability to combine information from businesses, as this could have chilling effect on the provision of analytic, data science, or other research, reporting, and innovation that could have a net benefit for the businesses served by the service provider and their consumers. If specific examples are to be given, then the internal use of data to improve products and services and offer aggregated analytics and research should be recognized as a valid use.

All internal uses of aggregate data should be allowed. As explained above, companies have a commercial free speech interest in their use of data, in accordance with the U.S. Supreme Court’s decision in *Sorrell*, 564 U.S. at 552. Consequently, the CCPA regulations are subject to heightened scrutiny and must use the least restrictive means of accomplishing their goal. Restricting internal uses of data by service providers does not further the government’s interest in preventing the sale of data.

IX. The regulations should allow for the use of record-keeping information to meet legal obligations.

The proposed regulations require that businesses maintain records of consumer requests under the CCPA and prohibit businesses from using those records for any other purposes.²⁴ This blanket prohibition could conflict with other laws where businesses are legally required to provide such information. The regulations should be revised to allow businesses to use the information to meet legal obligations, including the use for the purpose of asserting a legal defense or defending against claims.

X. The regulations should protect the personal information of all household members equally.

The proposed regulations require that businesses who receive requests to access or delete information that pertains to a household by providing aggregate household information.²⁵ This practice was not contemplated by the CCPA. It raises several questions such as how to verify the individuals are in the same household, and it increases consumer privacy risks by potentially exposing information about one member of a household to other member(s) of the household. This is especially true in situations where

²³ *Id.*

²⁴ *Id.* § 999.317(e).

²⁵ *Id.* § 999.318.

roommates are unrelated and where one member of the household may wish to keep information secret from the other household member who is making the request. The regulations should clarify that nothing in this section requires or allows companies to violate the privacy of other household members when providing information to one household member.

XI. The regulations should provide clear guidance on your expectations for reasonable security and a safe harbor for those that meet those expectations.

The regulations currently do not address what information security measures are necessary to achieve a “reasonable” level of security. SIFMA suggest that the regulations include guidance about the types of processes and governance that your office would deem to be reasonable. It will be important that this guidance not attempt to dictate particular information security controls, but rather articulate the types of safeguards that are required, in much the same way as the Gramm-Leach-Bliley Act (“GLBA”) Safeguards Rule. For example, the regulations could specify the following types of safeguards required by the Safeguards Rule, as appropriate to the size and complexity of the business, the nature and scope of the business’s activities, and the sensitivity of any personal information at issue:

- Reasonable Administrative safeguards, such as designation of a security program coordinator, identification of risks, assessment of safeguards, training of employees, and appropriate vendor selection and oversight;
- Reasonable technical safeguards, such as risk and threat assessment, detection, prevention, response, and testing; and
- Reasonable physical safeguards, such as proper information storage and disposal, detection and prevention of physical intrusions, and protection against unauthorized access to information.

In order to incentivize corporate compliance, the regulations should also provide a safe harbor against enforcement if an independent auditor certifies the company’s compliance with such a control structure. This would encourage companies to develop more robust information security practices and to have them reviewed by independent third parties. Such an expansion of the regulations would directly further the intentions of the CCPA in protecting consumer data.

XII. The regulations should clarify that provisions related to allowing consumers to opt out of the sale of their personal information do not apply to businesses that do not sell personal information.

Sections 999.330 through 999.332 of the proposed regulations relate to the sale of information. The applicability of these sections is not clearly stated in the proposed regulations, which could lead to businesses trying to comply with these regulations even if they do not sell consumer information. In such

cases, consumers may be left even more confused about how their personal information is used and shared. The regulations should clarify that these sections are inapplicable for businesses which do not sell personal information.

* * * * *

SIFMA greatly appreciates your office's consideration of the issues raised above and would be pleased to discuss these comments in greater detail. If you have any questions or need any additional information, please contact me at [REDACTED] or Edward McNicholas at Ropes & Gray at [REDACTED].

Sincerely,

Melissa MacGregor
Managing Director & Associate General Counsel

cc: Edward R. McNicholas, Partner, Ropes & Gray
Fran Faircloth, Associate, Ropes & Gray
Kim Chamberlain, Managing Director & Associate General Counsel, State Government Affairs

Message

From: Cynthia Pantazis [REDACTED]
Sent: 12/6/2019 11:22:27 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Submission of Google's comments to the proposed CCPA regulations
Attachments: Google Comments -- CCPA Proposed Regulations.pdf

Attached please find Google's comments to the proposed regulations to govern compliance with the California Consumer Privacy Act ("CCPA").

Thank you.

--

Cynthia Pantazis
Director, State Policy
Google LLC
25 Massachusetts Avenue, NW
Washington, DC 20001

[REDACTED] (O)

[REDACTED] (C)



December 6, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

To Whom It May Concern:

Please find below Google's comments on the Attorney General's draft regulations to govern compliance with the California Consumer Privacy Act ("CCPA"). We thank the Attorney General and staff for the time and effort to prepare these draft regulations.

1. Sec. 999.314(c): Draft Regulation Addressing Service Providers

Section 999.314(c) of the draft regulations would confirm that service providers may combine personal information received from one or more entities to the extent necessary to detect security incidents, or protect against fraudulent or illegal activity. This is helpful clarification to companies to confirm that a service provider may combine information to provide essential business purpose services related to fraud and security.

However, the proposed regulations should also make clear that service providers may combine personal information collected across their clients for other internal business purposes. The CCPA provides significant support for these practices, which are commonly requested by and serve to benefit contracting businesses and consumers. For example, the CCPA permits service providers to use the personal information they collect "on behalf of a business" and "for a business purpose pursuant to a written contract." Cal. Civ. Code. § 1798.140(v). "Business purpose," in turn, is defined to include using "personal information for the business's *or a service provider's* operational purposes, or other notified purposes" *Id.* § 1798.140(d) (emphasis added). The enumerated "business purposes," moreover, include an array of purposes beyond fraud and security for which a business or service provider may use personal information. These purposes include, for example, debugging to identify and repair errors; 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; providing analytic or similar services on behalf of the business or service provider; undertaking internal research for technological development and demonstration; and undertaking activities to verify or maintain the quality or safety of a device or service of a business." *See id.* Although the legislature detailed these "business purposes" and imposed a variety of limits on them, it nowhere stated or suggested that these functions could not be carried out by combining personal information from multiple sources.

Many of these business purposes--all performed under strict contractual requirements limiting the use of personal information--may rely on and/or benefit from the combination of personal information by a service provider to perform the requested business purposes on behalf of the business. For example, service providers often need to combine data collected across clients in order to most effectively and efficiently identify and repair errors, as bugs tend to be common across client systems and finding the best fix may depend on pooling data. Similarly, logistics, transportation and delivery services providers have historically improved mapping, efficiency, and even address reconciliation by combining personal information internally across their customers, thereby developing a better service for all of them. These practices can be equally critical to a service provider's ability to undertake internal research for technological development, improve safety, and to maintain and improve the services it offers to each of its customers.

Accordingly, the clearest way to implement the text and apparent intent of the statute would be to clarify that service providers may combine personal information collected from entities to which they are service providers for "business purposes." Short of that, Google suggests the Attorney General confirm that service providers may combine personal information collected from their customers so long as they do so only for internal purposes. To the extent the Attorney General is concerned that this clarification might lead to unintended advertising uses, this standard could be coupled with a clarification that such internal uses do not extend beyond the CCPA's delineated "business purposes," such as to personalizing advertising or building a profile on an individual.

Proposed amendment: "A service provider shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose of providing services to another person or entity. A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to detect data security incidents, ~~or~~ protect against fraudulent or illegal activity, **or engage in solely internal uses.**"

2. Sec. 999.315(a): Draft Regulation Addressing Designated Methods for Opt-Out Requests

The draft regulations would require that businesses treat user-enabled privacy controls, such as browser plugins or other privacy settings that communicate or signal a consumer's choice to opt out of the "sale" of their personal information, as a valid opt-out request. There is currently no such standard technology, and the draft regulations do not specify how such browser plugins or other privacy settings should communicate these choices or how such signals would need to be honored. We encourage the Attorney General to help develop and clarify the applicable technical standards before enforcing such a requirement. Without such clarity, companies would lack guidance on how, among other things, to reconcile such controls in the event of conflicting signals (for example, where a consumer had permitted the "sale" of his or her personal information by a particular publisher in exchange for a free, ad-supported, newspaper, but then used a plugin that purported to communicate a "no sale" preference). Companies also need clarity on how these signals should be read by or communicated to third parties with which consumers do not have direct relationships, and how such controls would relate to existing browser-based cookie controls and "Do Not Track" settings.

To avoid confusion by consumers and businesses alike, we encourage the Attorney General to consider the practical challenges posed by such a rule, to seek to facilitate consensus around a single standard, and to issue additional guidance or rulemaking to provide more legal certainty around such controls and how businesses should respond to them.

3. Sec. 999.325(c): Draft Regulation Addressing Verification of Non-account Holder Requests

The draft regulations acknowledge that requiring consumer account holders to log into their online accounts is an appropriate way of verifying their requests. The draft regulations also acknowledge that businesses should not be required to provide specific pieces of personal information to non-account holders unless the business can verify the consumer's identity to a "reasonably high degree of certainty." Recognizing the importance of using password-authenticated accounts for verification where consumers have accounts with businesses and establishing high verification standards for situations in which they do not is critical to protecting their privacy.

To further advance the goals set forth in the draft regulations of avoiding privacy harms that result from providing information to an individual other than the individual to whom the data relates, Google respectfully requests that the regulations provide additional flexibility to account for the difficulty of implementing the non-account holder verification standards where companies collect device-identifying information online and do not associate that information with a consumer's name, email address, or other identifying information. The draft regulations contemplate verifying non-account holders' identities by matching at least three pieces of personal information provided by the consumer to personal information maintained by the business, together with a signed declaration from the consumer confirming their identity. For companies that store device-identifying data in a manner that is not linked to identified data, applying this standard could require businesses to collect and maintain substantially more personal information than they collect in their day-to-day operations, undermining rather than serving consumer privacy interests.

In addition, even with such data points, businesses could not be certain that the device information being requested relates to the individual making the request, or even that the requesting individual had access to the relevant device; rather, the business would only know that the requesting individual obtained or was able to otherwise discern or recreate the relevant device identifier and data points at a time prior to the request. Accordingly, there would be no way for businesses to honor such requests without risking disclosing the personal information a person other than the person to whom the data relates, and forcing them to do so would undercut the very policy goal that the law seeks to address. See California Consumer Privacy Act (A.B. 375), Sec. 2(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.")

To address these issues, we recommend the Attorney General conduct further study and rulemaking to explore ways in which companies might respond to data access requests where

they do not connect identified information to device-identifying information in a privacy protective manner that does not require the collection of additional, potentially sensitive, information or expose consumers' personal information to others. For example, the regulations might encourage companies that do not associate device-identifying information with identifying information to develop tools that would allow them to deliver the information associated with such identifiers directly to the device that makes the request (for example, by reading the cookie or device identifier of the device making the request, and then surfacing the associated information in an online portal). This would help ensure that such businesses do not inadvertently provide personal information to individuals other than to whom the information relates, and would limit the quantity of personal information collected solely for verification purposes.

4. Sec. 999.305(a)(3): Draft Regulation Addressing Notice Required Upon Collection of Personal Information

The draft regulations would impose a new requirement not contained in the CCPA that a business obtain consumers' "explicit consent" where the business seeks to use personal information "for a purpose that was not previously disclosed to the consumer in the notice at collection." Sec. 999.305(a)(3).

This standard, if adopted, could force companies to either disclose every potential use that could conceivably be made of personal information, or else be forced to constantly ask consumers to consent to minor changes regardless of consumer expectations. Prompting for consent repeatedly and for benign, obvious uses may lead to "consent fatigue" and to consumers blindly consenting without understanding the implications of their actions, drowning out more significant decisions. As a practical matter, companies will also be stymied in making new uses of data, even those necessary for security or other operational purposes, regardless of any potential privacy harm and regardless of whether the use is consistent with user expectations.

Moreover, this standard is inconsistent with that imposed by the CCPA, which prohibits businesses from "us[ing] personal information collected for additional purposes without providing the consumer with notice consistent with [Cal. Civ. Code Section 1798.100]." Cal. Civ. Code § 1798.100(b). (By contrast, the Legislature imposed an "affirmative authorization" requirement for consumers under 16 with respect to the "sale" of their personal information, 1798.120(c), which underscores that the Legislature did not intend a similar requirement in connection with the *use* of personal information.)

This standard is also inconsistent with well-established and understood standards that have evolved over 20 years of Federal Trade Commission (FTC) enforcement actions. Specifically, the FTC has recognized that only material changes as to how businesses use personal information require explicit consent. *See, e.g., In the Matter of Gateway Learning Corp.*, No. C-4120 (Sept. 10, 2004), <https://www.ftc.gov/sites/default/files/documents/cases/2004/09/040917comp0423047.pdf>; 16 C.F.R. 312.4(b) (COPPA Rule) ("An operator must make reasonable efforts . . . to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any **material** change

in the collection, use, or disclosure practices to which the parent has previously consented.”) (emphasis added); Fed. Trade Comm’n, *Protecting Consumer Privacy in an Era of Rapid Change* 57 (2012) (reaffirming “the Commission’s bedrock principle that companies should provide prominent disclosures and obtain affirmative express consent before using data in a manner **materially** different than claimed at the time of collection”) (emphasis added).

Finally, the standard deviates from analogous provisions in the GDPR and EU-U.S. Privacy Shield Framework, as well as the California Privacy Rights Act of 2020 (the draft initiative that would amend the CCPA and that may appear on next year’s ballot), each of which focuses on uses that are “incompatible” with or “materially different” from disclosed purposes. See *General Data Protection Regulation (GDPR)*: Regulation (EU) 2016/679, Arts. 5(1)(b), 13(3); Dept. of Commerce, Int’l Trade Admin, EU-U.S. Privacy Shield Framework Principles, Section II(2)(a) (2016). These standards provide additional flexibility for compatible data uses while ensuring that consumers receive appropriate notice of the purposes for which their information is used.

Google respectfully requests that the regulations be aligned with existing law to encourage uniformity in business practices, while protecting consumers from material changes and incompatible uses of their information.

Proposed amendments: “A business shall not use a consumer’s personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use the consumer’s personal information for a purpose that ~~was not~~ is materially different from that which was previously disclosed to the consumer in the notice at collection, ~~the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose,~~ it must obtain consent for such new use.”

5. Sec. 999.306(d)(2): Draft Regulation Addressing Where Notice of Right to Opt-Out is Not Required

The draft regulations would go beyond the CCPA by deeming a consumer to have opted out of “sales” if a business collects personal information from the consumer without a “Do Not Sell” link posted. See Sec. 999.306(d)(2). This proposed provision would create a new, severe penalty beyond the civil penalties authorized by the statute, particularly for those businesses that, in good faith, believed no “sales” were occurring, where that view was subsequently changed by new judicial or regulatory authority or guidance. In such cases, every single customer of the business could instantly be deemed to have opted out. This issue would be exacerbated by other sale-related requirements of the statute and proposed regulations, such as those requiring businesses to treat all consumers from whom they had collected personal information as opted out for at least the next 12 months, prohibiting requests to opt in during such time, and requiring such consumers to authorize sales through a double opt-in.

Google respectfully requests that the Attorney General revise section 999.306(d)(2) to align with the CCPA as passed by the Legislature.

Proposed amendment: “A business is exempt from providing a notice of right to opt-out if:

(1) “It states in its privacy policy that it does not and will not sell personal information. **A**

~~consumer whose personal information is collected while a notice of right to opt-out notice is not posted shall be deemed to have validly submitted a request to opt-out."~~

6. Sec. 999.305(b)(2), 999.308(b)(1)(d): Draft Regulation Addressing Required Disclosures In Privacy Notices

The draft regulations would require businesses to list the categories of consumer's personal information the business has collected about consumers in the preceding 12 months and for each category of personal information collected, provide the categories of sources from which that information was collected, the business or commercial purposes for which the information was collected, and the categories of third parties with whom the business shares personal information. These requirements go beyond the requirements of the CCPA, which requires disclosure of the business or commercial purposes for collecting or disclosing personal information without requiring the tying of each such use to each category of personal information. Particularly for businesses that offer a broad array of services, tying every category of information collected to every purpose for which data is used would result in dense and confusing policies that do not provide consumers with a meaningful understanding of a business's data practices.

The regulations should, instead, focus on ensuring that notices are written in a manner that provides consumers a meaningful understanding of the way their personal information is collected and used. This more flexible standard is akin to the transparency principles reflected in other privacy regimes like the GDPR, which requires that information be provided to consumers in "a concise, transparent, intelligible and easily accessible form, using clear and plain language." GDPR, Art. 12(1). It would also accord with other provisions of the draft regulations, requiring that privacy policies "be designed and presented in a way that is easy to read and understandable to an average consumer" and "[u]se plain, straightforward language and avoid technical or legal jargon." Sec. 999.308(a)(2). Adopting this approach would provide businesses the flexibility to communicate with consumers in a manner that aligns with their specific business practices without creating undue confusion.

Proposed amendments:

Sec. 999.305(b): "A business shall include the following in its notice at collection:

...

(2) ~~For each category of personal information, the~~ The business or commercial purpose(s) for which ~~personal information it~~ will be used."

Sec. 999.308(b)(1)(d)(2): "~~For each category of personal information collected, p~~ Provide the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties with

whom the business shares personal information. The notice shall be written in **clear and plain language, and in** a manner that provides consumers a meaningful understanding of **the way their personal information is collected and used** ~~the categories listed~~.”

7. Sec. 999.317(g): Draft Regulation Addressing Requirements for Businesses that Annually Buy, Receive for Commercial Purposes, Sell, or Share for Commercial Purpose the Personal Information of 4,000,000 or More Consumers

The draft regulations require that a business that “alone or in combination, annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers” compile and disclose certain metrics related to consumer requests. Sec. 999.317(g). Many companies collect personal information from more than 4 million consumers, but the draft regulations do not provide guidance on whether such collection would be considered “receiving” this information for a “commercial purpose.”

We respectfully request that the regulations clarify which companies are covered by this requirement, as well as clarify the time frames for when the required metrics must be compiled and disclosed, to provide businesses adequate time to adopt processes for compiling and publishing these metrics.

Proposed amendment: “A business that alone or in combination, annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers, shall, **as of January 1, 2021**”

8. Sec. 999.313(c)(9): Draft Regulation Addressing Responding to Requests to Know

The draft regulations would require businesses to provide individualized responses to requests to know the categories of personal information collected, categories of sources from whom it is collected, and/or categories of third parties with whom it is shared. Under the draft regulations, businesses would be prohibited from referring the consumer to their general practices outlined in their privacy policy unless the response would be the same for all consumers and the privacy policy disclosed all of the information otherwise required in a response to such a request. In so doing, the regulations could effectively require a business to engage in an individualized privacy accounting for every consumer who exercises their right to know, even where these disclosures have previously been provided (for example, in the context of a specific product or service).

This goes beyond what the CCPA requires and would impose significant burdens on business. It is also inconsistent with the transparency approach that has worked under other privacy regimes. For example, the GDPR specifically allows companies to ask consumers to specify the information or processing activity to which their request relates. GDPR, Recital 63. Rather than impose rigid standards that are unlikely to provide meaningful transparency to consumers, the regulations should provide additional flexibility in responding to requests to know, including by allowing them to engage with consumers and seek clarification as to which specific data points

they wish to know.

Proposed amendments: "In responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response **in response to a consumer's specific request for such information to the consumer as required by the CCPA.** It shall not refer the consumer to the businesses' general practices outlined in its privacy policy unless its response would be **similar the same** for all consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories. **A business may request that the consumer specify the information being requested before providing such an individualized response.**"

* * * * *

We appreciate the opportunity to provide comments on the proposed regulations.

Sincerely,

A handwritten signature in black ink that reads "Cynthia Pantazis". The signature is fluid and cursive, with the first name "Cynthia" and last name "Pantazis" clearly distinguishable.

Cynthia Pantazis
Director, State Policy

Message

From: K Royal [REDACTED]
Sent: 12/7/2019 12:57:38 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Hilary Wandall [REDACTED]
Subject: Submission to CCPA Draft Regulations
Attachments: TrustArc Comments to Draft CCPA Regulations Submitted on December 6, 2019.pdf

Hello,

Please see attached for our comments to the draft regulations. We appreciate the opportunity to provide these comments and respect the amount of thoughtfulness it takes for the Office of the Attorney General to draft, review, and revise the implementing regulations. We look forward to continued developments to the California Consumer Privacy Act regulations.

Thank you,
K
on behalf of Hilary Wandall,
General Counsel and SVP, Privacy Intelligence



K Royal, FIP, CIPP/US / E, CIPM
Associate General Counsel, Privacy Intelligence
[REDACTED] [REDACTED]
835 Market Street, Suite 800 San Francisco, CA 94103

REIMAGINING PRIVACY

CONFIDENTIALITY NOTICE: This email, including any attachments, may contain information that is confidential. Any unauthorized disclosure, copying or use of this email is prohibited. If you are not the intended recipient, please notify us by reply email or telephone call and permanently delete this email and any copies immediately.

December 6th, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor,
Los Angeles, CA 90013

via email: PrivacyRegulations@doj.ca.gov

Re: TrustArc Inc comments to proposed regulations for California Consumer Privacy Act (CCPA) (Stats. 2018, Ch. 55 [AB 375], as amended by Stats. 2018, Ch. 735 [SB 1121])

Dear Mr. Attorney General,

TrustArc recognizes the importance of enhanced consumer privacy rights and the consequences of inadequate privacy laws and supports the efforts of California's lawmakers to both provide enhanced rights for consumers while requiring enhanced protection from businesses.

By way of background, TrustArc is a global technology business, headquartered in San Francisco, with more than two decades of experience in assisting organizations of all sizes and industries in building consumer trust and operationalizing privacy management. Since our inception in 1997, we have supported and enhanced the ability of businesses to protect the individuals who entrust their data, knowingly or not, to those businesses. Having worked with hundreds of large and small businesses across industries and regions, TrustArc is intimately familiar with the challenges both businesses and consumers face in this digital age.

Accordingly, TrustArc respectfully submits the following suggestions to build upon and strengthen the proposed California Consumer Privacy Act (CCPA)¹ regulations²:

1. Reconsider the provision to treat unverifiable requests for deletion as opt-outs;
2. Clarify that businesses need to disclose "Categories of third parties" to whom they share personal information even where those entities collect personal information directly from the consumer;
3. Reconsider requiring responses to requests for access or deletion within 45 days from receipt, rather than within 45 days from verification;
4. Define exceptions to fulfilling consumer requests when those requests are unreasonably burdensome, overly broad, or jeopardize a business's confidential corporate information;
5. Include all health information related to research in the CCPA exemptions;

¹ See California Consumer Privacy Act of 2018 available at https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

² See text of proposed Regulations to CCPA available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf>

6. Limit the ability of service providers to respond to consumer requests without the business's input;
7. Exempt businesses that may share common ownership or branding with a business subject to the CCPA but do not have access to that business's data; and
8. Explain the requirements for notice in certain situations that are challenging, such as offline interactions, connected devices, and the need for accessible notices.

Each of these points is addressed in further detail below along with recommended solutions to address the identified concerns.

1. Treating Unverifiable Requests to Delete as Opt-outs of Sales

The provision that an unverifiable request to delete personal information should be treated as an opt-out of sales, § 999.313(d)(1), is illogical and appears to contravene the intent of the CCPA that consumer requests be verified. This requirement creates a situation where businesses are forced to act on a request that may be contrary to consumers' actual desires. Given the prevalence of fraudulent requests under the European Union's General Data Protection Regulation³, one of the only bases for comparable research, it is highly possible⁴ that there will be fraudulent requests made pursuant to the CCPA.

Acting on fraudulent requests is against the intent of the CCPA, which is to give consumers rights to know and control aspects of how their personal information is collected, used, and disclosed.

Further, competitors or malicious actors could force a business not to sell valuable personal information that could be critical to their business model. Treating unverified requests for deletion as opt-outs of sales is a step not only unintended by the CCPA, but perhaps even directly against the stated purpose and requirements of the CCPA.

TrustArc requests that § 999.313(d)(1) be stricken from the regulations.

2. Categories of Third Parties

The CCPA uses the phrase "Categories of third parties" in relation to the consumers' right to know the third parties with whom a business shares consumers' personal information (§ 1798.110(a)(4)). In the proposed text of regulations at § 999.301(e), "Categories of third parties" is defined as "types of entities that do not collect personal information directly from consumers, including but not limited to advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers."

³ See alert posted by the National Commission for Data Protection in Luxembourg, the *Commission Nationale pour la Protection des Données* at <https://cnpd.public.lu/en/actualites/national/2018/November2018/fermeture-registre-public.html>.

⁴ See the article from the International Association of Privacy Professionals <https://iapp.org/news/a/fake-dsars-theyre-a-thing/discussing-the-problem-of-anonymous-fraudulent-requests>.

Because many of the examples of “Categories of third parties” do, in fact, collect personal information directly from consumers through cookies or tags, the regulations appear to allow a business to avoid disclosure of the types of entities it shares personal information with if those entities are also collecting personal information directly from consumers.

For example, if a business both 1) shares consumer personal information to a social network and 2) allows that social network to directly collect personal information via cookies on the business’s site, then the plain language of the regulation permits omission of the disclosure of the sharing of personal information to the social network because subsection (e) of the regulation states that the categories of third parties that must be disclosed are those that “do not collect personal information directly from consumers.”

At a minimum, the language is confusing because the definition of “Categories of third parties” excludes disclosing the sharing with the social network in this example, but the list of categories to be disclosed appears to include the social network.

As this appears to be an unintended consequence, we would request language to clarify whether businesses need to disclose the categories of third parties with whom they share personal information even where those third parties are simultaneously collecting personal information directly from consumers under § 999.301(e).

3. Response Timeframe to Requests

Proposed section § 999.313(b) explicitly states that requests to know and to delete must be responded to by businesses within 45 days of receipt “regardless of time required to verify the request.” Such a requirement may lead to the unintentional (and undesired) result of devaluing the significance of verification while potentially indirectly penalizing businesses acting in good faith.

To avoid the risk and liability from exceeding the 45-day response period as a result of a consumer not timely authenticating their identity until just before the deadline (or even after it), businesses will be forced to effectively prepare responses to all requests upon receipt. This denies the gatekeeper function of verification and forces businesses--particularly small- and medium-sized enterprises--to expend much needed resources on many requests that will ultimately go unverified.

Such a result is not realistically a goal of the CCPA and, in instances when verification occurs very close to the deadline, increases the likelihood of inadvertent or unauthorized disclosures of consumers’ personal information as a result of last-minute actions.

Respectfully, § 999.313(b) should be revised such that the 45-day period begins following verification of the request or, in the alternative, the Attorney General should

clarify that a request verification being completed after 30 days from receipt provides the basis for a 45-day extension of the response time.

4. Exceptions to Fulfilling Consumer Requests

The CCPA takes great care to provide exceptions to a consumer's right to access and deletion but does not appear to consider broad categories that should be subject to exceptions, such as requests that are unreasonably burdensome, overly broad, or that compromises a business's confidential information.

For example, with video surveillance images, consumers are not typically identified until or unless there is a situation wherein identification is necessary, such as if a crime is committed. Under the CCPA § 1798.100(e) provides that if personal information is retained in a way that is not identifiable, the business is not required to identify it solely for the purpose of providing that information to the consumer. Images of individuals are inherently identifiable, but not typically associated with identifiers making them readily accessible for purposes of fulfilling consumer requests. Thus, associating identifiers solely for the purposes of fulfilling a consumer's request is unreasonably burdensome on the business and overly broad for the purposes of consumer rights.

In addition, the exceptions to disclosure listed in § 999.313(c)(3) only address that "a business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business' systems or networks." There is no exception for compromising a business' intellectual property, confidential activities, or physical security. Providing images that disclose corporate confidential information should not be allowed.

The Attorney General is directed to establish "any exception necessary to comply with state or federal law, including ... trade secrets and intellectual property rights" (CCPA § 1798.185(a)(3)) in addition to adopting "additional regulations as necessary to further the purposes of the title" (CCPA § 1798.185(b)).

Potentially, the language of § 999.313(a)(3) could be changed to read "A business shall not provide a consumer with specific pieces of personal information if the disclosure is **unreasonably burdensome on the business; is an overly broad request; or** creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems, ~~or~~ networks, **physical property, or intellectual property or compromises the business' confidential corporate activities**" (additions noted in bold).

Given these challenges, TrustArc requests that exceptions addressing disclosure of confidential corporate information, unreasonably burdensome tasks, and overly broad requests as noted in the suggested language above be added into the regulation and / or clarification on how to manage these significant concerns.

5. Health Data

Along the same continuum as the exceptions requested above to provide exceptions for confidential corporate information, there is a subset of health data that is not explicitly exempted from the CCPA, although the intent appears to do so. Within clinical trials for pharmaceuticals or medical devices, there are activities required or advised by the U.S. Food and Drug Administration that do not fall under the Common Rule (45 C.F.R. 46), exempted from the CCPA in § 1798.145(c)(3). Not all data processed in research activities fall under the Common Rule or HIPAA (the U.S. Health Insurance Portability and Accountability Act of 1996 and its subsequent amendments).

The health information processed for these purposes, such as post marketing surveillance or other research purposes, are as critical to the public good and medical advances as those specifically covered by the Common Rule. Consumer access to that information or deletion of that data could have a detrimental impact on critical development and consumer safety.

The Attorney General has the authority to make sure that this critical information does not inadvertently fall between the lines under § 1798.185 under establishing necessary exceptions or additional regulations to further the purpose of the CCPA.

For this reason, we respectfully request that the regulations include a clarification that all health information related to research activities are exempted from the CCPA.

6. Service Providers

Under § 999.314(d), service providers are directed that if they collect, maintain, or sell “on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial.”

This appears to direct service providers to respond directly to consumers. However, the next sentence tells service providers to inform consumers to submit requests to the business. This seems contradictory and is confusing. Certainly, service providers should facilitate consumer requests in an expeditious manner.

It is unclear whether this provision is directed at service providers who collect personal information directly from consumers, presupposing a relationship conducive to the service provider responding independently. It is also unclear who the service provider is required to “explain the basis for the denial” to - the consumer or to the business. Potentially, if a service provider can grant the request, it should do so without informing the business beforehand or at all. The statement as written is unclear and subject to various interpretations.

In the absence of prior arrangements, service providers should not be permitted to respond to consumer requests directly.

TrustArc respectfully requests a clarification on service providers’ responsibility.

7. Businesses Sharing Common Management or Branding

The CCPA § 1798.140(2) definition of “Business” includes “[a]ny entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business” where “Common branding” means a shared name, servicemark, or trademark.” This definition puts an undue burden on businesses that may have no tie to California or would not be subject to the CCPA other than sharing a common branding, such as franchises.

Consider a small business that shares a brand located in Mississippi that may do \$2M in revenue and has no California data, but shares a brand with a business in California that is subject to CCPA is now required to implement provisions of the CCPA that are unduly burdensome, overly broad, and perhaps even outside the scope of California jurisdiction as common branding is not necessarily enough to qualify for personal and subject matter is questionable if the out-of-state business has no connection with California data. The same argument can be made for entities that are controlled by a business.

As California is truly concerned with the wellbeing of its residents’ personal information, this appears to be an unintended consequence to fold in businesses with no tie to California or its data other than sharing a common branding. Now, where the data is commingled, there may be cause; but where there is no access, there is no cause. The Attorney General has authority to enact the regulations necessary to implement the CCPA and to assure that there are exceptions where applicable to comply with state and federal laws under the CCPA § 1798.185(b) and (a)(3) respectively.

For the reasons above, TrustArc requests that the Attorney General provide an exception to the CCPA for businesses whose only nexus is being under the same management or sharing common branding if they have no access to California personal information collected, used, or otherwise processed by the pertinent qualifying business.

8. Notice - situational challenges, e.g. offline, IoT, accessible

The requirements for notice in several sections of the proposed regulations present challenges in various scenarios.

For example, § 999.305(a)(1) requires that consumers be informed, “at or before the time of collection . . . of the categories of personal information to be collected from them and the purposes for which the categories of personal information will be used.” In many in-person situations, the business may not have a website for the consumer to go to as directed by § 999.305(b)(4). The CCPA and the proposed regulations make it clear that offline encounters are subject to the notice requirements in § 999.305(a)(2)(e)), but presenting full notice at or before the time of collection will be challenging in a variety of settings, including, but not limited to, Internet of Things (IoT) devices and video.

IoT Devices that are connected to the internet are not necessarily embedded into other processes in a manner that supports providing notice, such as parking sensors. These

same challenges are present in other “offline” contexts such as video surveillance or crowd monitoring at venues. When hundreds of technologies come together in one space, “prominent signage” becomes ubiquitous to the point of invisibility.

In light of these challenges for the general public, making these notices accessible for individuals with disabilities, as required under § 999.305(a)(2)(d), is nearly impossible without further guidance on expectations and standards.

A method to consider as one part of the solution would be creating visual indicators that convey meaning quickly, prominently, and across language barriers. These indicators have been successful in many contexts such as indicating restrooms, prohibitions against smoking, and handicap accessible parking.

Under these various circumstances, even if the initial notice is provided, it is challenging to provide additional notice if the business who collected personal information decides to use it in a new or different way (§ 999.305(a)(3)).


TrustArc requests that the Office of the Attorney General provide specific guidance on what constitutes adequate notice in offline context, including standards on sufficiency for accessible notice, with consideration given to the use of visual indicators.

Please note that the concerns with accessible notices is also present in § 999.306(a)(2)(d), § 999.307(a)(2)(d), and § 999.308(a)(2)(d).

* * *

With the eight recommendations above, TrustArc has completed its comment submission. We appreciate the opportunity to provide these comments and respect the amount of thoughtfulness it takes for the Office of the Attorney General to draft, review, and revise the implementing regulations. We look forward to continued developments to the California Consumer Privacy Act regulations.

Respectfully submitted,



Hilary Wandall

General Counsel & SVP, Privacy Intelligence
[REDACTED]

Message

From: Carkhuff, Braden [REDACTED]
Sent: 12/7/2019 12:30:40 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Sutter Health Comments on the California Consumer Privacy Act Proposed Regulations
Attachments: Sutter Health Proposed CCPA Regulations Response.pdf

On behalf of Sutter Health, I respectfully submit the attached comments regarding the proposed regulations for the California Consumer Privacy Act. If you have any questions regarding our comments, please reach out.

Thank you,

Braden Carkhuff

Braden Carkhuff
Privacy and Information Security Officer – Special Projects
Communications | Design & Innovation | Marketing | Philanthropy
Office of the General Counsel
Cell: [REDACTED]
Email: [REDACTED]



Quick Tip: Watch where you surf, Phish take a bite out of your security.

w6rds™ Together, We Can Protect Patient Information



December 6, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: Comments on the California Consumer Privacy Act Proposed Regulations

Dear Attorney General Becerra:

Sutter Health is a not-for-profit healthcare organization providing comprehensive, integrated medical services in more than 100 Northern California communities. Our organization is staffed by over 55,000 employees and affiliated with 12,000 physicians providing care to more than 3 million patients. Central to our values are commitments to working with the diverse communities we serve, providing excellence, quality, and safety to our patients, and ensuring the privacy and security of our patients' information. We are writing to express our concerns with the proposed regulations around the California Consumer Privacy Act (CCPA) and to provide feedback, insight, and awareness on possible modifications that would allow healthcare organizations such as Sutter Health to continue protecting patient information and comply with the CCPA without creating risk and unnecessary confusion to our patients.

The CCPA directly affects the few for-profit entities controlled by Sutter Health, which is a not-for-profit 501(c)(3) tax-exempt entity. Thus, a not-for-profit healthcare organization such as Sutter Health, could be subject to the provisions of the CCPA. Our comments below outline the reasons why the drafted regulations should be revised to address the challenges the health care sector faces with having to comply with both consumer rights under CCPA and patient rights under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Confidentiality of Medical Information Act (CMIA). The CCPA exempts healthcare information from some requirements under the law, but, despite these noted exemptions, there remains ambiguity relating to consumer data that may also be directly related to patient health information. At Sutter Health, consumers are generally patients and patients are generally consumers, and both personal information and protected health information (PHI) are of most value to the patient when they are intimately connected. Without a clearer line of demarcation, the interplay between CCPA and HIPAA is strained, and all health care providers offering medical care, safety, and wellness within the state of California will be faced with similar issues. Consumers are now very aware of privacy issues and data protection challenges due to the mass privacy breaches some companies have faced. However, the draft regulations conflate consumer data, personal information, and PHI. The similarities and nuances that exist between consumer data and PHI will create unnecessary misunderstandings among consumers and patients about their data protection rights.

As a covered entity under HIPAA, Sutter Health is regulated and required to treat PHI with certain protections; however, in some instances consumer data and PHI are the same information. For example, consumer data may include social security numbers, street addresses, and zip codes and this data is also considered PHI. The dual nature of this data creates unintended negative consequences for health care providers faced with consumers and patients requesting to exercise their rights under CCPA. This is because the data they may request to access, delete, or restrict



resides in both the PHI and consumer data environments. For example, when a consumer, who is not yet a patient, visits Sutter Health's website to gain an understanding of the health and wellness services Sutter Health offers to the community by clicking on links relating to diabetes or dialysis services, and subsequently, that same consumer decides to become a patient of Sutter Health by creating an online patient account to book an appointment, the relationship between the previous consumer and the subsequent patient will continue to be commingled. Thus an argument may be made that the action of initially visiting Sutter's website by the consumer falls within the purview of the CCPA, but the subsequent actions taken to create a patient account are exempted. This dilemma for the health care sector is significant when magnified by the number of consumers/patients seeking information from health care providers. It is apparent that the legislature did not intend to create overly burdensome requirements for the health care sector to comply with this law. Therefore, an express carve-out should exist for HIPAA covered entities. Sutter Health seeks clarity in the regulations on behalf of our patients so we may best serve the communities in which we are located.

Article 2. Notices to Consumers

§999.305. Notice at Collection of Personal Information

Current Regulation: §999.305(a)(2)(e)

While providing consumers notice at or before the collection of a consumer's personal information is, and should remain, a central tenet of privacy rights, the requirements of §999.305(a)(2)(e) do not contemplate physical locations where only PHI is collected. This section's requirements, when applied to a covered entity's service locations, are likely to cause confusion to the consumer and patient. While a covered entity may have data subject to CCPA, the information collected at physical locations where covered services are provided is PHI and therefore out of scope of the CCPA. By requiring the presence of a paper notice or prominent signage directing consumers to the online notice, it will cause concerns and confusion as to the appropriate uses of their PHI as well as their separate, distinct rights under HIPAA.

Issue with Current Regulation:

Section 999.305(a)(2)(e) requires businesses to provide notice of collection of personal information before any information is collected. This approach is not practical for health care facilities, where PHI is collected and there is no way to separate PHI from personal information.

[Proposed] Regulatory Solution:

Revise §999.305(a)(2) to exclude HIPAA covered entities from this requirement, rather than cause confusion and misunderstandings among consumer and patient groups. The change would be consistent with current HIPAA laws and alleviate overly burdensome requirements placed upon HIPAA covered entities.

While a covered entity may engage in practices where notice is mandated, those same notice requirements should not be required in locations where *only* out-of-scope data is collected.

Current Regulation: §999.305(a)(3)

"A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the



business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.”

Issue with Current Regulation:

Section 1798.100 does not contemplate a consent requirement, much less an “explicit consent” requirement. The text of the CCPA only addresses consent when discussing selling the personal information of a minor, Cal. Civ. Code §1798.120(d), and surrounding a financial incentive program, Cal. Civ. Code §1798.125(b)(3).

Sutter Health feels the “explicit consent” requirement in §999.305(a)(3) goes beyond the scope of the CCPA, and also fails to explain how “explicit consent” is to be obtained.

[Proposed] Regulatory Solution:

Delete the extra statutory requirement of §999.305(a)(3).

§999.306. Notice of Right to Opt-Out of Sale of Personal Information

Current Regulation: §999.306(d)

“A consumer whose personal information is collected while a notice of right to opt-out notice is not posted shall be deemed to have validly submitted a request to opt-out.”

Issue with Current Regulation:

Sutter Health believes the consequences the health care sector will face was not intended or contemplated with this specific provision. Patients who are consumers can’t opt-out of the sharing of their PHI when it is mandated under HIPAA. As previously stated, PHI and personal information are and should be linked. Therefore, HIPAA covered entities should be exempt from this provision.

Because HIPAA covered entities are not in the business of mining consumers personal data for profit, they should be exempt from this law. Moreover, HIPAA covered entities both secure and protect PHI, which includes personal information, for patients’ health, safety, and welfare. The ‘Opt-Out of Sale of Personal Information’ should exempt these entities to avoid confusion of the issues by both consumer and patient groups.

The regulations also don’t consider that in some instances HIPAA covered entities are required to share PHI, which may include personal information, and this fact alone fosters confusion among both patients and consumers.

Pursuant to the draft regulations, businesses are required to keep a record of the opt-outs they receive. For businesses who don’t sell personal information but to whom consumers can be deemed to have submitted the default opt-out, this creates a compliance burden.

Also, if a business receives “default” opt-outs at a time when it didn’t sell information but decides to sell information within 12 months, the business will be preemptively prohibited from selling information for 12 months even though the business has not received explicit “direction from a consumer not to sell the consumer’s personal information,” as required by the CCPA.

Section 999.306(d)(2) may not be operable for businesses.

[Proposed] Regulatory Solution

Exempt HIPAA covered entities from this provision or provide language that states consumers may exercise their right to opt-out if their personal information is not linked to their PHI.

§999.308. Privacy Policy

Issue with Current Regulation:

The requirement for posting the privacy policy as outlined in §999.308(a)(3) should be revised to not dictate the use of the word “privacy” as a link to the CCPA notice. Covered entities are already required by HIPAA to post conspicuously on their website a link to the covered entity’s notice.¹ By requiring covered entities to use the word “privacy” as a link to a CCPA compliance web page or notice, this will confuse the consumer or patient when they are looking for the covered entity’s approach to patient privacy. The Attorney General should not dictate the terms required for a link to a business’s privacy materials when there are competing federal requirements for conspicuously posting on a website and what material should be posted there. Businesses should be allowed to define what words should link to the appropriate content.

We encourage the Attorney General to review and revise the terms used in §999.308(b)(1)(d)(2) and §999.308(b)(1)(e)(2). In the former section, relating to the categories of personal information collected, it is required to designate the categories of their parties with “whom the business *shares* personal information.” [Emphasis added] Then, the notice also requires a listing of categories of personal information “that it *disclosed or sold* in the previous 12 months.” [Emphasis added] The definition of “sale” is broad under the CCPA and also encompasses “discloses” in the definition.² However, it does not define “shares” but this could reasonably be understood as “make available” as in the definition.³ If the current requirements for the notice (particularly on the website of a business) requires the use of a button stating “Do Not Sell My Information,” the notice should reflect the same broad definition of sale, rather than parsing out “shares,” “discloses” and “sells.”⁴ To a consumer in the ordinary course of business, each of these terms, when read plainly, all have different meanings and present a problem when drafting appropriate language for a privacy policy.

[Proposed] Regulatory Solution:

Modify language to provide consistent terms, for example, “shares,” “discloses” and “sells” are used interchangeably throughout the section. These terms should be defined and used consistently.

Article 3. Business Practices for Handling Consumer Requests

§999.312. Methods for Submitting Requests to Know and Requests to Delete

Issue with Current Regulation:

The regulation did not contemplate HIPAA covered entities who predominantly handle PHI, which encompasses specific personal information. As drafted, this may be confusing for the consumer. It might be better if the two pieces were divided – a section on submitting requests to know and a section on submitting request to delete.

The proposed regulations also create a conflation between CCPA and other applicable privacy laws. While requiring businesses to provide a method of submitting requests that reflects the manner in

¹See 45 CFR § 164.520(c)(3)(i).

² See Cal. Civ. Code § 1798.140(t)(1).

³ *id.*

⁴ See §999.305(b)(3).

which the business primarily interacts with the consumer generally makes sense, it does not in the context of a provider who is a covered entity. Most providers will interact with patients in person. In the context of a covered entity, generally all of the data created and collected as a part of a service provided is PHI and out of scope of the CCPA. By requiring an in-person method of submission of those requests (in addition to the notice being available in the in person setting addressed earlier) it is conflating the information covered by CCPA. To a consumer/patient, it would have the implication that the covered entity “sells” their health information. Additionally, requiring front-line staff to be able to speak to the nuance between HIPAA patient rights and CCPA consumer rights is untenable. Not only does this requirement cause confusion to consumers/patients, it also will confuse front-line employees.

[Proposed] Regulatory Solution:

Exempt HIPAA covered entities from this provision or provide language that states consumers may exercise their right to delete if their personal information is not linked to their PHI.

§999.313. Responding to Requests to Know and Requests to Delete

Issue with Current Regulation:

The methods outlining the steps a business may take to comply with a consumer’s request to delete their information does not align with the spirit of the law or a consumer’s reasonable understanding of the word “delete.” The draft regulations state a business may either permanently erase, de-identify, or aggregate the personal information. The only appropriate understanding and application of a Request to Delete should be permanently and completely erasing the personal information. If all documents to the consumer should be in plain language and be written to provide consumers a “meaningful understanding,” it is difficult to provide the techniques used to de-identify or aggregate under CCPA in a plain language understanding.⁵ Most consumers would reasonably assume that when they exercise a Request to Delete, their information will be *deleted*. The other listed methods, de-identification and aggregation still leave a trace and record of the individual. In a response to a Request to Delete, the consumer will likely be confused that their request was processed as a de-identification or aggregation, rather than a true deletion.

§999.315. Requests to Opt-Out

Issue with Current Regulation:

Additional clarification is required as to notification requirements for alerting consumers who opt out that third-party notification has been completed. The proposed regulations require that action on an opt-out request should take no longer than 15 days from the date of receipt.⁶ Additionally, the business processing the request must notify all third parties with whom it has sold personal information in the 90 days preceding the date the request was made.⁷ The business must notify the consumer that this notification to third parties is completed.⁸ However, it is unclear how this notification and process occurs when the opt-out is initiated from user-enabled privacy controls as noted in §999.315(c). This section requires a business to comply with user-enabled privacy controls as a valid form of opt-out for the browser or device, or, if known, for the consumer.⁹ We request the

⁵ See §999.313(c)(11).

⁶ See §999.315(e).

⁷ See §999.315(f).

⁸ *id.*

⁹ See §999.315(c).

Attorney General to provide additional information as to how to effectively respond to an opt-out request initiated by user plug-ins when we may not have any identifying information for the individual or any avenue to notify the consumer of the completion of the request.

Additionally, in the instance of public or shared computers, we may be opting individuals or browsers out that are not actually requesting an opt-out. This may cause individuals to be inadvertently opted out and then subject to a price difference for a service in which they are permitting the sale of their data as permissible under §999.336. This then requires the consumer to follow the two-step opt-in process for the sale of their data causing a burden to the consumer who did not want to opt-out initially.

§999.317. Training; Record-Keeping

Issue with Current Regulation:

Section 999.317(a) could be interpreted to mean that all employees of a business that could be asked questions about a business's privacy practices need to understand all the requirements of the CCPA and how to handle consumer questions. This section could be improved by adding clarifying statements. For example, following the example of the GDPR, the regulations could require "The department" responsible for handling consumer ...". This type of change would show that while frontline staff may get asked questions about the CCPA, they are not required to have knowledge beyond where to direct questions. Alternatively, the regulation could be updated to read "All individuals directly responsible for handling consumer inquiries ...". Organizations such as Sutter Health have employees tasked with a variety of responsibilities, however the employees with the ability to respond to CCPA inquiries in a way that best meets the needs of the consumer reside in the privacy and information security department – not a patient services representative tasked with checking in patients, obtaining basic patient information, and the like. Adding clarifying statements will afford businesses the ability to more easily educate the workforce to best assist the consumer because it allows the business to instruct and train employees who to direct questions to instead of creating an appearance that all employees should be able to answer CCPA inquiries. Additionally, the Attorney General's Standardized Impact Assessment identified that "privacy professionals" would be trained for handling consumer requests or be responsible for the business's CCPA compliance.¹⁰

[Proposed] Regulatory Solution:

The regulations should clearly reflect that the training requirement is specific to the individuals *specifically* designated to respond to consumer rights requests.

Article 4. Verification of Requests

§999.323. General Rules Regarding Verification

Section 999.323(b)(1) should state that a business may match the "identifying information provided by the consumer" to "the *in scope* personal information of the consumer already maintained by the business." In the context of healthcare organizations, the entity may have a large amount of information on the consumer, but most of it falls within an exemption to the CCPA. The law should require only the use of the data that is in scope of CCPA as to not commingle in-scope and out-of-scope data. This could lead to misunderstandings on the side of the business and cause a violation of other privacy laws. Verification processes should rely only on data considered in-scope of CCPA, not

¹⁰ Impact Assessment at 26.



all information the business may have on an individual, especially when the business is a covered entity under HIPAA and maintains considerable PHI.

§999.325. Verification for Non-Accountholders

We request clarification between the terms “data points” and “pieces of personal information.” Sections (b) and (c) in this section outline the methods for identifying an individual without a password-protected account. The former requires validating two data points to release categories of personal information regarding a Request to Know. The latter requires “three pieces of personal information” regarding a request to know specific pieces of personal information. Neither terms are defined. Parity should be reached between these two sections.

On behalf of Sutter Health, thank you for the opportunity to provide these comments on the proposed regulations implementing the CCPA. Please contact me directly with any questions via email [REDACTED] or at [REDACTED]

Respectfully,

A handwritten signature in purple ink that reads 'Jacki Monson'.

Jacki Monson
Chief Privacy and Information Security Officer
Sutter Health

Message

From: Courtney Jensen | [REDACTED]
Sent: 12/6/2019 11:06:46 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: TechNet Comment Letter Regarding Proposed CCPA Regulations
Attachments: TechNet CCPA Regulations Comment Letter 12.06.19.pdf

Good Afternoon,

Attached please find TechNet's written comments regarding the CCPA proposed regulations.

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 916.600.3551
915 L Street, Suite 1270, Sacramento, CA 95814
www.technet.org | @TechNetUpdate

December 6, 2019

The Honorable Xavier Becerra
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Dear Mr. Attorney General Becerra,

TechNet appreciates the opportunity to submit written comments regarding the draft California Consumer Privacy Act ("CCPA") regulations.

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 continues to contain 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. It is imperative for businesses and consumers in California that CCPA regulations move forward with the goal of providing clarity to the statute.

Consumer privacy continues to be an evolving landscape that is always under construction in California. CCPA is effective on January 1, 2020 and the industry has already worked diligently to go live with requirements to come into compliance, all of which took place before draft guidance was issued by the AG's office. At the same time, an initiative is likely to be on the ballot in 2020 which would completely change the features, system changes, user interface, and backend workflow which was designed and implemented by industry. These additional layers and comprehensive changes are costly and also confusing for consumers.

Compliance has been costly and every small change to the requirements of AB 375, via Attorney General regulations, necessitate expensive changes to platforms. Essentially, industry was required to build products without the criteria they would

be graded on and now, we believe, the regulations could cause further confusion and additional layers that were not clearly delineated when businesses began planning for and implementing technologies to go live in 2020. We urge that any new requirements beyond those delineated in the statute be removed from the regulations or, at the very least, have a delayed effective date.

Respectfully, please find our specific comments regarding the regulations below.

§ 999.301. Definitions

- The new definition of “*categories of third parties*” creates a new level of confusion for businesses. Businesses, such as internet service providers (ISPs), generally have a direct relationship with consumers. Although they may receive personal information indirectly at times, ISPs, advertising networks, data analytics providers, and social networks should be removed from the third-party definition because they usually collect data directly or may be considered “service providers” under the CCPA.
- The draft rules also define “*affirmative authorization*” as “*an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information.*” Within the context of a parent or guardian acting on behalf of a child under 13, it means that the parent or guardian has provided consent to the sale of the child’s personal information in accordance with the methods set forth in section § 999.330. For consumers 13 years and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.” We suggest striking the language mandating a two-step process as it can be cumbersome and disruptive for consumers and overly prescriptive for businesses. It can prevent businesses from developing innovative consent flows based on extensive User Experience (UX) and User Interface (UI) research.

§ 999.305. Notice of Collection of Personal Information

- § 999.305 sets forth the purpose and general principles relating to a covered business’ provision of notice at or before the time of collection of personal information to a consumer. However, it does not contemplate businesses that collect personal information over the telephone and/or the manner in which notice should or could be provided. For example, it would be exceptionally burdensome to inform a consumer of the categories of the personal information to be collected from them and the purposes for which the categories of the personal information will be used (§ 999.305(a)(1)) during a telephone call, particularly where call time is critical to a business’ success. If businesses are forced to deliver a privacy notice to a consumer over the telephone, businesses are extremely likely to suffer losses in call volume and

revenue. Further, it is also unlikely that consumers would be willing to stay on a call to listen to a privacy notice being read aloud.¹

- We respectfully suggest that § 999.305 be amended to clarify that a covered business that collects personal information from consumers over the telephone can direct consumers to a notice at collection (as defined in 999.301(i)). This provides the consumer with transparency around the business' privacy practices and the consumer rights with less impact on the consumer experience and lesser risk of harm to the business.
- The draft regulations in § 999.305(a)(3) propose "*A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.*" This new purpose limitation requiring obtaining explicit consent from the consumer to use personal information for a new purpose exceeds the scope of the CCPA's statutory language, which only requires notice of new purposes (see Civil Code 1798.100 (b)).
 - Accordingly, the draft language should be revised to, "*A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use ~~and obtain explicit consent from the consumer to use it for this new purpose.~~*"
 - An alternative approach to consider is clarifying this limitation so that it applies only to material changes that are retroactive. Accordingly § 999.305(a)(3) should be revised to, "*A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer's personal information for a material retroactive purpose*"

¹ See, e.g. Balebako, Rebecca, et al. "Designing Effective Privacy Notices and Controls" (June 16, 2017). IEEE Internet Computing. Available at <https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=4236>; Obar, Jonathan A. and Oeldorf-Hirsch, Anne, "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services" (June 1, 2018). TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy, 2016. Available at SSRN: <https://ssrn.com/abstract=2757465> or <http://dx.doi.org/10.2139/ssrn.2757465>; Smith, Aaron, "Half of online Americans don't know what a privacy policy is" (December 4, 2014) Pew Research Center. Available at <https://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/>

that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new material retroactive use and obtain explicit consent from the consumer to use it for this new purpose.”

- Provisions on notice when the information is not directly collected should be more flexible (§ 999.305(d)(2)). The regulations should clarify that a business that receives personal information from an indirect source may comply with its CCPA obligations through contractual provisions that require other businesses to provide the requisite notice to consumers. The requirements to contact the source and obtain signed attestations are confusing and duplicative.

§ 999.306. Notice of Right to Opt-Out of Sale of Personal Information

- Respectfully, TechNet has the same concerns with the delivery of the notice of the right to opt-out of the sale of personal information as the notice provision above for businesses collecting personal information over the telephone, and suggest the same solution as outlined above.
- Overall, TechNet believes the proposed rules in this section governing the “right to opt-out of sale of personal information” exceeds CCPA’s statutory language, place business at risk for unfair and deceptive claims, and create untenable compliance obligations.
- The proposed rule § 999.306(a)(1) references a consumer’s right to direct a business *“that sells (or may in the future sell) their personal information to stop selling their personal information, and to refrain from doing so in the future.”* The CCPA does not govern a business’s future potential to sell personal information, but instead governs the practices of businesses that sell personal information at the time of processing the personal information. The draft rule references not only businesses that actually sell personal information but that may in the future, which exceeds the current statutory language.
- The proposed rule § 999.306(d) also states that a business is exempt from providing a notice of right to opt-out if it does not sell “and will not” sell personal information and if it states in its privacy policy that it does not and “will not” sell personal information. This is counter to the text of the CCPA, which allows for new uses of data pursuant to notice. In addition, there is a lack of clarity as to when businesses will be able to seek authorization from these consumers who will have been “deemed” to have opted out. Mandating that businesses make future representations like this unnecessarily restricts businesses from evolving their business models and roadmaps. And in the event that a business in good faith makes a representation that it will not sell information and at a later time decides to sell personal information with

adequate notice to consumers, the business now risks that it has made an unfair and deceptive claim to consumers by previously representing that it will not sell personal information.

- § 999.306(d)(2) states, “A consumer whose personal information is collected while a notice of right to opt-out notice is not posted shall be deemed to have validly submitted a request to opt-out.” First, the proposed rule conflates general personal information collection (not selling) with the right to opt-out of the selling of personal information. Second, the CCPA explicitly references that a business shall be prohibited from selling a consumer’s information after receiving “*direction from a consumer not to sell the consumer’s personal information*” (1798.120 (d)) The rule has replaced this “direction” requirement, which requires an explicit action through the opt-out button, with a “default” opt-out. Third, pursuant to the draft regulations, businesses are required to keep a record of the opt-outs they receive. For businesses who don’t sell personal information but to whom consumers can be deemed to have submitted the default opt-out mentioned above, how would this work once selling begins – this would create a cumbersome compliance burden. Also, if a business is deemed to receive “default” opt-outs at a time where it didn’t sell information, when are they permitted to seek a consumer’s consent to in fact sell?
 - One approach to consider is amending the section to clarify that it only applies to previously collected information. Accordingly, the draft language should be revised to, “*It states in its privacy policy that that it does not and will not sell personal information. A consumer whose personal information is collected while a notice of right to opt-out notice is not posted shall be deemed to have validly submitted a request to opt-out with respect to personal information collected during such time that the opt-out notice did not appear.*”

§ 999.307. Notice of Financial Incentive

- The disclosures required in § 999.307(b)(5) in relation to financial incentives are impractical and deal with competitively sensitive information. It is challenging for any business to assign value to a single consumer’s data, and data often gains value when it is aggregated. Consequently, financial incentive programs will more likely be based on a complex calculation of costs to the business and market comparisons. Any number that a business ultimately discloses will not be meaningful to consumers. Every business and service is different, and requiring a business to disclose its methods and calculations will likely require disclosure of competitively-sensitive information. The CCPA statutory language is already sufficiently protective of consumers with regard to discounts.

- As noted above, data doesn't have independent value. The perceived value of data is subjective, in flux and depends on context. Because data lacks clear, objective value, academics have come up with wildly different estimates for the value of certain services to people, and experts are likely to come up with differing values for other services as well. Concerning free, ads-based services, personalized services, people don't give up or exchange data for their experience; instead the experience is made possible by data. Data is what enables ads-based services to provide the core of the service itself, which is personalized content. The reason certain businesses can offer their services for free isn't that they're being compensated with people's data. It's that they make money by selling ads: these businesses sell advertisers the opportunity to present their messages to people. And advertisers pay the businesses based on object metrics such as the number of people who see their ads or the number of people who click on their ads.
- Specifically, § 999.307(b)(5) requires "[a]n explanation of why the financial incentive or price or service difference is permitted under the CCPA, including: a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and a description of the method the business used to calculate the value of the consumer's data." The rules articulate standards by which businesses can calculate the value of consumer data. We strongly recommend removing any requirements for providing an estimate of the value of consumer data.
 - The draft language should be revised to: "[a]n explanation of why the financial incentive or price or service difference is permitted under the CCPA, ~~including: a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and a description of the method the business used to calculate the value of the consumer's data.~~"
 - We also propose striking § 999.337, which describes the methods in calculating the value of consumer data. This requirement to disclose the value and methodology goes beyond CCPA statutory language. We urge that this requirement be struck from the draft regulations.

§ 999.308. Privacy Policy

- For consistency with the statute (1798.130(a)(5)(C)(i)) §999.308(b)(1)(d)(2) should be revised to the following: "For each category of personal information collected, provide the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties ~~to~~ ~~with~~ whom the business sells ~~shares~~ personal information. The notice shall be

written in a manner that provides consumers a meaningful understanding of the categories listed."

- § 999.308(a)(1) requires businesses to disclose a comprehensive description of a business's online and offline practices which is burdensome and operationally challenging. Consumers should be provided with a privacy statement of a company's overall privacy practice that involves the collection, usage and sharing of the consumers' personal information.

§ 999.312. Methods for Submitting Requests to Know and Requests to Delete

- We request that this section be revised to allow for businesses that interact with consumers online only to not have the toll-free number requirement, but rather an email requirement per AB 1564 (Berman). The provisions specifying methods of submitting consumer requests appear to ignore recent changes to the underlying statute – specifically AB 1564's change to Civil Code 1798.130(a)(1)(A), which states that "*A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.*"
- The proposed rules also appear to potentially require a business to have three methods for requests, exceeding requirements of CCPA to have two designated methods. § 999.312 (a) and (b) say, businesses shall provide two or more designated methods for submitting requests to know and requests to delete, but § 999.312(c)(1), Example 2 references a business "shall offer three methods to submit requests to know." We recommend aligning the examples in this section with CCPA's statutory requirements.
- Also, § 999.312(d) mandates a two-step process that actually disempowers the consumer as many companies may operate a "self-serve" type process where consumers can make their choices as to information to be deleted. Requiring this two-step process could frustrate consumers. Companies should have the flexibility on process flow. Because of this, the two-step process should not be mandated.
- § 999.312(f) requires companies respond to all requests by treating it as a properly submitted request or sending specific directions to the consumer to correct any deficiencies *regardless* of what method is used to submit the request (designated method or not). It is unclear how this interacts with § 999.313 which requires business to confirm receipt of a request within 10 days of the date received and to respond within 45 (regardless of how long verification takes).

- CCPA requires that a business designate two or more methods for such requests to be submitted and this proposed language defeats the purpose of a business designating a method if consumers can still submit requests not using a designated method of submission (i.e. to be able to staff with trained personnel and meet statutory deadlines). Accordingly, we recommended striking § 999.312(f).

§ 999.313. Responding to Requests to Know and Requests to Delete

- Businesses are concerned that the CCPA's statutory requirement to provide certain specific pieces of personal information to consumers will create a risk of identity theft by malefactors. The prohibition on disclosing sensitive personal data elements to consumers represents good security practice. Additionally, the balancing tests laid out in the proposed regulations are helpful clarifications that businesses must weigh the benefit to the consumer of receiving specific pieces of personal information with the risk of facilitating improper disclosure of such information. We welcome the fact that de-identification of personal information serves as an acceptable method of deletion. This provision similarly strikes the proper balance between consumers' rights and the interests of businesses and the public in analyzing data that presents little risk to consumer privacy.
 - However, the 10-day period to confirm receipt of a consumer request should be at a minimum, 10 **business** days (§ 999.313(a)) and the 45-day period for responding to consumer requests should begin to run once the request has been verified (§ 999.313(b)). The proposed regulations recognize businesses' responsibility to verify requests properly, a task that may take days or weeks to complete and is reliant upon a consumer's collaboration in providing accurate information in a timely manner. After a request is verified, a company must then find the information that it holds on a consumer – information which may be kept in separate databases – and convert it into a form which can be delivered to the consumer. If receipt of the request initiates the 45-day period, businesses will be incentivized to rush through one of these processes, which does not serve the consumer. It is likely that in the months after the CCPA takes effect, businesses will receive a flood of consumer requests. The Attorney General should incentivize businesses to handle these requests responsibly and efficiently. Businesses should also be incentivized to utilize technologies to avoid potential unintended consequences of CCPA during consumer verification including, collecting more personal information than needed. Additionally, the requirement that businesses either execute or maintain "*a signed declaration under penalty of perjury*" in order to verify requests is confusing and unnecessary (§ 999.325(c)).

- § 999.313 excuses a business from disclosing certain sensitive personal information in honoring an individual's exercise of rights under CCPA; however, the list of data in this section does not include information that is extremely likely to cause harm to the consumer if disclosed to an unintended recipient, i.e. prescription drug or provider information, genetic information, information related to one's sex-life or sexual orientation, etc. Notably, this information is not always protected by HIPAA, GLBA or FCRA and may still be in-scope for CCPA. For example, a company may collect certain drug and provider information from a consumer during his or her shopping experience so that the company can match an individual to the best health plan that covers those drugs and has those providers in-network. If that drug and provider data is disclosed to an unintended recipient, it could reveal the consumer's medical conditions, mental health status, treatment for addiction, etc. That information is highly sensitive and likely to cause the consumer significant harm, whether embarrassment or potential financial harm, if obtained by an unintended recipient.
 - We respectfully request this section be expanded to include such sensitive personal information noted above. Further, where a business does disclose specific pieces of data as required under this section, meeting the verification requirements set forth in § 999.313(b)(1)-(4), we request a businesses be granted a safe harbor from any breach liability under CCPA or any other law if that information is disclosed to an unintended recipient despite compliance with these provisions.
- § 999.313(c)(3) states, "*A business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks.*" We recommend amending this to reference security risks to personal information of other consumers as well: "*substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's or another consumer's account with the business, or the security of the business's systems or networks.*"
- § 999.313(c)(4) prohibits the sharing of government identifiers when responding to requests to know. While we agree that account passwords and security question answers should not be disclosed, the prohibition on sharing social security numbers and other government identifiers may not align with a consumer's expectation. For example, a consumer may wish to access certain documents (e.g., medical or tax forms) with the intention of using or porting the documents for another purpose. Some consumers may want to

take those forms with the identifier and use it for another purpose and with redactions the document could be significantly less useful.

- We recommend allowing businesses to consider the intent of the consumer's request by deleting the current proposed language in (c)(4) and revising the language to state, "A business, taking into account the context and purpose of the consumer's request, may disclose a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, or any health insurance or medical identification in response to a verified request to know."
- § 999.313(c)(5) requires that if an access request is denied because of federal or state law, the consumer must be notified of the reason why. Under certain circumstances, this could have negative consequences in areas such as active law enforcement purposes, exercising or defending legal claims, regulatory investigation, or criminal inquiry. We therefore recommend that companies should also be allowed to include CCPA exemptions in their privacy policies and point consumers to those exemptions in the case that they deny a request because of an exemption listed in the privacy policy per CCPA.
 - Accordingly, we recommend the draft language be revised to, "*If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial, provided however that a business shall be deemed to be in compliance with this requirement if bases for denial are set forth in its privacy policy and the business refers the consumer to its privacy policy. If the request is denied only in part, the business shall disclose the other information sought by the consumer.*"
- § 999.313(d)(1) requires a business to treat a request to delete as an opt-out request if the identity of the requestor cannot be verified. This goes beyond the statutory basis of the CCPA. Also it calls into questions if a business cannot identify a requestor for purposes of deletion, how can it effectuate an opt-out? This may be feasible for online identifiers, where you can simply opt-out on an identifier basis, rather than delete. But in the non-identifier context this would not be feasible. In addition, this entire requirement runs counter to the verification requirements in the regulation. Consumer requests to delete personal information that cannot be verified

should not be treated as opt-out requests. Businesses should act upon requests when a consumer expresses a clear preference, and the regulations should not presuppose consumers' wishes by treating an unverified delete request as a do not sell preference. The CCPA provides consumers with several distinguishable rights that a consumer can choose to exercise. Requiring businesses to conflate consumer rights requests is eliminating consumer choice, may be confusing for consumers and is not supported by the CCPA statutory language.

- § 999.313(d)(6) requires a business to tell a consumer why they are denying their request to delete, which again could interfere with active law enforcement purposes, exercising or defending legal claims, regulatory investigation, or criminal inquiry. Also, if a business is not required to comply with the law because an exemption applies then it is not a "denial." The draft regulations suggest that businesses must provide the categories of sources of information, uses of information, categories of third parties to which information is disclosed or sold, and the purposes of such disclosures or sales for each category of personal information that it collects. These requirements require disclosures beyond what the statute requires, as the statute does not require such disclosure for each category of information.
 - Accordingly, we recommend the draft language be revised to, "(6) *In cases where a business denies a consumer's request to delete the business shall do all of the following: (a) Inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including any statutory and regulatory exception therefor, provided however that a business shall be deemed to be in compliance with this requirement if bases for denial are set forth in its privacy policy and the business refers the consumer to its privacy policy.*"

§ 999.314. Service Providers

- When a person or entity is providing services to an organization, that is not a business under CCPA, it would simply be illogical to impose any CCPA requirements on such entities. We recommend § 999.314(a) be revised to state: "*To the extent that a person or entity provides services to a person or organization that is not a business, no obligations under CCPA shall apply to such person or entity. and would otherwise meet the requirements of a "service provider" under Civil Code section 1798.140(v), that person or entity shall be deemed a service provider for purposes of the CCPA and these regulations.*"
- The new restrictions on service providers in § 999.314(c) also go far beyond the scope of the CCPA and contradicts the statutory definition of "business

purpose” and “service provider” in a few key ways. The text of the statute explicitly permits disclosures to “service providers” for a broad list of enumerated “business purposes” defined under the statute. Importantly, the statute defines “business purpose” to include both a business’s **or a service provider’s** operational purposes or other notified purposes. The statutory text also permits a service provider to use the personal information it receives from one business for such business purposes of both that business and the service provider where the use is authorized as part of the contracted-for “services” provided to the business. Because the service provider’s business purposes may include using personal information for the benefit of one business in a way that might also benefit other businesses, the CCPA statute is best interpreted to permit the service provider to use the personal information that it receives to provide services to all of its business partners, as long as such use is for the benefit of the business that provides the information to the service provider and also is contemplated in the “services” provided under the written agreement and otherwise consistent with the CCPA.

- For reference, § 999.314(c) states (with emphasis): “A *service provider shall not use personal information received either from a person or entity it services or from a consumer’s direct interaction with the service provider **for the purpose of providing services to another person or entity**. A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.*” The plain text of the section appears to prohibit service providers from using the personal information they receive from one entity to provide services to another person or entity, unless such services are necessary for detecting security incidents or preventing fraud or other illegal activity.
- The draft regulations improperly focus solely on the business purpose of the *business*, and ignore the fact that the statutory definition of “business purpose” in Civil Code 1798.140 (d) also includes the use of personal information for the “**service provider’s operational purposes or other notified purposes.**” Second, the activities included in the list of business purposes, also in 1798.140(d)(1)-(7) (such as “performing services on behalf of the business **or service provider**, including providing advertising or marketing services, providing analytic services, or providing similar services on behalf of

the business **or service provider**") require the combination and use of personal information received from and for the benefit of multiple businesses. As such, focusing solely on the business purposes of the business, as the proposed regulations do, would both render the bolded language above surplusage, contrary to well-established canons of statutory interpretation, as well as potentially render impermissible a number of the activities explicitly included on the list of permissible business purposes.

- The restrictions could also be interpreted to not allow certain internal operations for the service provider that might require the combining of data, including improving the quality of the service provider's services that it provides for businesses generally. While the CCPA allows a business to use or share personal information with a service provider that is necessary to perform a business purpose under certain circumstances, the proposed regulations appear to limit what businesses and service providers may do with data in a way that is unnecessary and threatens to harm the data economy. Given the broad definition of "personal information," this provision will limit a business' capacity to utilize its data for legitimate business purposes agreed to and defined within the boundaries of a contract, and in circumstances in which personal information will not be sold but only used by the service provider to provide services to the business. The CCPA statutory language already subjects service providers to robust standards.
 - We request that § 999.314(c) be revised to, *"A service provider shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose of providing services to another person or entity. A service provider may, however, combine personal information received from one or more entities to which it is a service provider, ~~or~~ behalf of such business, in order to provide the services specified in a contract with the business, or to the extent necessary to detect data security incidents, ~~or~~ protect against fraudulent or illegal activity, or engage in solely internal uses."*
- Additionally, § 999.314(d) requires that a service provider that receives but "does not comply" with a consumer's request to know or delete must inform the consumer of the reason for the denial, explain that the consumer should submit the request directly to the business, and when feasible, provide the contact information for the business. This requirement creates new obligations for service providers beyond the statutory text of the CCPA

because service providers do not have an obligation to comply with such deletion requests.

§ 999.315. Requests to Opt-Out

- Proposed regulations § 999.315(c) and (g) refer to user-enabled privacy controls. The CCPA emphasizes consumer choice. It specifically defines a mechanism, the “Do Not Sell” button, that businesses must make available to consumers on their Web sites to exercise their choices. It is not consistent with the statute to create this additional mechanism, nor is it clear that consumers, who use plug-ins, intend to opt out of CCPA sales. Currently, there are no such controls. And to the extent they are developed, codifying browser-based signals could give significant power to browsers, who could unilaterally turn on “Do Not Sell” or even do it selectively for certain companies. We support an industry-based efforts to develop consistent technical signals for “Do Not Sell” technology, an effort that has been underway for over a year.
 - In the event a browser-based program will be established, the law should empower the Attorney General to establish a uniform mechanism that browsers and devices would be required to implement so there is a level playing field for businesses and clarity for consumers.
 - At the very least, we recommend the following revisions:
 - *“(a) A business shall provide two or more designated methods for submitting requests to opt-out, including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information,” or “Do Not Sell My Info,” on the business’s website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information. User-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information shall not automatically opt-out consumers. Consumers must take an affirmative action to opt-out.”*

- *“(c) If a business collects personal information from consumers online, the business shall treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer, provided that the consumer undertakes an affirmative action to opt out of the sale of their information. Default opt-outs shall not constitute an affirmative step to opt out.”*
- Finally, CCPA does not include the requirement in § 999.315(f) to notify anyone to whom data was sold in the prior 90 days. This requirement is beyond the scope of CCPA and is not feasible given that businesses would not have control over how third parties treat the data.

§ 999.316. Requests to Opt-In After Opting Out of the Sale of Personal Information

- Requiring a two-step opt-in process is unnecessary and creates consumer confusion (§§ 999.301(a), 999.316(a)). Business should be given flexibility concerning how consumer should use an opt-in process. We recommend striking the reference to a “two-step” process. This requirement is not consistent with other laws or with consumer expectations. It would require businesses to build new systems and to make users jump through unnecessary hurdles in order to express a preference. It appears to nudge consumers toward a course of action, rather than empowering them to make their own decisions in a straightforward manner.

§ 999.317. Training; Record-Keeping

- § 999.317(g): The reporting requirements in § 999.317(g) exceed the scope of the AG’s authority and are not related to the purposes of the CCPA. We recommend that the record-keeping requirements in “g” should be struck. Nowhere in the CCPA is there a provision regarding record-keeping, and it is unclear what policy goal this requirement seeks to fulfil. It imposes an additional burden on businesses, which does not appear tied to consumer benefits or rights, and it requires the collection of more personal information and therefore goes against the spirit of the CCPA. Imposing additional record-keeping and disclosure requirements on businesses that handle the personal information of 4 million or more consumers appears arbitrary. The CCPA already requires that businesses provide multiple disclosures to consumers, and this information is unlikely to give them a more meaningful understanding of their privacy protections. Moreover, it is unclear what should constitute a request “complied with” vs. “denied” in that there are

various permutations such as lack of verification, or an applicable exemption. Also, should they be retained, at a minimum, the requirement to report the “median” number of days should be changed to “average” and this requirement should be delayed until at least January 1, 2021.

§ 999.325. Verification for Non-Accountholders

- § 999.325 illustrates a scenario of a business maintaining a card verification value (CVV) code. Companies are already prohibited from maintaining the CVV code per Payment Card Industry (PCI) DSS Requirement 3.2 compliance and therefore this should not be used as an example, given that this could be interpreted as a requirement.
- § 999.325(c) requires businesses to match from a California resident at least three pieces of personal information together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request and keep such declaration. This requirement imposes an additional burden on businesses with respect to the verification of identity and introduces a new record-keeping obligation, which CCPA did not intend to do. We recommend striking out this requirement in order to minimize unnecessary collection of more personal information to process an individual’s data subject access or deletion requests.

§ 999.326. Authorized Agent

- § 999.326 states a business’ privacy policy should explain how a consumer can designate an authorized agent to make a request under CCPA on the consumer’s behalf; however, no guidance is provided for the business as to what is acceptable to verify that the agent is in fact authorized. Without such guidance and a safe harbor for businesses complying with that requirement under CCPA, businesses risk creating or committing a data breach by facilitating the consumer’s request via authorized agent. We respectfully request further guidance on what constitutes an authorized agent, and a safe harbor for responding to consumer requests made by an authorized agent.

§ 999.330. Minors Under 13 Years of Age

- The CCPA should allow for any method permitted by the Children’s Online Privacy Protection Act (COPPA) for disclosure. This will allow for any new methods approved by the Federal Trade Commission to be also permitted under CCPA. Accordingly, this section should simply be a reference to the methods approved by the FTC for disclosure.
- The regulations should clarify the standard governing the “knowledge” a business must have to trigger a duty to obtain affirmative authorization for the sale of the personal information of consumers under 13 in order to ensure consistency with the Children’s Online Privacy Protection Act (COPPA).

A website operator is subject to COPPA when it has actual knowledge that it is collecting personal information from a user who is a child, not from “children” in general. This is reflected in the COPPA statute, regulations and longstanding FTC commentary. See, e.g., 15 U.S.C. 6502(a)(1) (“It is unlawful for . . . any operator that has actual knowledge that it is collecting personal information from **a child**, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b).”) (emphasis added); 16 C.F.R. 312.3 (“It shall be unlawful for . . . any operator that has actual knowledge that it is collecting or maintaining personal information from **a child**, to collect personal information from a child in a manner that violates the regulations prescribed under this part”) (emphasis added); FTC, Complying with COPPA: Frequently Asked Questions A.14 (“COPPA covers operators of general audience websites or online services only where such operators have **actual knowledge** that a child under age 13 is the person providing personal information.”). Requiring a standard different from what is required under COPPA would cause confusion and potentially complicate a business’s efforts to protect minors and their personal information. What is more, it would be impermissible under COPPA’s preemption clause. See 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 that is inconsistent with the treatment of those activities or actions under this section.”)

- § 999.330(a)(1) should also be modified to make clear that a consent methodology that satisfies COPPA necessarily satisfies the “affirmative authorization” requirement of the CCPA. Under COPPA’s preemption standard, it is clear that the Attorney General may not impose additional or otherwise inconsistent consent requirements beyond those imposed by COPPA.
 - Accordingly, we recommend the draft language be revised to, “A business that has actual knowledge that it collects or maintains the personal information of a child~~ren~~ under the age of 13 shall utilize ~~establish, document, and comply with~~ a reasonable method, in light of available technology, for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. Verifiable parental consent that complies with the Children’s Online Privacy Protection Act and regulations thereunder shall satisfy this obligation. ~~This affirmative authorization is in addition to any verifiable parental consent required under the Children’s Online Privacy Protection Act, 15 U.S.C. sections 6501, et seq.~~”

§ 999.331. Minors 13 to 16 Years of Age

- § 999.331(a): We suggest the following changes to § 999.331(a) “A business that has actual knowledge that it collects or maintains the personal information of minors at least 13 and less than 16 years of age and wishes to sell such personal information, shall establish, document, and comply with a reasonable process for allowing such minors to opt-in to the sale of their personal information, pursuant to section 999.316.” If a company does not plan to sell this personal information, they need not have an opt-in mechanism. Accordingly, these revisions should be made.

§ 999.336. Discriminatory Practices

- § 999.336 permits a business to offer a price or service difference if “reasonably related to the value of the consumer’s data” (as defined in § 999.337). Civil Code 1798.125, as recently amended, allows financial incentives if “reasonably related to the value provided to the business by the consumer’s data.”
 - We recommend amending the rule to align with the recent amendments to Civil Code 1798.125 in AB 1355 (Chau).

§ 999.337. Calculating the Value of Consumer Data

- As noted in our comments in section § 999.307, we propose striking § 999.337, which describes the methods in calculating the value of consumer data. This requirement to disclose the value and methodology goes beyond CCPA statutory language. We urge that this requirement be struck from the draft regulations.

TechNet thanks you for taking the time to consider our comments on the proposed CCPA regulations. It is imperative for businesses and consumers in California that CCPA regulations move forward with the goal of providing clarity to the statute. We urge that any new requirements beyond those delineated in the statute be removed from the regulations or, at the very least, have a delayed effective date. Regulations should help facilitate compliance on the part of California 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: Mohamed Hafez [REDACTED]
Sent: 12/6/2019 3:02:48 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: The CCPA needs several clarifications


Hi, I'm the president/developer of a small 3 person app company, and am very concerned about the impact of the CCPA on my business. There are several clarifications that would really help us out, and I'm sure a lot of other small business as well:

- The rule for determining if the Personal Information of 50,000 consumers, households, or devices has been received, thus making the CCPA applicable to a small business, needs to be clarified as following:
 - While "consumer" is defined as "a natural person who is a California resident", its not clear whether "devices" means just devices used in CA or belonging to CA residents, or if 50,000 devices accessing the app/website from anywhere in the world makes my small business susceptible to this law. The latter case will end up placing a lot of onerous regulation and costs on small businesses, which doesn't seem to be the intent of this law, so I hope you clarify that it's only CA devices that are concerned. What if a small out of state business has 50,000 users that access their site from devices almost entirely in New York, but has a handful of them in CA? It wouldn't make sense to have them be subject to this entire set of regulations, and that doesn't seem to be the intention. **It would be great to specify that explicitly by defining "devices" as devices used in CA or belonging to a CA resident.**
 - Lets say I collect Personal Information on a CA consumer, and on the two devices they use to access my app/website/service. When counting towards the 50,000 limit, does this count as 1 because this is all the information of just one person, 2 because it's two devices, or 3 because there's information on one consumer their two devices? **This needs to be specified explicitly.**
- The definition of Unique Personal Identifier needs to explicitly omit "session cookies", which are necessary for the functioning of a lot of websites, including mine, and *are automatically deleted by a browser when the user closes the browser*, making them useless at being "used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services". Note that I'm not talking about persistent cookies, and definitely not tracking cookies, which rightfully fit this description. The reason this is important to me is I don't collect any Personal Information for random visitors of my who don't intentionally sign up for an account in order to keep under the 50,000 limit, but I have to place that session cookie there for things to function correctly, like to display error or success messages after a user submits a form. The session cookie will be different in the next "session", i.e. the next time the user visits the site, so it's useless for tracking anyway, it's just a basic mechanism to add statefulness to website. **It would be great if session cookies could explicitly be whitelisted as not counting as a Unique Personal Identifier.**
- The 50,000 consumer/device limit is stated as follows (emphasis mine): "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." It would be great if the definition of commercial here explicitly excluded IP address, not tied to any user, that is used **only for diagnostic purposes**. What I mean is it is common practice to log

every time an IP address makes a specific request of your server, so you can see if some group of IP Addresses is making excessive requests in an attempt to take the site down (called a Denial of Service attack), see if a particular IP address is trying to log in with bad passwords over and over trying to guess the password of a particular user, etc. This is all standard practice, is necessary to keep a service running these days, and would be really difficult to tie to an individual anyway without a warrant. If these logs are disposed of in a timely manner, they shouldn't count as Personal Information and shouldn't count towards the 50,000 consumer/device limit. This should be made explicit to ease the burden on small businesses that might otherwise come under the scope of this law.

These questions and points of view can be found on law blogs concerning the CCPA all over the internet, many people are worried and confused about these points, and clarification would be greatly appreciated by many small business owners like myself. Thank you very much for your consideration.

Sincerely,
Mohamed Hafez,


President, SubstituteAlert Inc.

Message

From: Friedrich, Kate (TR General Counsel) [REDACTED]
Sent: 12/7/2019 12:00:51 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Thomson Reuters Written Comments to CA Atty General on Draft CCPA Regulations
Attachments: Thomson Reuters Comment Ltr to CA Attorney General on Draft CCPA Regulations.pdf
Importance: High

Attached please find Thomson Reuters written comments in response to the Attorney General's Draft CCPA Regulations. If you have any questions, please do not hesitate to be in contact with me.

Sincerely,

Kate Friedrich
Vice President, Government Affairs
Thomson Reuters
the answer company

Phone: [REDACTED]
[REDACTED]
thomsonreuters.com



THOMSON REUTERS

December 6, 2019

Via Email and Mail

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

RE: Written Comments on Draft CCPA Regulations

To Whom It May Concern:

Thomson Reuters submits these comments in response to the Attorney General's Notice of Proposed Rulemaking to implement the California Consumer Privacy Act ("CCPA" or "Act"). As California breaks new ground with the nation's first general data privacy law, other states, federal officials, and data protection regulators around the world are looking to California to both promote meaningful individual privacy rights and advance important principles of personal and public safety and free speech. The draft CCPA regulations provide much-needed clarification of the CCPA's statutory requirements, and we appreciate the significant work and careful attention that the Attorney General's Office has spent on this unprecedented and critically important undertaking.

Thomson Reuters' customers rely on our services to access legal, regulatory, and business information that is critical to (for example) prevent and investigate money laundering, fraud, and other criminal activities; comply with legal and regulatory requirements (such as "know your customer" laws); find missing children and address human trafficking; and locate witnesses and prepare for litigation. The draft CCPA regulations appropriately acknowledge the importance of these types of public policy practices,¹ and Thomson Reuters requests that the Attorney General provide further clarification to ensure that the CCPA regulations do not unintentionally frustrate our customer's ability to access and use these information services to keep people and their property safe and engage in similar activities that advance the public interest.

¹ See, e.g., Draft CCPA Regulations § 999.314(c) (specifying that service providers may "combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to detect security incidents, or protect against fraudulent or illegal activity.")

1410 Spring Hill Road
McLean, VA 22102

T: [REDACTED]



Specifically, Thomson Reuters asks the Attorney General to:

- strike the new regulatory requirement that businesses pass-through opt-out requests to third parties, which could produce results inconsistent with the consumer's expectations;
- eliminate the new requirement that businesses treat unverified deletion requests as requests to opt-out;
- include measures to minimize the risk that bad actors will abuse the CCPA's consumer rights to evade detection and further their harmful activities;
- make the notice of collection of personal information time bound to apply only to data collected after the effective date of the CCPA.

Each of these requests is discussed in more detail in the following sections.

I. Requiring businesses to pass through opt-out requests will have the unintended effect of harming consumers.

Under the proposed regulations, if a business receives an opt-out request, it must not only itself stop selling that consumer's data but also communicate that consumer's request to any third party to whom the business sold that consumer's data in the previous 90 days. § 999.315(f).² The pass-through requirement is a new obligation that is not contained in the CCPA statute. While well intended, this new provision is not necessary to further the purposes of the Act and could have the contrary effect of frustrating the Act's goals.

First, the new pass-through requirement is likely to produce results that are inconsistent with the consumer's reasonable expectations and preferences. For example, if a consumer has a bad customer service experience with one business, she might close her account and ask the business to opt her out of its sale of her personal information. When submitting this request, the consumer might reasonably expect that this opt-out request applies only to future sales (not past sales) and to that specific business. As a result, she might be surprised to learn that this opt-out has a downstream ripple effect that could affect other businesses that the consumer might want to affirmatively permit to sell her information (such as Thomson Reuters, which makes data commercially available for anti-fraud and similar public policy purposes that benefit that consumer and other consumers). To avoid this ripple effect, the consumer either would need to withdraw her opt-out request before it is communicated to downstream recipients of the data or opt back in through a stringent two-step process for every business where she wants to permit data sales. This result would frustrate the Act's goals by chilling the consumer's willingness to exercise her opt-out right and defying the consumer's actual preferences.

² As the regulations are drafted, this pass-through requirement would appear to apply only where the recipients of personal information are permitted to further sell such information. Consequently, if the contract between the business and the third party prohibits the third party from selling the data, the business should not need to notify the third party of a consumer's opt out.



Second, this new requirement also could harm other consumers who significantly benefit from sales of personal information. While a significant portion of the information that Thomson Reuters makes available through its Westlaw legal research and CLEAR services is publicly-available information sourced from government records,³ we also purchase information from businesses that make data commercially available. If these businesses are required to pass-through opt-out requests, our customers could be stymied in their efforts to use our Westlaw and CLEAR services. Ultimately, this result harms consumers, who suffer the consequences of a fraudster or other bad actor who may go undetected if Thomson Reuters is required to restrict customers' access to the information that otherwise would be available through its services.

Third, imposing a new pass-through obligation on businesses also is inconsistent with the statutory text. The CCPA statute contains one explicit pass-through provision; Section 1798.105(c) requires a business to forward a consumer's *deletion* request onward to its service providers. It is a longstanding rule of statutory construction that where the legislature "includes particular language in one section of a statute but omits it in another . . . , it is generally presumed that [the legislature] acts intentionally and purposely in the disparate inclusion or exclusion."⁴ Consequently, the Attorney General should not read a new pass-through requirement into the statute because doing so would be contrary to the presumption that the California legislature intentionally and purposely intended to exclude such a requirement.

Fourth, the stated policy concerns underlying the pass-through requirement for opt-outs already are addressed through other regulatory provisions. The Initial Statement of Reasons ("ISOR") accompanying the draft regulations suggests the new pass-through requirement for opt-out requests is needed because consumers may not know who the business sold the information to and therefore cannot effectively opt out of sales by downstream recipients of the data. ISOR at 25. However, the proposed regulations already include other safeguards to address this concern. For example, the proposed regulations mandate that a business that does not collect information directly from consumers but intends to resell personal information must either contact the consumer directly to provide notice of resale or contact the source from which they received the personal information to confirm that the consumer received notice at collection. § 999.305(d).

For these four reasons, we encourage the Attorney General to strike Section 999.315(f) of the draft CCPA regulations.⁵

³ This publicly available information is not governed by the CCPA. Cal. Civ. Code § 1798.140(o)(2).

⁴ See, e.g., *Bates v. United States*, 522 U.S. 23, 29-30 (1997) (citing *Russello v. United States*, 464 U.S. 16, 23 (1983) (quoting *United States v. Wong Kim Bo*, 472 F.2d 720, 722 (CA5 1972))).

⁵ Relatedly, the Attorney General should revise Section 999.315(d) to clarify that businesses have broader flexibility in the types of granularity that they provide in their opt-out requests: "*In responding to a request to opt-out, a business may present the consumer with the choice to opt-out of sales of certain categories of personal information, to certain categories of third parties, or for certain types of purposes as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices.*"



Alternatively, if the Attorney General chooses to retain this new pass-through requirement, then Thomson Reuters requests that the Attorney General clarify that businesses and recipients of the information need not respond to the opt-out request if the information will be used for public policy purposes that are already recognized as exemptions in the CCPA statute and draft regulations. Specifically, we recommend that the Attorney General include the following language in **bold** to Section 999.315 of the draft CCPA regulations:

*A business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the consumer's request that the consumer has exercised their right to opt-out and instruct them not to further sell the information. The business shall notify the consumer when this has been completed. **A business or a third party may, however, sell the information to the extent necessary to detect security incidents, or protect against fraudulent or illegal activity.***⁶

These revisions are supported by the CCPA's recognition that the statute is not intended to restrict a business's ability to prevent, detect, or defend against unlawful activities (such as fraud, human trafficking, and money laundering) and therefore further the statute's goals.⁷

II. **Businesses should not be required to treat unverified deletion requests as requests to opt-out.**

Section 999.313(d)(1) of the draft CCPA regulations adds a new requirement that businesses treat deletion requests that cannot be verified as opt-out requests. For reasons similar to the concerns raised in Section I above, this new obligation would not further any statutory purpose—it does not accurately reflect the consumer's actual preferences, inadvertently diminishes the consumer's control over their personal information, and may unintentionally chill the consumer's willingness to exercise their deletion right. We therefore encourage the Attorney General to strike this new requirement from the final regulations.

From the consumer's perspective, converting the deletion request into an opt-out does not accurately reflect the consumer's stated preferences. Because businesses must notify consumers of their CCPA rights, the consumer is well aware that they have both a right to request deletion and a right to opt-out. The fact that this informed consumer exercises only her

⁶ Thomson Reuters notes that the additional language proposed mirrors, nearly identically, an analogous exception set forth for service providers in the Proposed Text of Regulations in section 999.314(c).

⁷ See, e.g., Cal. Civ. Code § 1798.105(d), § 1798.140(d), § 1798.145(a); see also Draft CCPA Regulations § 999.314(c); ISOR, at 22 ("The subdivision, importantly, provides an exception for security and anti-fraud purposes. This exception is consistent with the purposes of the CCPA and with similar exceptions in other California privacy laws. (See Student Online Personal Information Protection Act, Bus. & Prof. Code, § 22584; California Financial Information Privacy Act, Fin. Code, § 4056; Consumer Credit Reporting Agencies Act, Civ. Code, § 1785.15.).").



deletion right (and not also her opt-out right) when contacting the business is evidence that she explicitly did not want to opt-out at that time. There are multiple reasons why a consumer might want to request deletion, but not opt out. For example, given the new pass-through requirement in Section 999.315(f), she might want to delete her data but not trigger the cascading opt-out to downstream recipients of the data, which (as explained above in Section I, similarly could chill the consumer's willingness to exercise the deletion right if the deletion right is automatically converted into an opt-out that is passed through to downstream recipients of the data). Of course, the consumer may choose to change her mind and exercise her opt-out rights at any time (or may exercise her opt-out right simultaneously with her deletion right). Consequently, the proposed new requirement inadvertently and unnecessarily diminishes the consumer's control over her personal information by preventing the consumer from effectively exercising only the deletion right.

Requiring the business to convert the deletion request into an opt-out request also creates practical challenges. For example, a business might designate a toll-free telephone number and a designated email address as its two methods for receiving a deletion request but use a "Do Not Sell My Info" link and a browser privacy setting as its two methods for receiving an opt-out request. To verify the identity of the consumer submitting the deletion request, and considering the factors set forth in the draft regulations, the business might require the consumer to provide the following personal information: full name, account number, and date of birth. In contrast, the "Do Not Sell My Info" link and browser privacy setting might operate based on a unique cookie ID or similar browser or device identifier. If, when submitting his deletion request by email, the consumer provides an email address that is not in the business's records, an invalid account number, and no name or date of birth, the business likely would conclude that the request is not verifiable and inform the consumer that it will not comply with the request. It may not technically be possible, however, to successfully convert this deletion request into an opt-out request because the information that the consumer provided is not the type of information needed, from a technological perspective, to effectuate the opt-out (i.e., the cookie ID or similar browser or device identifier).

Because the new requirement to convert an unverifiable deletion request into an opt-out request is contrary to the consumer's expressed choice and unworkable in practice, Thomson Reuters requests that the Attorney General remove Section 999.313(d)(1) from the final regulations.

III. The regulations should include protections to minimize the risk that bad actors will abuse the CCPA's consumer rights to further their own unlawful purposes.

Since the European Union's General Data Protection Regulation (GDPR) took effect, there have been a number of reports and research studies on how fraudsters, identity thieves, hackers, and other criminals abuse the GDPR's consumer rights to further their own malicious and unlawful purposes.⁸ As the Attorney General prepares to implement and enforce the

⁸ See, e.g., Pavur & Knerr, "GDPArrrr: Using Privacy Laws to Steal Identities," Blackhat USA 2019 Whitepaper, available at <https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf>; Martino et al., "Personal Information



nation's first comprehensive general data privacy law, it is critical that the regulations are carefully crafted to avoid similar gaps and ambiguities that bad actors will try to exploit.

The CCPA grants the Attorney General specific authority to enact broad exceptions that further this important purpose. Section 1798.185(a)(3) of the CCPA directs the Attorney General to adopt regulations that 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." Significantly, the statute is *not exclusive* in its mandate to enact exceptions that address trade secret theft and intellectual property infringement. Consequently, the Attorney General can (and should) include an exception in the final regulations clarifying that the statute does not impede any efforts to address money-laundering, fraud, human-trafficking and missing persons reports, and other unlawful activities. This exception would also not impede activities that promote the public interest. This can be achieved by adding the following new section to the regulations:

Neither these regulations nor the California Consumer Privacy Act restrict a business, service provider, third party, or any other person or entity from preventing, detecting, investigating, or responding to security incidents, theft of trade secrets or intellectual property infringement, fraudulent or illegal activity, or threats to personal or public safety and property.

Notably, these activities appear to already be exempt under the blanket exceptions contained in Section 1798.145 of the CCPA statute, which similarly prevent the statute from being applied or enforced in a manner that would impede a business from engaging in a wide range of activities in the public interest.⁹ However, an explicit exception in the final regulations would be helpful because the regulations, as drafted, could be interpreted to be in tension with these broad statutory provisions. For example, the draft regulations explicitly permit a service provider to broadly use personal information to "detect security incidents, or protect against fraudulent or illegal activity" but does not contain parallel provisions for third parties or other entities to engage in the same activities, notwithstanding the fact that the ISOR recognizes that similar exceptions are common across other California privacy laws.¹⁰ Adding the new section proposed above to the final regulations would align the regulations with the broad purposes contained in Section 1798.145 of the statute and avoid any uncertainty regarding the scope of these exceptions, which promote important principles of personal and public safety and free speech.

Leakage by Abusing the GDPR 'Right of Access,'" available at <https://marianodimartino.com/dimartino2019.pdf>; Andrew Ross, "How Cyber Threats Could Grow Under GDPR," Information Age (May 14, 2018), available at <https://www.information-age.com/cyber-threats-gdpr-123472491/>.

¹⁰ ISOR, at 22; see also CCPA Draft Regulations § 999.324(b) (allowing a business that suspects fraudulent or malicious activity from a password-protected account to not comply with a request to know or delete until further verification can be completed); § 999.315(h) (specifying that a business may deny a request to opt-out if it has a "good faith, reasonable, and documented belief" that the request is fraudulent).



IV. Explicit notice must only be required after the effective date of the CCPA.

Section 999.305(d) of the draft CCPA regulations should be revised to acknowledge that in some cases downstream third parties sell personal information that was collected years ago and that retroactively applying the explicit notice requirement to this previously collected data would be impractical and unintended by the legislature. Thomson Reuters, therefore, requests that the Attorney General make the notice of collection of personal information time bound to apply only to data collected after the effective date of the CCPA.

Thomson Reuters requests that the Attorney General revise Section 999.305(d) as follows:

*(d) A business that does not collect information directly from consumers does not need to provide a notice at collection to the consumer, but before it can sell a consumer's personal information, it shall do either of the following, **for personal information collected after the effective date of the CCPA:***

(1) Contact the consumer directly to provide notice that the business sells personal information about the consumer and provide the consumer with a notice of right to opt-out in accordance with section 999.306; or

(2) Contact the source of the personal information to:

a. Confirm that the source provided a notice at collection to the consumer in accordance with subsections (a) and (b); and

b. Obtain signed attestations from the source describing how the source gave the notice at collection ~~and including an example of the notice.~~ Attestations shall be retained by the business for at least two years and made available to the consumer upon request.

Thomson Reuters appreciates the opportunity to submit these comments, and we look forward to working with the Attorney General and his staff to achieve the shared goals of promoting consumer privacy and protecting personal and public safety.

Sincerely,

Steve Rubley
Managing Director, Government Segment

Message

From: Pierre Valade [REDACTED]
Sent: 12/6/2019 7:43:55 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Zoe Vilain [REDACTED]
Subject: To the attention of Deputy Attorney General Kim - Comments with regards to CCPA
Attachments: 20191206 - Jumbo Privacy - Written comments regarding the proposed CCPA regulations - .pdf

To the attention of Deputy Attorney General Kim

Dear Deputy Attorney General Kim,

Please find attached a letter to your attention containing our comments regarding the proposed CCPA regulations.

I am available for any queries,

Best regards,
Pierre Valade
Jumbo Privacy
www.jumboprivacy.com



Jumbo Privacy,
2121 Atelier Inc.
20 Jay Street, suite 624
Brooklyn, NY 11201
USA

Lisa B. Kim
Deputy Attorney General
California Department of Justice
Consumer Law Section – Privacy U.
300 South Spring Street, 1st Floor
Los Angeles, CA 90013
USA

December 6th, 2019

By email (privacyregulations@doj.ca.gov)

Subject: Written comments regarding the proposed CCPA regulations

Dear Deputy Attorney General Kim,

We are writing to you to suggest some comments to the proposed rulemakings of the California Attorney General with regards to the California Consumer privacy Act ("CCPA").

2121 Atelier Inc, which is a Delaware corporation, with its principal place of business located at 20 Jay Street, suite 624 – Brooklyn, NY 11201, owns and operates an iOS and Android mobile application entitled "Jumbo Privacy", available at the following URL address: www.jumboprivacy.com.

Jumbo Privacy enables users to take back control of their privacy, notably by suggesting them changes to their privacy settings, or deleting old content on their dedicated social media accounts. It is available for download worldwide, and notably for California residents.

As a company, we believe that privacy rights are fundamental rights, therefore that the exercise of such rights should be easy and accessible to all individuals in particular to consumers. The current state of the data industry, its opacity, and the numerous data scandals surrounding it, show us that there is a significant imbalance between consumer's rights and business practices leading to a quasi-impossibility for a consumer to exercise his privacy rights.

Jumbo Privacy
20 Jay Street, suite 624
Brooklyn, NY
11201

RJ

We have been following with great attention California's Congress progressive proposal for the CCPA, which will provide Californian consumers with greater privacy protection, notably through the introduction of a key player: the "authorized agent".

We believe that the use, or hiring, of an authorized agent in the exercise of data privacy rights is one of the best remedies to the imbalance between data processors and consumers. In particular since such authorized agent will most likely ensure effectiveness of the exercise of a consumer's privacy rights by being dedicated to such mandate and knowing best available laws.

Please find attached our suggestions and comments to the proposed rulemakings of the California Attorney General notably regarding provisions related to such "authorized agent".

Sincerely,



Pierre Valade,
Jumbo Privacy
www.jumboprivacy.com



Appendix 1
Jumbo Privacy Proposed Amendments

1. § 999.312. Methods for Submitting Requests to Know and Requests to Delete

“(f) If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either:

(1) Treat the request as if it had been submitted in accordance with the business's designated manner, or

(2) Provide the consumer with specific directions on how to ~~submit the request or~~ remedy any deficiencies with the request, if applicable.”

Jumbo Privacy Comment: We would like to suggest that the consumer, or an authorized agent, be allowed to submit a request in a manner of its choosing, even if such manner defers from the designated methods of submission of the business, and that the business be forced to comply with such request not submitted through its designated methods. This would ensure that the request is submitted in a manner best suited to the consumer and his needs, without the business imposing its processes, helping balancing relations between consumers and data processors.

2. § 999.313. Responding to Requests to Know and Requests to Delete

“(b) Businesses shall respond to requests to know and requests to delete within ~~45~~30 days. The ~~45~~30- day period will begin on the day that the business receives the request, regardless of time required to verify the request. If necessary, businesses may take up to an additional ~~45~~30 days to respond to the consumer's request, for a maximum total of 9060 days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than ~~45~~30 days to respond to the request.”

Jumbo Privacy Comment: Requests to know and requests to delete very often concerns sensitive personal information that need to be rapidly addressed, notably requests to delete personal information such as a consumer's IDFA that is in practice used by businesses for advertising targeting on a daily basis. We would suggest that a 30 days' delay would be more appropriate to such requests.

3. § 999.326. Authorized Agent

“(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, the business may require that the consumer:

(1) Provide the authorized agent written permission to do so; and

PV

(2) Verify their own identity directly with the business, in case the authorized agent has not provided reasonable proof of the consumer's identity."

Jumbo Privacy Comment: It seems reasonable to state that consumers would use or hire an authorized agent to avoid having to manage data requests themselves. We believe that allowing a business to ask the consumer for additional identity verification would lead to addition of heavy processes and unnecessary delays to the processing of the original data request.

Therefore, we would suggest this addition to ensure that the business needs to, or can, verify the consumer's identity of the consumer only if the business can prove the authorized agent has not provided reasonable proof of such consumer's identity. This addition would prevent any unnecessary verification by the business, and disproportionate verification measures, ensuring respect of the consumer's privacy rights.

R

Message

From: Derek Onysko [REDACTED]
Sent: 12/7/2019 12:06:39 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Written Comment to Proposed Regulations for CCPA

The California Consumer Privacy Act of 2018 (the “CCPA”) provides California consumers with the right to request a business to disclose:

1. Specific pieces of personal information the business has collected about the consumer;
2. Categories of personal information it has collected or sold about that consumer;
3. The purpose for which it collected or sold the categories of personal information; and
4. Categories of third parties to whom it sold the personal information.

See CCPA §§ 1798.100, 1798.110, 1798.115.

CCPA section 1798.130(a)(1) directs businesses to “[m]ake available to consumers **two or more** designated methods for submitting requests for information required to be disclosed pursuant to Section 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.”

CCPA section 1798.185(a)(7) supplements section 1798.130(a)(1) and directs the Attorney General to establish rules and procedures to further the purposes of section 1798.110 and 1798.115 and to facilitate a consumer’s . . . ability to obtain information pursuant to Section 1798.130, **with the goal of minimizing the administrative burden on consumers**

The proposed regulations fail to fulfill the CCPA’s mandate to minimize the administrative burden on consumers who exercise their rights under CCPA sections 1798.110 and 1798.115.

The Attorney General estimated that the CCPA vested California consumers with the right to know how their data is being used by approximately “15,000 to 400,000 businesses” in California. *See* Notice of Proposed Rulemaking Action 11, Oct. 11, 2019. Yet, the Attorney General declared that there will be “no cost impacts on consumers” from exercising their rights from these businesses. *Id.* at 14.

Assuming it takes just one minute for California consumers to exercise their right to know via a toll-free number or website, at a \$12 California minimum wage for base consumer costs, it would cost a single California consumer between \$3,000 and \$6,666.66 to enforce his or her right to know against all these businesses.

Of course, most California consumers will not enforce rights against even 15,000 businesses. It would not be unreasonable, however, for 200 businesses to have collected personal information about a California consumer. At a more reasonable time of ten minutes to enforce a right to know against a business, it would take 33 hours and cost \$400 to exercise all rights to know against 200 businesses. Extrapolated to all California consumers, that’s \$11,867,113,500 if every California consumer enforced his or her rights to know. The proposed regulations fail to minimize administrative costs on consumers and shifts the billions of dollars of CCPA costs onto California consumers.

The Federal Trade Commission established the National Do Not Call Registry in 2003 to great success and satisfaction of the American public. The Attorney General could propose regulations to establish a similar registry for California consumers. Such a registry would establish a “one-stop shop” for California consumers to enforce their privacy rights. There would be less of a burden on businesses to comply with a standardized registry. And the costs to California

consumers would be reduced to almost zero, fulfilling the CCPA mandate. A registry could be established for consumers to enforce their right to know, right to delete, and right to opt-out.

Please re-consider the proposed regulations to with the goal of reducing the administrative costs to consumers. As currently drafted, the proposed regulations discourage reasonable consumers from enforcing their privacy rights because of the exorbitant costs associated with enforcement. A statewide registry will provide for more effective enforcement. Without a registry, the CCPA affords California consumers new privacy rights but without any remedy to enforce those rights.

Message

From: MFF [REDACTED]
Sent: 12/1/2019 12:01:33 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: privacy [privacy@doj.ca.gov]
Subject: Written Comments [Before 12/6/19@5:00pm-PT]
Flag: Follow up

To: Privacy Regulations Coordinator
California Office of the Attorney General
300 So. Spring St., First Floor
Los Angeles, CA 90013
E: PrivacyRegulations@doj.ca.gov

cc: Privacy Enforcement and Protection Unit
E: privacy@doj.ca.gov

To Whom It May Concern:

The aforementioned comments and questions concern the need of active enforcement for protection of Safe at Home program participants.

1) What department, whom and how should Safe at Home members contact for enforcement purposes, per CA Government Code sections 6205-6217, specifically CA Govt. Code section 6208.1, regarding immediate and permanent online removal of 'personally identifiable information' ("PII") from data brokers, data mining and data aggregators, whose software (from incompetent and complacent CTO's & their tech team members) continuously and consistently allow PII to be placed online as the "site hosts" which affect Safe at Home members?

(The Safe at Home managerial staff has been complacent & clueless for years, along with certain employees in the Executive Office at the Secretary of State Office, including but not limited to, Chief Counsel Steve J. Reyes, to not communicate with Consumer Law Section-Privacy Unit, Stacey D. Schesser, Supervising Deputy Attorney General, CIPP/US, regarding immediate 'Call to Action' safeguards and protection enforcement for Safe at Home members.)

Enough is enough. It has been outrageous. There has been no "liberty and justice under law." Moreover, per the press release on Thursday, July 18, 2012, when Kamala D. Harris announced the creation of the Privacy Enforcement and Protection Unit, there has been no right to privacy. See the entire press release. One sentence included these words: "The California Constitution guarantees all people the inalienable right to privacy." ;

2) Why hasn't, AND when will, the Privacy Enforcement and Protection Unit do any active enforcement for Safe at Home Program Participants? [If another Govt. Code section needs to be explicitly added to give mandatory enforcement power to CA's DOJ, then please so advise. If so, Assemblymember Ed Chau for the 49th District, and his District Director, Daisy Ma, will be immediately contacted.]

Finally regarding question & comment for #2, for years and years the Privacy Enforcement and Protection Unit, seemingly has acted like the monkeys who "see no evil, hear no evil and speak no evil," when the Unit should have corrected and enforced against so much online PII evil. With what I know and have been told about, this Unit has done no active enforcement for Safe at Home members, except their passive "Online Opt-Out Form" and their outdated, antiquated and incomplete "Directory Web Site List With Opt-Out Information" ("List"), which MUST be immediately revised. (See below.)

Q: Where are the email addresses for all the data mining, data broker and data aggregator companies on their "List?"

Q: Why only snail mail information? (I know for a fact that all of the data mining companies, et. al, have email addresses AND/OR contact us pages or links to easily and quickly request removal of one's PII, because I have done it and became an expert in online PII removal.)

Finally, the "Opt-Out Form" fails to give any protection to Safe at Home members to press-related companies, including magazines like PEOPLE, formerly owned by Time, and now owned by the Meredith Corporation (located in Des Moines, Iowa). The attorney for PEOPLE, Robert A. Bertsche at Prince, Lobel Tye, LLP in Boston, MA, will not remove online letters, names of the letter writer(s), and the cities and states for Safe at Home members. (Exact reason can be provided upon request.)

****Any individual can be found online with merely a name, city and state. (I obtained atty Bertsche's home address online with just his name and state.)****

3) When will the "Opt-Out Written Demand Form for California Safe at Home Program Participants" ("Form") of 7_13_17, be revised, rewritten, and updated to reflect less unnecessary and unneeded information on page 1 of the Form? Page 1 of the Form, needs immediate serious reconstruction and revisions;

4) The "List" must be update immediately because it contains outdated, antiquated and old information. Many of the data broker, data mining and data aggregator companies are not even included. Where are the email addresses for PII removal? Where are the website addresses? Where are the 'Contact Us' links for Safe at Home member to quickly and expeditiously use to be the best and easiest way for companies to be contacted for immediate PII online removal.

Q: Does the CA DOJ think abused women have time to take the time to get their online PII removed by snail mail? (Hypothetical Q: Are you serious?)

In sum, whomever composed the List and finished it on 6_30_17 did a real sloppy, complacent, incompetent and nasty negligent job. (You can quote me too.)

5) Under CA Government Code, section 6254.21 (3)(f), Safe at Home members should be included as an "elected or appointed official" or in the alternative, include a separate code section to specifically include them.

...

The above information took over two hours to intelligently, factually and carefully compose. If the CA DOJ would like to consider hiring me as a consultant, I will seriously entertain the offer.

In the meantime, the CA DOJ offices in Los Angeles and in San Francisco have a tremendous amount of work to do on behalf of Safe at Home members.

Respectfully,
Safe at Home Member
Los Angeles, CA
Sat, 11/30/19@4:01pm(PT)

Message

From: Anthony Stark [REDACTED]
Sent: 12/7/2019 12:34:21 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Henry Schuck [REDACTED]; Margaret Gladstein [REDACTED]
Subject: Written comments - §§ 999.300 through 999.341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations concerning the California Consumer Privacy Act
Attachments: ZoomInfo - Written Comments on Draft CCPA Regulations (12.6.19).pdf

Dear Privacy Regulations Coordinator:

Attached please find written comments submitted on behalf of ZoomInfo regarding the proposal to adopt sections §§ 999.300 through 999.341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations concerning the California Consumer Privacy Act.

Please let me know if you are unable to access the attachment, or if you have any other questions or concerns.

Sincerely,

Anthony Stark

General Counsel

805 Broadway St., Suite 900 | WA | 98660

O: [REDACTED]

www.zoominfo.com



A dark-themed banner for a ZoomInfo webinar. On the left, it says 'zoominfo | Live Webinar' and 'Powered by DiscoverOrg'. In the center, the year '2020' is written in large, white, outlined numbers. To the right of '2020' are stylized white fireworks and a champagne glass. Further right, a white banner with a gold border contains the text 'DECEMBER 19 | 2:00 PM ET'. At the bottom right, there is a white button with the text 'Save my seat'.

Powered by Sigstr

December 6, 2019

VIA EMAIL

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

Re: ZoomInfo's Comments on Draft CCPA Regulations

Dear Attorney General Becerra:

ZoomInfo¹ submits these comments regarding the draft regulations released by your office on October 10, 2019. Thank you for the opportunity to comment and to you and your staff for the work that you put in to preparing the draft regulations.

ZoomInfo provides a database of business contact information for business-to-business ("B2B") sales and marketing. Primarily, we seek to profile business organizations and to help our customers understand basic information about those organizations and who works there, and provide up-to-date information including primarily work emails and phone numbers. One could think of us as a "white pages" for business professionals.

This information is critical to the modern economy. According to TOPO, annually in the United States, approximately \$26 trillion is transacted in business-to-business commerce, and of that, approximately \$8 trillion originates from or is significantly impacted by access to B2B contact information. The commercial availability of databases like ZoomInfo not only creates massive efficiency, eliminating the need for businesses to each individually engage in manual research, but it levels the playing field for small and innovative businesses and increases competition on the merits of goods and services.

Meanwhile, the information ZoomInfo provides regarding consumers is not sensitive information that implicates serious privacy concerns. The vast majority of business professionals publish their names, employers, job titles and similar information on the internet, and many of them include likenesses, email addresses and phone numbers, physical addresses, work history, and educational history. ZoomInfo essentially provides the information that a person would typically include on a business card. And moreover, with or without the CCPA, ZoomInfo has a policy of honoring requests from any consumer to be removed from our database.

Our reading of the regulations comes primarily from the viewpoint of a business that collects and licenses "third-party" information, i.e. information not collected directly from the consumer. We use a number of means, including primary research and agreements with other businesses, to gather information and

¹ ZoomInfo (formerly known as DiscoverOrg) means DiscoverOrg Data, LLC and its affiliates.

curate our database. We are also concerned, as every business is, with the service provider rules as well as the general rules around processing and responding to consumer requests.

Pre-Collection Notice and Third-Party Data

We would first like to express our support for Section 999.305(d). This is a crucially important provision, and it addresses a widely recognized ambiguity in the CCPA in eliminating the pre-collection notice requirement for third-party data. In the third-party context, a pre-collection notice would be impossible, and the requirement that notice be provided prior to selling the information is the appropriate balance of interests. This approach is also consistent with the CPREA, specifically proposed Section 1798.100(b).

Pre-sale Notice

As to the pre-sale notice options, we propose adding a new subsection 999.305(d)(3) to permit a registered data broker to provide pre-sale notice via an online privacy policy or statement. The existing options in 999.305(d)(1) and (2) do not account for the possibility that the information does not contain a means of communicating with the consumer. For example, a business may gather information through research of newspaper articles. Information thereby collected could include the names of individuals mentioned in the articles but is not likely to include any contact or address information for such persons. And yet, the CCPA does not contemplate preventing the sale of this type of information. Rather, CCPA Section 135 contemplates notice of sale in general being provide via an online policy or statement.

Applying this to data brokers is both consistent with CCPA and consumer protective. Direct notifications may in some ways be helpful, but access to a registry of data brokers (combined with such data brokers' posted policies) gives consumers access to the relevant information upon demand. A consumer can refer to the registry at any time, whereas notices may be lost in a sea of information.

We propose that new section 999.305(d)(3) would read as follows:

If the business is a data broker registered pursuant to [___], provide the consumer with a notice of right to opt out in accordance with section 999.306 in an online privacy policy accessible via the business's internet homepage.

Maintenance of Personal Information for Suppression and other CCPA Purposes

We propose a provision expressly providing that businesses may maintain personal information as necessary to honor consumer rights or requests submitted pursuant to the CCPA or these regulations or otherwise to comply with the CCPA. Section 999.317(b) requires businesses to maintain records of all requests, but subsection (e) provides that the required records cannot be used for any other purpose. Business should be able to use those records for other purposes reasonably necessary for CCPA compliance and especially for purposes of implementing or honoring consumer rights and requests.

For example, ZoomInfo continually gathers information from available sources, such as company web pages or news articles. If a consumer submits a deletion request, we would delete the information from our normal production systems, but, both for our sake and the consumer's, we would like to keep a record of the request and the person's information solely for purposes of preventing that consumer's information from being re-added to the database.

We appreciate that the CCPA does not (and should not) *require* businesses to retain information solely for the purpose of consumer privacy requests. However, they should be expressly *permitted* to do so, since the extra effort will reduce consumer confusion and frustration. Without being able to implement suppression, consumers who were re-added to our database could feel that we had failed to honor their deletion or opt-out request, resulting in potential disputes even where the consumer's request was in fact honored.

We note that the right to maintain suppression lists is explicit in the CPREA ballot initiative, specifically proposed section 1798.105(c)(2), which reads as follows:

The business may maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws, or for other purposes solely to the extent permissible under this title.

We propose adding a similar provision to the regulations and making appropriate clarifying revisions to Section 999.317(e) as well as Sections 999.313(d)(2) and (3).

New Obligations Not Supported by CCPA

There are several instances where the proposed regulations would impose new obligations on businesses that we feel go beyond what is contemplated by the statute and that would create unfair additional burden on businesses.

First, businesses should not be required to treat unverifiable deletion requests as if they were opt-out requests. *See* Section 999.313(d)(1). There is no statutory basis for this obligation, and it requires businesses to act without consumer direction and upon information that is by definition unreliable. In addition, the statute and regulations already provide that business must clearly present the right to opt out, so this provision provides no corresponding benefit to consumers (*even if* we were correct in assuming that the person who submitted the unverifiable request nonetheless was the person they purported to be and that such person desired to opt out of the sale of their personal information).

Second, businesses should not be required to provide individualized feedback to consumers beyond what is required by the statute. In particular, the proposed obligation in Section 999.312(f) that businesses help consumers rectify deficiencies in their requests should be deleted. It is quite enough of a challenge for businesses to implement protocols for receiving and processing valid requests as required by the statute; the additional burden of helping consumers remedy deficiencies is unreasonable. For one thing, a business may simply not know that a particular communication it receives is intended to be a request pursuant to the CCPA, and it would be extremely onerous for a business to perform a fact-based analysis in each case to determine whether additional guidance is required by the regulation. This is in addition to the additional resources a business must devote to making these determinations, beyond the resources already required to process requests that are properly submitted. Finally, the statute and the regulations are robust in terms of the disclosures that are required; those disclosures are the appropriate place to specify what guidance businesses must provide consumers.

Third, businesses should not be required to provide additional contact information or support regarding consumer questions or concerns. See Section 999.308(b)(6). As with the above point, the CCPA requires very robust and detailed disclosures regarding a business's privacy practices, and those disclosures are already required to be presented in a manner that is understandable by average consumers. Those requirements should stand on their own, and it is unreasonably burdensome to expect businesses to devote additional resources to also answering questions and concerns about those already extensive disclosures. Moreover, this additional burden is not provided for in the CCPA.

Additional Disclosure Requirements

There are several instances where the proposed regulations would require businesses to include information in its notices, responses, or policies that would be unhelpful to consumers, unnecessarily burdensome to businesses, and not required by the statute. The following are examples of new disclosure requirements that should be eliminated or clarified:

- Section 999.308(b)(5). Businesses should not be required to explain to consumers how to designate an authorized agent. Unless guidance is provided in the regulations for how such designations may be made, it is unclear what is being required, or why this information should come from the businesses at all. If this provision remains, we ask that form language be provided for businesses to include.
- Section 999.313(a). A business should not be required to explain *how* said business will process the consumer's request or describe its verification process beyond providing instructions to the consumer for how to submit such a request. This proposed requirement goes beyond the statute, is unduly onerous to businesses, and will not provide benefit to consumers. It will not aid a consumer in any fashion to be presented with academic information about the specific manner in which the business performs its CCPA obligations, and this requirement appears to require disclosure for its own sake. For businesses, it is unduly burdensome to be required *not only* to process consumer requests and verify consumer identities *but also* to explain all of those processes and procedures in each and every response to a consumer request. This disclosure requirement also undercuts the goal of simple, clear communication that average consumers can understand.
- Section 999.313(d)(4). It is simply unclear what it would mean for a business to "specify the manner in which it has deleted the personal information."
- Section 999.313(d)(5). It is unclear why a business should be required to "disclose that it will maintain a record of the request pursuant to Civil Code section 1798.105(d)." This is not onerous, but simply adds information to the disclosures that is unlikely to be interesting or helpful to the consumer.
- Sections 999.305, 999.306, 999.307, and 999.308 require that notices and policies be "accessible to consumers with disabilities" and "provide information on how a consumer with a disability may access the notice in an alternative format." It is not clear what it means to make this information accessible to consumers with disabilities or what alternative formats would be accessible. It is also unclear how the additional information will be helpful if the disability in question prevents the

person from accessing the notice or policy. We request further clarity on what is required by this provision. It may be that services already exist to allow persons with specific disabilities to access such notices or policies in a manner that would be more effective than what individual businesses could provide.

Standards for Disclosure and Verification

In certain instances, the standards to be applied by businesses in verifying and responding to consumer requests are unclear. We request that the following issues be clarified:

Section 999.313(c)(3) provides that, under certain circumstances, a business may *not* provide certain information in response to a request that it would otherwise be required to provide under the CCPA. Specifically, “[a] business shall not provide a consumer with specific pieces of personal information *if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer’s account with the business, or the security of the business’s systems or networks.*” (Emphasis supplied.) This provision conflates two separate concepts, putting businesses in an impossible position. First, a business should be *permitted* (not required) to refuse to disclose certain information if the *business* can articulate substantial risks. Second, it may be appropriate to *require* a business to refuse such disclosure under certain circumstances as well, but that cannot be the exact same standard. This puts a business in the impossible position of applying a vague and subjective standard (substantial, articulable, *and* unreasonable) to determine the exact line between when it *must* make the disclosure and when it *cannot* make the disclosure.

The standard provided for when a business must honor an opt-out request is also confusing. Section 999.315(h) provides “[a] request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request.” Even though CCPA does not specify that the request be a “verifiable” request, it does contemplate that the request be “from the consumer.” The requirement that the business affirmatively form a “good-faith, reasonable, and documented” belief that the request is “fraudulent” is a different standard. It should be enough that the business cannot in good faith determine that the request is “from the consumer.” At a minimum, the regulations should clarify whether “fraudulent” is intended to mean something other than the submission of a request by a person who is not the consumer to whom the personal information relates and is not such person’s authorized agent.

Service Provider Provisions

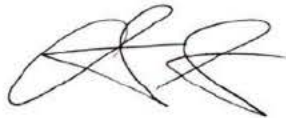
Section 999.314(c) requires clarification. As drafted, it prevents a service provider from using personal information it obtains for providing services to any other party. This makes sense in concept, but it requires nuance to account for the different roles a business may play and for different contractual arrangements it may have. A business may meet the definition of a service provider, but still have other legal rights and obligations separate from its role as a service provider. For example, a business might both provide services to another business and also purchase personal information from such other business with the intention of using such information in a manner otherwise permissible under the CCPA. If the purpose is to make express that a service provider’s violation of contractual limitations limiting the service provider’s use of personal information shall also constitute a violation of the statute (a reasonable aim), that should be clarified.

We propose that the regulations be revised to reverse the approach taken by proposed Section 999.314(d). That section provides that a service provider must provide responses to consumers even where it has the consumer's data solely as a service provider. This is problematic. For one thing, a service provider may not have access to the personal information it possesses on behalf of a business to whom it provides services. We think that imposing any obligations on service providers with respect to data processed solely on behalf of a business is the wrong approach. Rather, service providers should be required solely to comply with instructions from the business they serve with respect to the personal information processed pursuant to that relationship. We think that personal information processed by a service provider solely in its capacity as service provider should be deemed to be in the possession of the business and not the service provider, and the service provider's only obligation with regard to consumer request should be to comply with the business's instructions with regard to consumer requests received by the business.

Once again, we appreciate the opportunity to submit these comments. I would be happy to answer any questions you may have. I can be reached by email at [REDACTED] or by phone at [REDACTED]

Sincere Regards,

ZOOMINFO



Anthony Stark
General Counsel

805 Broadway St., Suite 900
Vancouver, WA 98660
[REDACTED]

Message

From: Peter Leroe-Muñoz [REDACTED]
Sent: 12/6/2019 5:10:39 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Written Comments on Proposed CCPA Regulations | Silicon Valley Leadership Group
Attachments: Attorney General CCPA Regulations - Public Comment - Final.pdf

Please find attached written comments from the SV Leadership Group regarding the Attorney General's proposed regulations for the CCPA.

We look forward to working with the Attorney General to clarify the CCPA and ensure that its operation and enforcement protects consumers and enables economic growth.

Peter Leroe-Muñoz
General Counsel & Vice President, Tech & Innovation
Silicon Valley Leadership Group
[REDACTED]



2001 Gateway Place, Suite 101E
San Jose, California 95110
(408)501-7864 svlg.org

CARL GUARDINO
President & CEO

Board Officers:

STEVE MILLIGAN, Chair
Western Digital Corporation
JAMES GUTIERREZ, Vice Chair
Insikt
RAQUEL GONZALEZ, Treasurer
Bank of America
GREG BECKER, Former Chair
SVB Financial Group
STEVE BERGLUND, Former Chair
Tomble Inc.
AART DE GEUS, Former Chair
Synopsis
TOM WERNER, Former Chair
SunPower

Board Members:

BOBBY BELL
KLA-Tencor
DAWNET BEVERLEY
Donnelley Financial Solutions
GEORGE BLUMENTHAL
University of California, Santa Cruz
JOHN BOI AND
KQED
CARLA BORGNO
Genentech
CHRIS BOYD
Kaiser Permanente
JOE BURTON
Plantronics
RAM BRANTZKY
Sapphire Ventures
KEVIN COLLINS
Accenture
LISA DANIELS
KPMG
JENNY DEARBORN
SAP
MICHAEL ENGH, S.J.
Santa Clara University
TOM FALLON
Infirera
JOHN GAUDER
Cymcard
KEN GOLDMAN
Hillspire
DOUG GRAHAM
Lockheed Martin
LAURA GUIO
IBM
STEFAN HECK
Nauto
ERIC HOUSER
Wells Fargo Bank
AIDAN HUGHES
ARUP
VICKI HUFF ECKERT
PwC
TOM KEMP
Centify
ERIC KUTCHER
McKinsey & Company
JOHN LEDEY
BO Biosciences
ENRIQUE LORES
HP Inc.
MATT MAHAN
Brigade
TARKAN MANER
Nexenta
KEN MCNEELY
AT&T
BEH MINICUCCI
Alaska Airlines
MARY PAPAIZIAN
San Jose State University
JES PEDERSEN
Webcor Builders
ANDY PERCE
Stryker Endoscopy
KIM POLESE
ClearStreet
RYAN POPPLE
Proterra
RUDY REYES
Verizon
BILL RUH
GE
SHARON RYAN
Bay Area News Group
RON SEGE
Echelon
DARREN SNELGROVE
Johnson & Johnson
JEFF THOMAS
Nasdaq
JED YORK
San Francisco 49ers

Established in 1978 by
David Packard

December 4, 2019

Honorable Xavier Becerra
California Attorney General

California Office of the Attorney General
Privacy Regulations Coordinator
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: California Consumer Privacy Act – Proposed Regulations

Honorable Xavier Becerra:

I am writing on behalf of the Silicon Valley Leadership Group to provide feedback on the California Consumer Privacy Act (CCPA) Regulations that were proposed on October 10, 2019.

The Leadership Group was founded in 1978 by David Packard of Hewlett-Packard and represents more than 350 of Silicon Valley's most respected employers. Leadership Group member companies collectively provide nearly one of every three private sector jobs in Silicon Valley and we have a long history of supporting policies that promote innovation, stronger economic growth and improved transportation in California.

Our feedback is provided in the attached Appendix A.

We are eager to work with your office to help clarify portions of the CCPA, bring greater certainty to consumers and business about their respective rights and responsibilities, and establish a framework that promotes both privacy and economic growth.

Sincerely,

Peter Leroe-Muñoz
General Counsel and VP of Tech & Innovation Policy
Silicon Valley Leadership Group

APPENDIX A

Public Comment on California Consumer Privacy Act Proposed Regulations

§ 999.305(a)(3) Notice at Collection of Personal Information

Where a business has proactively and directly notified consumers, including through its standard terms and use, that the business intends to use personal information in a new way, explicit consumer consent should not be required for such use.

§ 999.306(d)(3) Notice of Right to Opt-Out of Sale of Personal Information

A business should be exempt from providing a notice of a right to opt-out when the business publishes a change in its Privacy Policy for a determined period of time to give consumers the right to opt-out.

§ 999.307(b)(6) Notice of Financial Incentive

This section should eliminate language referencing any estimated value of a consumer's data, as well as any description of the methodology for calculating such value. Determining the value of any particular consumer's personal information is highly-specific and time-intensive. Moreover, any estimation would require significant speculation at the time of collection, rendering the calculation unreliable.

§ 999.308(b)(1)(c) Privacy Policy

This section would require businesses to describe the process used to verify consumer requests, including information the consumer provides. Businesses use a variety of verification methods for different types of information, including non-public methods. This would require frequent updates to the Privacy Policy as methods change, and disclosure of non-public or sensitive verification methods. A better practice would be to have the business verification processes explained to users in general and without specifics, in the request interface, or via a link to an FAQ page.

§ 999.312(g) Methods for Submitting Requests to Know and Requests to Delete

If a consumer submits a request in a non-conforming method or manner, businesses should not attempt to treat the request as if it were properly submitted, nor should they be required to remedy any such request.

§ 999.313(b) Responding to Requests to Know and Requests to Delete

The proposed requirement that business must respond to a request within 45 days of receipt should be amended to respond within 45 days of when the request was verified. This allows businesses to properly verify requests, which may take an extended period of time through no fault of the businesses, since the process of verification may include a number of third-party sources and participants.

§ 999.315(c) Requests to Opt-Out

User-enabled privacy controls should not be presumed to speak for consumers regarding their choice to opt out of the sale of their information. Opting out should require an affirmative act and conscious choice by consumers.

§ 999.317 Training; Record-Keeping

The requirement of maintaining records of consumer requests for a minimum of 24 months is overly lengthy. Moreover, the reporting requirements under subsection (g) will not distinguish between valid and invalid requests. As such, the numbers will provide little value. This subsection should be removed.

§ 999.323(f) General Rules Regarding Verification

Businesses should be able to use their industry's standard authentication methodology to verify consumer requests.

§ 999.337 Calculating the Value of Consumer Data

Determining the value of any particular consumer's personal information is highly-specific and time-intensive. Moreover, any estimation would require significant speculation at the time of collection, rendering the calculation unreliable. This element should be removed from consideration.

Message

From: Storey, Joanna L. [REDACTED]
Sent: 12/6/2019 6:03:29 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Written Comments re the proposed regulations for the California Consumer Privacy Act
Attachments: Hinshaw and Culbertson Letter to the Attorney General 2019-12-06.pdf

Please see the attached written comments regarding the proposed regulations for the California Consumer Privacy Act for consideration by the Attorney General's office. Thank you,

Joanna L. Storey, Esq.
Hinshaw & Culbertson LLP
One California Street, 18th Floor
San Francisco, CA 94111
Tel: [REDACTED] | Fax: (415) 834-9070
<https://www.linkedin.com/in/joannastorey/>

[REDACTED] | www.hinshawlaw.com



Hinshaw & Culbertson LLP is an Illinois registered limited liability partnership that has elected to be governed by the Illinois Uniform Partnership Act (1997).

The contents of this e-mail message and any attachments are intended solely for the addressee(s) named in this message. This communication is intended to be and to remain confidential and may be subject to applicable attorney/client and/or work product privileges. If you are not the intended recipient of this message, or if this message has been addressed to you in error, please immediately alert the sender by reply e-mail and then delete this message and its attachments. Do not deliver, distribute or copy this message and/or any attachments and if you are not the intended recipient, do not disclose the contents or take any action in reliance upon the information contained in this communication or any attachments.



ATTORNEYS AT LAW

One California Street, 18th Floor
San Francisco, CA. 94111

415-362-6000

415-834-9070 (fax)

www.hinshawlaw.com

Joanna L. Storey

December 6, 2019

VIA EMAIL

PrivacyRegulations@doj.ca.gov

The Honorable Xavier Becerra
c/o Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: Comments on Proposed CCPA Regulations

Dear Mr. Becerra:

I write on behalf of myself and Hinshaw & Culbertson LLP to offer comments on the proposed regulations for the California Consumer Privacy Act. This letter follows the oral comments I made at the December 4, 2019 Public Hearing in San Francisco.

Proposed Regulation §999.314(c) May Unintentionally Frustrate the Tripartite Relationship between an Insurer, its Insured, and the Law Firm Retained to Represent the Insured and Interfere with §1798.145(a)(4) of the CCPA

As currently drafted, the proposed regulation §999.314(c) relating to “Service Providers” may frustrate the tripartite relationship between an insurer, its insured and the law firm retained by an insurer to represent its insured. Law firms that do not qualify as a covered “Business” under §1798.140(c) of the CCPA may still be subject to the Act and the proposed regulations if the law firm meets the definition of a “Service Provider” and processes information on behalf of a business.

A Service Provider is defined in §1798.140(v) as:

[A] sole proprietorship, partnership, limited liability company, corporation, association or other legal entity that is

organized 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 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 . . .

Because law firms are typically organized to make a profit, they may qualify as a service provider to the extent that the law firm provides legal services to businesses that are subject to the CCPA. Insurance carriers doing business in California that have more than \$25 million in annual gross revenues meet the CCPA's definition of a business. When an insurance carrier that meets the definition of a business retains a law firm, if the written agreement between the law firm and insurance carrier, or the carrier's outside counsel guidelines prohibit the law firm from retaining, using, or disclosing the personal information for any purpose other than the services the law firm was retained to provide, then the law firm meets the definition of a Service Provider, and §999.314(c) is implicated. Today, insurance carriers trying to meet their own data security and privacy obligations routinely limit in writing how law firms may use the information provided by the carrier to the law firm.

Under proposed regulation §999.314(c), a service provider "shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose of providing services to another person or entity." This regulation frustrates the nature and purpose of the tripartite relationship between the law firm, its client – the insured, and the client's insurance carrier. For example, if the law firm (a service provider) is retained by an insurance carrier (a business) to defend its insured, any personal information that the carrier obtained during the claims review process or prior to suit being filed could not be used by the law firm in providing services to its client, the insured. This sharing quagmire extends further and would seemingly prohibit the law firm from sharing information provided by the carrier with experts and consultants necessary to defend the insured.

The Exercise or Defend Claims and Privilege Exceptions in §1798.145(a)(4) and §1798.145(b) Do Not Appear to Apply to Service Providers

While §1798.145(a)(4) and §1798.145(b) of the CCPA provide exceptions to the CCPA's obligations when exercising or defending legal claims and when compliance would violate an evidentiary privilege under California law, those exceptions by their express terms *only* apply to a "Business." There is nothing in the CCPA or your proposed

implementing regulations that extends subsection (a)(4), (b), or any of §1798.145's other subsections to law firms when acting as a service provider on behalf of a business.

While the obvious intent of §1798.145(a)(4) and (b) is to prevent the obligations imposed by the CCPA from impeding litigation and protecting attorney-client and other evidentiary privileges, unless these provisions are interpreted to extend to a law firm service provider retained by a business to defend legal claims such as in the typical tripartite relationship, the intent of this exception will be frustrated. Moreover, proposed regulation §999.314(c) further frustrates the intent of §1798.145(a) and (b). The proposed regulation would impair the ability of a business to defend legal claims through law firm service providers. We ask that the Attorney General consider addressing these issues in a regulation.

The Regulations Should Define "Processing" by Further Explaining the Meaning of "Operation"

We also ask that proposed regulations offer additional clarity to terms defined in the CCPA. For instance, Civil Code §1798.140(q) defines the term "Processing" as "any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means." The terms "operation" and "set of operations" are not defined within the CCPA or the proposed regulations.

It appears the CCPA's definition of "Processing" is drawn from Article 4(2) of the General Data Privacy Regulation ("GDPR"), but it does not include examples of the types of operations encompassed by the CCPA's processing definition as in Article 4(2) of the GDPR. Do those terms, for instance, include merely the storage of information or the use of information in litigation?

Because of the promise of enhanced security offered by cloud providers, many law firms are using a cloud provider to store their data. Does storing personal information in the cloud by a law firm constitute processing that data? Law firms also often use software to collect, manage and search electronically stored information for discovery purposes. It is unclear under the current scheme whether such efforts would constitute "Processing." We request you provide clarification on these points.

The Regulations Should Provide Guidance on §1798.145(a) of the CCPA

Finally, we also write to express our concern about the absence of any regulation clarifying the meaning and intent of Civil Code §1798.145(a), which provides that the obligations imposed on a business by the CCPA shall not "restrict" a business's ability to, among other things, comply with federal, state or local laws, comply with subpoenas or regulatory inquiries or investigations or to exercise or defend legal claims. Does the use of the phrase "shall not restrict" mean that a business does not have to comply with

§1798.105 when it is reasonably anticipated that information a consumer requests be deleted, may be necessary to exercise or defend legal claims, or to comply with state or federal law? Or does this mean that a business must still comply with some parts of the CCPA that are not affected by its efforts to exercise or defend legal claims? This is especially concerning because subsection (b) expressly uses the phrase “shall not apply” when addressing privileged information:

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.

Cal. Civil Code §1798.145(b) (emphasis added). The scope of the “exercise or defend legal claims” exception is simply unknown. It is also unclear how transactional legal services may fall into the scope of the CCPA.

We appreciate your efforts to bring clarity and logic to the CCPA through well-reasoned regulations. We recognize the considerable time pressures under which you and your staff have been working. We ask that you consider our comments as you revise the proposed regulations. Thank you for your time and consideration.

Very truly yours,

HINSHAW & CULBERTSON LLP


Joanna L. Storey

Message

From: Scott Jordan [REDACTED]
Sent: 12/6/2019 5:40:23 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Written comments regarding proposed CCPA regulations
Attachments: Jordan CCPA regulations comments.pdf

Attached please written comments regarding the proposed CCPA regulations (Sections 999.300 through 999.341 of Title II, Division 1, Chapter 20 of the CCR).

-Scott Jordan

Scott Jordan
3214 Bren Hall, Department of Computer Science, University of California, Irvine, CA 92697-3435
[REDACTED] <http://www.ics.uci.edu/~sjordan>

**BEFORE THE
CALIFORNIA ATTORNEY GENERAL**

In the Matter of

Sections §§ 999.300 through 999.341
of Title 11, Division 1, Chapter 20,
of the California Code of Regulations (CCR)
concerning the California Consumer Privacy Act (CCPA)

COMMENTS OF SCOTT JORDAN

Scott Jordan
Department of Computer Science
University of California, Irvine
Irvine, CA 92697-3435
[REDACTED]

December 6, 2019

About the Author: Scott Jordan is a Professor of Computer Science at the University of California, Irvine. Scott received the Ph.D. degree in Electrical Engineering & Computer Science from the University of California, Berkeley. In 2006, he served as an IEEE Congressional Fellow, working in the United States Senate on communications policy issues. During 2014-2016, Scott served as the Chief Technologist at the Federal Communications Commission, advising on technological issues across the Commission. In writing these reply comments, Professor Jordan represents no one but himself, and is not speaking on behalf of his employer or any other party.

Table of Contents

1. §999.301. Definitions.....	3
A. Categories of third parties	3
B. Categories of sources	4
2. §999.305. Notice at Collection of Personal Information	4
A. List of required disclosures	4
B. Detail and clarity	5
3. §999.308. Privacy Policy	5
A. Collection of personal information	5
B. Disclosure or sale of personal information	6
4. 999.313. Responding to Requests to Know and Requests to Delete.....	6
5. 999.314. Service Providers	7

1. §999.301. DEFINITIONS

A. *Categories of third parties*

The term “categories of third parties” is one element of disclosures related to a consumer’s right to request.¹ Draft §999.301(e) defines “categories of third parties” as “types of entities that do not collect personal information directly from consumers, including but not limited to advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers”.²

While advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers are all good examples of categories of third parties, **the definition errs when it implies that such third parties are “entities that do not collect personal information directly from consumers”**. CCPA places no such restriction on categories of third parties.

CCPA defines “third party” as a person who is neither “the business that collects personal information from consumers” nor a service provider.³ CCPA clearly does not intend that the term “third party” excludes a person who both collects personal information directly from consumers and who collects additional personal information by obtaining or receiving it from another business. Indeed, Internet service providers commonly both collect personal information directly from consumers and collect additional personal information by obtaining or receiving it from other businesses.

Instead, CCPA explicitly gives consumers a “right to opt-out” of a business selling that consumer’s personal information to third parties⁴. Furthermore, CCPA defines “sell” as “selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by

¹ CCPA, Sections 1798.110(a)(4), 1798.110(c)(4), 1798.115(a)(2), and 1798.130(a)(4).

² NOPA, § 999.301(d).

³ CCPA, Section 1798.140(w).

⁴ CCPA, Section 1798.120.

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."⁵

A consumer's right to opt-out cannot be interpreted as limited to third parties that do not themselves collect information directly from a consumer. Instead, the right to opt-out clearly includes selling a consumer's information to third parties that do themselves collect information directly from a consumer, but the right to opt-out is limited to the consumer's personal information included in the sale and thus does not include additional personal information that the third party may itself collect directly from a consumer.

The definition should be revised to make it clear that categories of third parties includes entities that may collect personal information directly from consumers, in addition to obtaining or receiving personal information from another business.

B. Categories of sources

The term "categories of sources" is one element of disclosures related to a consumer's right to request.⁶ Draft §999.301(d) defines "categories of sources" as "types of entities from which a business collects personal information about consumers, including but not limited to the consumer directly, government entities from which public records are obtained, and consumer data resellers".⁷

While the categories of sources should include the business itself (directly from consumers), government entities, and consumer data resellers, this list (although clearly stated as not an exhaustive list) mistakenly seems to imply very broad categories. The purpose of CCPA including "categories of sources" as one element of disclosures related to a consumer's right to request is to inform consumers about where the consumer's personal information came from.

The terms "categories of sources" and "categories of third parties" are related. Consumer personal information may be sold by a business to a third party. The business shall disclose the categories of third parties and the third party (if a business) shall disclose the categories of sources. **Correspondingly, the definition of "categories of sources" should mirror that provided in the definition of "categories of third parties", and should include not only the business itself (directly from consumers), government entities, and consumer data resellers, but also advertising networks, internet service providers, data analytics providers, operating systems and platforms, and social networks.**

2. §999.305. NOTICE AT COLLECTION OF PERSONAL INFORMATION

A. List of required disclosures

Draft §999.305(b) states information that a business shall include in its notice at collection. The proposed text includes (i) "[a] list of the categories of personal information about consumers to be collected" and (ii) "[f]or each category of personal information, the business or commercial purpose(s) for which it will be used."⁸ These requirements are consistent with Section 1798.100(b). They facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130(a)(5)(B), and therefore fall within CCPA's delegation of authority to the Attorney General.⁹ In particular, the requirement to disclose the business or commercial purposes(s) *for each category of personal information*

⁵ CCPA, Section 1798.140(t)(1).

⁶ CCPA, Section 1798.110(a), 1798.110(c).

⁷ NOPA, § 999.301(d).

⁸ NOPA, § 999.305(b).

⁹ CCPA, Section 1798.185(a)(7).

further the purpose of “inform[ing] consumers at or before the time of collection of a consumer’s personal information”¹⁰, further “[t]he right of Californians to know what personal information is being collected about them”¹¹, and provides Californians with the information that empowers their “right ... to say no to the sale of personal information”¹². Only by knowing the purpose for each category of personal information may consumers meaningfully exercise their right to say no to the sale of personal information.

B. Detail and clarity

Draft §999.305(a)(2) states that “[t]he notice at collection shall be designed and presented to the consumer in a way that is easy to read and understandable to an average consumer”.¹³ It is certainly important that the notice at collection shall be easy to read and understandable. **However, the regulations should also address both the detail and clarity of notices.**

Regarding detail, notices should be required to be *sufficiently detailed to enable users to make informed contextual decisions about their privacy and their use of the service*. Only with *sufficient detail* can a notice be “easily understood by the average consumer”.¹⁴ In addition, the notice at collection provides consumers with the *information* necessary to exercise their “right ... to say no to the sale of personal information”¹⁵. Consumers view this decision as one that is made in the *context* of both the categories of personal information collected and the purposes for which each category is collected. Consumers require a *sufficient* level of detail to meaningfully exercise this right.

Regarding clarity, notices should be required to be *not misleading*. Only if a notice is *not misleading* can a notice be “easily understood by the average consumer”.¹⁶

3. §999.308. PRIVACY POLICY

Draft §999.308(b)(1) states information that a business shall include in privacy policy to support a consumer’s right to know about personal information collected, disclosed, or sold.

A. Collection of personal information

With respect to the collection of personal information, the proposed text includes (i) a “[l]ist [of] the categories of consumers’ personal information the business has collected about consumers ...” and (ii) “[f]or each category of personal information collected, ... the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties with whom the business shares personal information.”¹⁷ These requirements are consistent with Sections 1798.100(a), 1798.110(a), 1798.110(c), 1798.115(a), and 1798.115(c). They facilitate a consumer’s or the consumer’s authorized agent’s ability to obtain information pursuant to Section 1798.130(a)(5)(B), and therefore fall within CCPA’s delegation of authority to the Attorney General.¹⁸ In particular, the requirement to disclose the categories of sources, the purposes, and the categories of third parties with whom the personal information is shared, *for each*

¹⁰ NOPA, § 999.305(a)(1).

¹¹ AB 375, Section 2(i)(1).

¹² AB 375, Section 2(i)(3).

¹³ NOPA, § 999.305(a)(2).

¹⁴ CCPA, Section 1798.185(a)(6).

¹⁵ AB 375, Section 2(i)(3).

¹⁶ CCPA, Section 1798.185(a)(6).

¹⁷ NOPA, § 999.308(b)(1)(d).

¹⁸ CCPA, Section 1798.185(a)(7).

category of personal information collected, furthers the purpose of “provid[ing] the consumer with a comprehensive description of a business’s online and offline practices regarding the collection, use, disclosure, and sale of personal information”¹⁹, furthers “[t]he right of Californians to know what personal information is being collected about them”²⁰, furthers “[t]he right of Californians to know whether their personal information is sold or disclosed and to whom”²¹, and provides Californians with the information that empowers their “right ... to say no to the sale of personal information”²². Only by knowing the categories of sources, the purposes, and the categories of third parties with whom the personal information is shared, for each category of personal information, may consumers meaningfully exercise their right to say no to the sale of personal information.

B. Disclosure or sale of personal information

With respect to the disclosure or sale of personal information, the proposed text includes a “[l]ist [of] the categories of personal information, if any, that it disclosed or sold to third parties for a business or commercial purpose ...”²³. **However, the proposed text omits a similar requirement to disclose the purposes for which each category of personal information was shared with each category of third parties. Draft §999.308(b)(1)(e) should be modified to include this requirement.** This would ensure that the requirements for notice at collection (§999.305(b)), privacy policies regarding collection of personal information (§999.308(b)(1)(d)), and privacy policies regarding disclosure or sale of personal information (§999.308(b)(1)(e)) are consistent. This proposed requirement is consistent with Sections 1798.110(a), 1798.110(c), and 1798.115(a). It facilitates a consumer’s or the consumer’s authorized agent’s ability to obtain information pursuant to Section 1798.130(a)(5)(B), and therefore falls within CCPA’s delegation of authority to the Attorney General.²⁴ It furthers the purpose of “provid[ing] the consumer with a comprehensive description of a business’s online and offline practices regarding the collection, use, disclosure, and sale of personal information”²⁵, furthers “[t]he right of Californians to know whether their personal information is sold or disclosed and to whom”²⁶, and provides Californians with the information that empowers their “right ... to say no to the sale of personal information”²⁷. Only by knowing the purpose for which personal information is shared for each category of personal information may consumers meaningfully exercise their right to say no to the sale of personal information.

4. 999.313. RESPONDING TO REQUESTS TO KNOW AND REQUESTS TO DELETE

Draft §999.313(c)(10) states information that a business shall provide in response to a verified request to know the categories of personal information collected. The proposed text includes for each identified category of personal information it has collected about the consumer, the categories of sources from which the personal information was collected, the business or commercial purpose for which it collected the personal information, the categories of third parties to whom the business sold or disclosed the category of personal information for a business purpose, and the business or commercial purpose for which it sold or

¹⁹ *NOPA*, § 999.308(a)(1).

²⁰ AB 375, Section 2(i)(1).

²¹ AB 375, Section 2(i)(1).

²² AB 375, Section 2(i)(3).

²³ *NOPA*, § 999.308(b)(1)(e).

²⁴ *CCPA*, Section 1798.185(a)(7).

²⁵ *NOPA*, § 999.308(a)(1).

²⁶ AB 375, Section 2(i)(1).

²⁷ AB 375, Section 2(i)(3).

disclosed the category of personal information.²⁸ These requirements are consistent with Sections 1798.100(a), 1798.110(a), 1798.110(c), 1798.115(a), and 1798.115(c). They facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130(a)(5)(B), and therefore fall within CCPA's delegation of authority to the Attorney General.²⁹ In particular, the requirement to disclose the categories of sources, the categories of third parties with whom the personal information is shared, and the purposes for collection, disclosure, and sale, *for each category of personal information collected*, furthers the purpose of "provid[ing] the consumer with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information"³⁰, furthers "[t]he right of Californians to know what personal information is being collected about them"³¹, furthers "[t]he right of Californians to know whether their personal information is sold or disclosed and to whom"³², and provides Californians with the information that empowers their "right ... to say no to the sale of personal information"³³. Only by knowing the categories of sources, the purposes, and the categories of third parties with whom the personal information is shared, for each category of personal information, may consumers meaningfully exercise their right to say no to the sale of personal information.

5. 999.314. SERVICE PROVIDERS

Draft §999.314 states that in order to qualify as a service provider under CCPA, the service provider "shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose of providing services to another person or entity."³⁴ This is consistent with CCPA, in which a service provider is defined as an entity "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."³⁵ The text in §999.314 properly clarifies that if a service provider collects personal information directly from a consumer on behalf of a business, then it is similarly *prohibited from using that personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business*. **However, this could be made more explicit in the regulations by mirroring the text in CCPA ("for any purpose other than for the specific purpose of performing the services specified in the contract for the business") instead of introducing new language ("for the purpose of providing services to another person or entity").**

Draft §999.314 also states that a service provider receives a consumer request to know or request to delete, the service provider must either "comply with the request" or "inform the consumer that it should submit the request directly to the business on whose behalf the service provider processes the information".³⁶ This

²⁸ NOPA, § 999.313(c)(10).

²⁹ CCPA, Section 1798.185(a)(7).

³⁰ NOPA, § 999.308(a)(1).

³¹ AB 375, Section 2(i)(1).

³² AB 375, Section 2(i)(1).

³³ AB 375, Section 2(i)(3).

³⁴ NOPA, § 999.314(c).

³⁵ CCPA, Section 1798.140(v).

³⁶ NOPA, § 999.314(d).

is consistent with CCPA, and it enables a consumer to exercise the right to know and right to delete by contacting the business.

Message

From: Ryan Bittle [REDACTED]
Sent: 12/6/2019 10:27:25 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Written public comment for CCPA

To Whom It May Concern:

I am a California consumer who only heard about CCPA for the first time a few weeks ago. With the magnitude of the impact to both consumers and businesses I am shocked so few are speaking about this Act.

I commend the Attorney General's proposed regulations and legislative effort to further consumer's rights and privacy in today's world of technology. While many of these mandates will place a heavy burden on businesses which partake in collecting and/or selling consumer data, these businesses have a responsibility in allowing consumers to exercise their right to privacy. As time goes on I suspect the cost of compliance will drop as workflows and systems are put in place to streamline the process.

Regarding the proposed regulations, I do have a few concerns:

1) Both the right to delete as well as the right to know require a business to act only on a "verifiable consumer request". This potentially places a burden on the consumer if a business makes it exceptionally difficult or complex to meet by requesting overbearing proof, such as by providing scans of personal documents. Doing so also potentially puts the consumer at further risk by providing sensitive information the business did not intend to collect in the first place. Currently, only the right to opt out does not require this verifiable request, and I propose that businesses be prohibited from requiring extensive proof of identity for opt-out requests.

2) Many businesses today communicate with their customers primarily via email for updates as well as advertising. Under current proposed regulation businesses will likely add a web form on their website in order to request removal of information - either to aid in collecting proof of identity or to intentionally make the process more cumbersome for the consumer, or both. Furthermore there are currently projects being built, free to the consumer, which would allow consumers to send pre-written emails to the businesses in order to easily exercise their right under CCPA. Requiring consumers visit each website individually would be burdensome to the consumer as they would potentially be submitting requests to many different businesses, each with its own variation of the form. I propose that businesses shall accept requests to delete, know, or opt-out via email and not require the consumer to go through other means in order to process the request.

3) Consumers may wish to utilize a third-party service as an authorized agent to help exercise their rights under CCPA. An authorized agent, when registered with the Secretary of State, may include a written declaration stating they have verified the consumer's identity through specified means (such as viewing a government issued document produced by the consumer). In my interpretation of CCPA, a business may require the consumer to directly verify with the business making the use of an authorized agent a null and void procedure. I propose upon receipt of the declaration the business be required to either accept the consumer as verified, or count the declaration as a data point towards verifying the request.

Thank you for allowing consumers a public comment period to voice their concerns. I hope awareness of CCPA increases allowing consumers to exercise their rights to privacy.

Regards,

Ryan

Message

From: Gregory Guarnay [REDACTED]
Sent: 12/8/2019 7:08:03 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Denis Bandera-Duplantier [REDACTED]; Damon Magnuski [REDACTED]
Subject: [Non-Profit Request] Protecting Californians' Data Privacy
Attachments: DAMD Foundation Inc Broker Letter Version 7.docx

Dear Privacy Regulations Coordinator,

My name is Gregory, I am a California resident living in Mountain View, and I work with the [Delete All My Data](#) Foundation, a non-profit dedicated to deleting individuals' personal data wherever possible.

We look forward to the CCPA entering into effect on January 1st, as we believe this will give Californians greater control over their personal data.

With your permission, we would like to CC the Office of the California Attorney General, when, as part of our mission, we send out cease and desist letters to data brokers that do not have our members' consent to store, process, or share their data, and/or do not provide value to them.

Attached is an example of such letter that we currently forward to the Office of the Massachusetts Attorney General. We would love to also have the support of the Office of the California Attorney General.

Happy to jump on a call if you have any questions, or if you would like to edit the language, for instance making it more CCPA oriented, on the Delete All My Data Broker letter template (attached).

Thanks for your consideration.

Gregory Guarnay

[REDACTED]
<https://www.linkedin.com/in/gregoryguarnay>
[REDACTED]

11-20-19
Delete All My Data Foundation Inc
320 Broadway
PO BOX 45622
Somerville, MA 02145

TowerData
Attn: Privacy Officer
33 Irving Place, 3rd Floor STE 4048
New York, New York 10003

Re: CEASE AND DESIST USE OF PERSONAL DATA

Dear Data Broker:

We reached out to you in the last year and have since changed to non-profit foundation. We now include signed affidavits and forward correspondence to the Massachusetts Attorney General's office. Also, please note the change of address at the top of the letter.

At the request of the individuals listed under Addendum A attached hereto ("Member") you are hereby directed to take the following immediate actions in compliance with applicable state, federal and international consumer protection, and data privacy laws. This letter is privileged and confidential. Delete All My Data Foundation Inc has full power and authority to make such request and this letter shall be considered a direct request from the Member to you. This authority and relationship is evidenced by a power of attorney granted by the Member to Delete All My Data Foundation Inc, and supported by an affidavit and sworn declaration executed by the Member.

Your firm has been identified as a "Data Broker". Our definition is a company that collects information "Data" about a person and sells / licenses that information without the explicit consent of that person. If you are not a Data Broker by this definition, please respond with a general description of your services and we will review if we should continue pursuing the actions outlined below.

If your firm is a "Data Broker" or otherwise subject to the rules and regulations outlined below, please comply with the request of this letter.

You and your affiliates are hereby directed to:

CEASE AND DESIST ALL USE, SALE, RETENTION AND DISTRIBUTION OF
ALL MEMBER'S PERSONAL INFORMATION AND DATA ("DATA").

We further demand that you and your affiliates take the following immediate actions:

- a) Delete all Data;
- b) Provide a list of where the Data came from;
- c) Terminate all further attempts to collect, retain, purchase, sale or distribute Data in any way;
- d) Do not assign or transfer Data to any other party;
- e) Provide a list of affiliates that are covered by this letter;
- f) Confirm to us in writing that all actions requested in this letter have been completed;
- g) Send a copy of the Data to the Member's address listed in Addendum A

Data shall include all Member non-public personal information, including but not be limited to, the following:

Social Security Numbers
Credit Card Account Numbers
All other financial information
All location Data

If you fail to properly take the above listed actions within thirty (30) days of receipt of this letter, our Member

Delete All My Data Foundation Inc Broker Letter Version 7

may suffer significant damages as a result, particularly if the Data currently being held and distributed by you is false or misleading. Upon the expiration of applicable statutorily required notice periods, Members may move forward with exploring their options of relief available under any applicable laws, including engaging an attorney, to seek damages, as applicable, for injuries, triple damages as appropriate, and attorneys' fees in addition to the demands in this letter, including but not limited to notification of Attorneys General with appropriate jurisdiction.

Some entities may not be able to delete the Data. If that is the case, please identify the reasons why in response to this letter. Depending on the type of Data, please take the following steps:

Opt Out

For all products / services that are subject to opting out, please process the request as well as provide a list of products / services that the Member was opted out of. We understand that your firm may have a consumer facing opt-out facility, but as there are hundreds of Data Brokers, our Members have requested that we opt them out on their behalf. Our Members have granted us power of attorney to process this request, per our attached terms and conditions.

Fair Credit Reporting Act

For all products / services that are subject to the Fair Credit Reporting Act, please enact a "security freeze" or similar stop to the selling or licensing of this Data.

Also, please mail a copy of the Data to the Member at the address provided in Addendum A.

GDPR

Several Members on this list may be European citizens and/or reside within the European Economic Area ("EEA"). You are required under the General Data Protection Regulation (GDPR) to provide access to and rectification or erasure of such Member's Data, Data portability, restriction of processing of their Data, the right to object to processing of their Data, and the right to lodge a complaint with a supervisory authority. Such Member(s) hereby request that all such actions be taken immediately.

Any transfers of Data by you from the European Economic Area ("EEA") must be done pursuant to European Commission approved Model Contractual Clauses.

Non-compliance with GDPR requests will be forwarded to the relevant Data Protection Authority and potentially followed by legal proceedings. **GDPR guidelines require a response to this letter within 30 days.**

We look forward to your response.

Our intention is to send a similar letter multiple times per year. We would prefer to work with your team in a more streamlined way. This is especially relevant regarding sending a copy of existing Data. We harbor no ill will, our Members would like to opt out permanently and delete existing Data where appropriate. We hope to work with your team to make this happen in the most efficient way possible.

Kind Regards,
Delete All My Data Foundation Inc

CC Office of the Massachusetts Attorney General
Attn to: Director of Data Privacy & Security

Message

From: Crenshaw, Jordan [REDACTED]
Sent: 12/9/2019 6:15:12 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Amended U.S. Chamber Comments
Attachments: CA AG Privacy Comments.pdf

I am submitting amended comments to the AG for the privacy rulemaking. It is the same content but a correct title in the letterhead. Thank you.

Jordan Crenshaw

Policy Counsel, Chamber Technology Engagement Center
U.S. Chamber of Commerce
Direct [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

December 6, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Proposed California Consumer Privacy Act Regulations

Dear Attorney General Xavier Becerra:

The U.S. Chamber of Commerce (“Chamber”) respectfully submits these comments in response to the proposed California Consumer Privacy Act (“CCPA” or “Act”) regulations (“Regulations”) put forward by the Attorney General.¹ As national economic growth becomes increasingly reliant on data-driven innovation, consumers should be able to have certainty that companies respect personal information. Congress should enact a national privacy law that protects *all* Americans equally regardless of which state they call home. The Chamber’s 225-member company Privacy Working Group, comprised of all industry sectors and small, medium, and large businesses, adopted principles for a national privacy framework during October 2018.² In furtherance of these principles, the Chamber proposed model privacy legislation to Congress on February 13, 2019, which draws upon many of the provisions of CCPA including information, opt out and deletion rights.³

Unfortunately, the CCPA, due in part to time pressures on the State of California (“State”) to pass privacy legislation before the deadline to remove a ballot initiative in 2018, contains many inconsistencies and ambiguities that makes it difficult for companies acting in good faith to operationalize its requirements. Complicating matters is the ongoing proposed ballot initiative known as the California Privacy Rights Act (“CPRA”)⁴ which would change many of CCPA’s requirements after companies spent time investing in compliance with the original Act.

¹ See Notice of Proposed Rulemaking, California Department of Justice (Oct. 11, 2019) *available at* <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf>.

² See U.S. Chamber Privacy Principles (October 2018) *available at* https://www.uschamber.com/sites/default/files/9.6.18_us_chamber_-_ctec_privacy_principles.pdf.

³ See U.S. Chamber Model Privacy Legislation (February 13, 2019 updated June 18, 2019) *available at* https://www.uschamber.com/sites/default/files/uscc_dataprivacymodellegislation.pdf.

⁴ See Proposed California Privacy Rights Act (November 13, 2019) *available at* https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

Because of statutory deficiencies, an unreasonable amount of time for companies to comply, and many ambiguities and requirements exceeding the authority of the CCPA, the Regulations will have a serious and deleterious effect on the national economy. According to the State's own Regulatory Impact Assessment ("RIA"), the proposed CCPA Regulations will cost up to **\$55 billion** in compliance costs for California companies alone.⁵ The RIA estimates fail to account for lost revenue for companies, compliance with CPRA (if adopted), and integration of other state frameworks with CCPA. These costs will impose a significant burden on businesses.

Even more worrisome to the Chamber is the fact that CCPA applies to companies outside California in states that are contemplating passage of fundamentally different privacy frameworks. Small businesses in particular will bear the burden of compliance and be competitively disadvantaged. CCPA applies to any company that does business in California and that "[a]lone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares the personal information of 50,000 or more consumers, households, or devices."⁶ A food truck operator that takes electronic payments for 137 unique customers per day or an online seller in Arizona that advertises to 137 unique devices per day could be subject to the requirements of the Act and its Regulations. The State's RIA assumes that the Regulation will require companies with fewer than 20 employees to incur up to \$50,000 in compliance costs.⁷

The Chamber asserts that consumers are entitled robust privacy rights but many small business owners, who are consumers themselves, should be afforded certainty and well-tailored regulations that enable them to operate and offer consumer protections. In addition all companies subject to CCPA should have certainty as to the scope of their requirements.

I. CONSUMERS SHOULD KNOW COMPANIES ARE READY TO PROTECT THEIR CCPA RIGHTS

Any major regulation, including those authorized by CCPA, should give the regulated community adequate time to institute compliance programs. The State's RIA estimates that the Regulations will cover up to 570,066 California companies, the vast majority of which are small and medium-sized businesses ("SMEs"). In order to give consumers more certainty about proper implementation of CCPA, giving companies the ability to know what the final Regulations are and have adequate compliance time will be paramount. Unfortunately, according to a July 2019 nationwide survey that poll mostly small businesses, only 11.8 percent of companies knew if CCPA applied to them.⁸ Many small businesses are just becoming aware of CCPA and will need adequate time to develop solutions to protect consumers' CCPA rights.

⁵ See Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, State of California Department of Justice and Office of the Attorney General at 11 (August 2019) *available at* http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

⁶ CAL. CIV. CODE § 1798.140(c)(1)(B).

⁷ See *supra* note 5.

⁸ See ESET CCPA Survey Results (July 19-22, 2019) *available at* https://cdn1.esetstatic.com/ESET/US/download/ESET_CCPA_Survey_Results.pdf.

Many SMEs must rely on technological solutions to be developed and become available many months before the new law's effective date in order to implement the CCPA's new requirements. As witnessed in Europe, a robust market for solutions to new privacy regulations takes time to develop and can only get started once the implementing regulations are in final form.

For a benchmark for a reasonable time for compliance, California should look to the European Union's General Data Protection Regulation ("GDPR"). The European Union adopted the GDPR's final regulations in April 2016 with a two-year implementation period before it took effect in May 2018. The GDPR gave regulated entities two full years to review the final regulations and develop or purchase compliance systems to implement into their daily business operations before those regulations took effect. In stark contrast to Europe's GDPR, CCPA's deadline for the Attorney General's rulemaking is July 1, 2020⁹, which is six months after the law becomes effective on January 1st. In fact, as currently written, it is possible that the Attorney General could begin State enforcement of CCPA on July 1, 2020—*the same day that final rules could be published*—leaving companies *little time* to comply with the final rules.

We encourage the Attorney General to begin enforcement on January 1, 2022 giving companies 18 months to comply, which is still fewer than GDPR's two years. We believe this is a sensible and balanced approach, especially since the GDPR was also predicated on a similar, well-established 1995 Data Protection Directive that EU Member States and businesses had long understood and complied with for many years, whereas the CCPA is an entirely new law with substantial new obligations for companies to undertake for the very first time. This timeline would also enable companies to integrate possible changes to CCPA if ballot initiatives like CPRA are adopted by voters.

Californians deserve to have their privacy protected in ways that are both strong and responsibly implemented. We strongly urge the Attorney General to grant consumers and companies adequate time to understand the yet-to-be published regulations and appropriately comply. Extending the implementation timeline until January 1, 2022 is responsible because it protects consumers from rushed and potentially incomplete compliance programs, and maximizes the ability of businesses to provide consumers with their privacy rights. Consumers benefit when they can trust that companies have built well-planned compliance and accountability programs to protect their statutory privacy rights.

II. THE PROPOSED REGULATIONS SHOULD BE MODIFIED TO ENHANCE CONSUMER PROTECTIONS AND COMPLY WITH CCPA AND ITS AMENDING STATUTES

A. Notice at Collection of Personal Information

Covered business under CCPA must "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

⁹ CAL. CIV. CODE § 1798.185(a).

categories of personal shall be used.”¹⁰ CCPA prohibits covered entities from collecting additional categories of personal information or alter the purposes for use without providing a consumer notice.¹¹

Section 999.305(a)(3) of the proposed Regulations would require covered businesses to obtain “explicit consent” from consumers to use data for purposes not described in the initial collection notice. No language in the Act authorizes the Attorney General to include an opt-in requirement for the use of data, especially in this context. From a policy standpoint, such a requirement would incentive companies to provide less specificity in their privacy policies weakening the Act’s intent to provide consumers notice. Additionally, the Regulations do not provide clarification as to how “explicit consent” is given. The final Regulations should focus on required updates to privacy policies as opposed to new obligations outside the scope of the statute.

B. Methods for Submitting Requests to Know and Requests to Delete

1) Companies Operating Exclusively Online

In October 2019, the Governor of California signed AB 1564 amending CCPA to enable companies doing business exclusively online to have to provide at a minimum an email address to accept consumer privacy rights requests. Prior to enactment of the amending statute, these companies would have been required to provide a toll-free telephone number to consumers for this purpose as well.¹² Companies that do not operate exclusively online still must provide a toll-free telephone number. The proposed Regulations at Section 999.312 do not account for this change and the Attorney General should modify the Regulations to comport with AB 1564.

2) Two-Step Deletion Requests

CCPA gives consumers the right to have any personal information, subject to exceptions, deleted.¹³ The Proposed Regulations at Section 999.312(d) would require companies to “use a two-step process for online requests to delete where the consumer must first, clearly submit the request to delete and then second, separately confirm that they want their personal information deleted.” The Chamber asserts that companies should have the flexibility to determine how deletion requests are processed. For example, consumers may prefer a “self-serve” process in which they are empowered to determine which types of data to delete.

3) Primary Interaction Method for Deletion and Right to Know Requests

In addition to providing at least two methods for receiving requests to delete and know information, the Regulations at Section 999.312(c) require that “[a]t least one method offered shall reflect the manner in which the business primarily interacts with the consumer, even if it requires a

¹⁰ CAL. CIV. CODE § 1798.100(b)

¹¹ *Id.*

¹² CAL. CIV CODE § 1798.130(a).

¹³ *Id.* at § 1798.105.

business to offer three methods for submitting requests to know.” The text of the CCPA does not contemplate this requirement; thus, the Attorney General lacks the authority to create an additional required submission procedure. The Regulations also fail to address how a business can determine its primary interaction channel with consumers.

C. The Presumption of a Request to Opt-Out of Sale

Section 999.313(d)(1) proposes that with regard to deletion requests, “if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified and shall instead treat the request as a request to opt-out of sale.” CCPA only requires that businesses delete data and request service providers do so upon verifiable request.¹⁴ The proposed Regulations exceed statutory authority because CCPA does not explicitly direct companies to treat unverified deletion requests as requests to opt out of sales.

From a practical perspective, the proposed Regulation may practically require companies that do not sell personal information—and for that reason do not offer a “Do Not Sell” button—to unnecessarily develop processes regarding opt-out requests. Secondly, the proposed Regulations threaten the trust relationship between companies and their consumers because the rules could force companies to stop sharing information at the request of individuals making fraudulent and unverifiable deletion requests in the name of another consumer.

D. Request to Opt-Out of Personal Information Sales

1) Browser-Initiated Opt-Out

CCPA requires that covered businesses honor requests by consumers directing them not to sell personal information.¹⁵ The Act further states that companies bound to this requirement must “[p]rovide a clear and conspicuous link on the business’s Internet homepage, title ‘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.”¹⁶

The proposed Regulations create requirements that go beyond what CCPA mandates. Section 999.315(c) of the Regulations would obligate covered entities collecting information online to “treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.” Although CCPA enables “authorized agents” to make opt-out requests on behalf of consumers, Section 999.135(g) would consider browser plugin or settings “requests” to be a request received directly from a consumer.

¹⁴ *Id.* at § 1798.105(c).

¹⁵ CAL. CIV CODE § 1798.120.

¹⁶ CAL. CIV CODE § 1798.135(a)(1).

A requirement that browser settings or plugins be construed as an opt-out request for purposes of CCPA fails to consider that these types of technology were designed in other contexts, and are not aligned with the Act's complex and extremely broad definitions of "sale"¹⁷ and "personal information."¹⁸ The CCPA emphasizes consumer choice and specifically defines the "Do Not Sell" button as a mechanism for opt-out. It is neither consistent with the statute to create this additional mechanism nor clear that consumers who use plugins intend to opt out of CCPA-defined sales.

Currently, browser-based opt-out technology is not sufficiently interoperable and developed to ensure that all parties that receive such a signal can operationalize it. Instead, the Chamber supports industry-based efforts to develop consistent technical signals for "Do Not Sell" technology, an effort that has been underway for over a year. Accordingly, the Regulations should clarify that any mechanisms not designed specifically for CCPA need not be honored as intending to effectuate a choice under CCPA.

2) Notifying Third Parties of Opt Out Requests

Consumers under the CCPA have the right to direct businesses not to sell personal information to third parties.¹⁹ Once a covered business has received the opt-out request, the statute mandates they refrain from selling personal information about the consumer to third parties and wait 12 months to contact the consumer about opting back into sales.²⁰

Section 999.315 of the Regulations though exceeds its statutory authority by imposing an additional requirement of notifying third parties of an opt-out request. Under the proposed Regulation,

A business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the consumer's request that the consumer has exercised their right to opt-out and instruct them not to further sell the information. The business shall notify the consumer when this has been completed.

CCPA Sections 1798.120 and 1798.135, granting the consumer opt-out right, do not state an obligation upon covered businesses to notify third parties of an opt-out request. Such a request

¹⁷ CAL. CIV CODE § 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.

¹⁸ See AB-874 (signed into law amending CCPA October 11, 2019) "Personal information" means information that identifies, relates to, describes, is reasonably 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 reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.

¹⁹ CAL. CIV CODE § 1798.120(a).

²⁰ *Id.* at § 1798.135(a)(4)-(5).

unnecessarily burdens the operations of covered businesses, as they would not have control over how third parties have treated personal information.

E. Training and Recordkeeping

Section 999.317 of the proposed Regulations requires businesses to maintain records of consumer requests and responses for at least 24 months. In particular, the Regulations mandate unnecessary and arbitrary recordkeeping and notice requirements for companies dealing with the personal information of 4,000,000 or more consumers. Under the proposal,

A business that alone or in combination, annually buys, receives for the business's commercial purposes, sells or shares for commercial purposes, the personal information of 4,000,000 or more consumers, shall:

- (1) Compile the following metrics for the previous calendar year:
 - a. The number of requests to know that the business received, complied with or in part, and denied;
 - b. The number of requests to delete that the business received, complied with in whole or in part, and denied;
 - c. The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and
 - d. The median number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.
- (2) Disclose the information compiled in subsection (g)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy.”

CCPA requires that company privacy policies need only include a description of a consumer's privacy rights and categories of data collected and shared.²¹ The statute does not require any metrics about consumer privacy rights requests and denials in its required privacy policy language.

The Attorney General delineates the recordkeeping requirements at businesses dealing with the personal information of 4,000,000 or consumers. The Attorney General's Initial Statement of Reasons (“ISOR”) indicates that the Office of Attorney General held discussions with SMEs about compliance. According to the ISOR, “[b]ased on these discussions and internal analysis, the Attorney General took a hybrid approach, limiting the more rigorous training and record-keeping requirements to businesses that handle the personal information of approximately 10% of California's population.”²² The reasoning to differentiate recordkeeping requirements based upon the 10 percent threshold arbitrarily fails to explain why the Attorney General settled on this number.

²¹ CAL. CIV CODE § 1798.130(a)(5).

²² See Initial Statement of Reasons, Proposed Adoption of California Consumer Privacy Act Regulations, at 44 (October 11, 2019) available at <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf>.

As noted above, the Regulations under Section 999.315 could also force covered entities to treat undefined user-enabled controls like a “browser plug-in” as a request to opt out of data sales. The contemplated signal requirements create operationalization challenges, as it is not clear that a covered business would or could actually count the number of “requesters” that have made opt-out requests, as those requests would not be moved through an active, business-tracked process.

Give the technological challenges associated with implementation of Section 999.315, the arbitrary decision to delineate recordkeeping requirements at 4,000,000 consumers, and the lack of statutory authority to implement such a requirement, the Chamber respectfully requests that the Attorney General eliminate the proposed Section 999.317 from the final Regulations.

F. Loyalty Programs and Financial Incentive Notice

1) Loyalty Programs

CCPA prevents covered businesses from engaging in “discriminatory” practices such as denying goods or services, charging different prices, or giving a different level of quality, against consumers that exercise their privacy rights under the Act.²³ An overly broad interpretation of the Anti-Discrimination rights in CCPA threatens the ability of retailers, banks, airlines, restaurants, and entertainment companies to offer loyalty and reward programs that greatly benefit consumers. According to one study, the overwhelming majority of consumers agree that loyalty programs save them money.²⁴ The Chamber strongly urges the Attorney General to interpret CCPA in a manner that ensures that the consumers continue to enjoy loyalty and rewards programs without disruption to businesses or their customers.

2) Financial Incentive Notice

Although prohibiting discrimination against consumer who exercise privacy rights, the Act permits covered businesses to offer financial incentives for data collection, sales, and deletion if the difference in price or quality of goods and services “is directly related to the value provided to the business by the consumer’s data.”²⁵ The covered entity must also provide notice to consumers and receive prior opt-in consent to enroll consumers in the incentive program.²⁶

The Regulations at Section 999.307(b)(5) propose that as part of the financial incentive disclosure, covered businesses must provide:

An explanation of why the financial incentive or price or service difference is permitted under the CCPA, including:

²³ CAL. CIV CODE § 1798.125(a).

²⁴ 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>.

²⁵ *Id.* at §1798.125(b)(1) as modified by the legislature.

²⁶ *Id.* at § 1798.125(b)(2)-(3).

- a. A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and
- b. A description of the method the business used to calculate the value of the consumer's data.

Currently, it remains a challenge for any business to assign value to a single consumer's data, and data often gains value when aggregated. The valuation of data is difficult for raw and individual data as opposed to insights from data that are dependent on context.²⁷ Every business and service is different, and requiring a business to disclose its methods and calculations could likely require disclosure of competitively sensitive information. Any Regulation regarding the financial incentive notice should specifically relieve companies from having to reveal trade secrets or proprietary information. CCPA already sufficient protects consumers with regard to discounts and such a requirement is unnecessary and could have a chilling effect on discounts.

G. Special Rules for Minors Under 13 Years of Age

CCPA requires that in order for a covered business to sell legally the personal information of children under 13 years of age, a consumer's parent or guardian must provide affirmative authorization.²⁸ Section 999.330 of the Regulations would require covered businesses with actual knowledge of collecting or maintaining personal information of children under 13 to "establish document, and comply with a reasonable method for determining that the person authorizing the sale of the personal information about the child is the parent or guardian." The Chamber strongly recommends that if a covered business follows comparable provisions of the Children's Online Privacy Protect Act to CCPA, the Attorney General should deem such business to have complied with those provisions of the Act.

III. THE CALIFORNIA ATTORNEY GENERAL SHOULD REMEDY THE MISSED OPPORTUNITY TO PROVIDE REGULATORY CERTAINTY THROUGH SAFE HARBORS IN ITS DRAFT REGULATIONS.

With this rulemaking, the Attorney General has the opportunity to clarify and strengthen the CCPA's statutory safe harbors that were designed to protect well-meaning businesses that take reasonable precautions to protect consumer data.²⁹ The CCPA provides that businesses are subject to a private right of action where they do not "implement and maintain reasonable security procedures and practices appropriate to the nature of the information," which results in the "unauthorized access and exfiltration, theft, or disclosure" of a consumer's "nonencrypted and

²⁷ See Testimony of Will Rinehart, Hearing on Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation at 2 (October 24, 2019) available at <https://www.banking.senate.gov/imo/media/doc/Rinehart%20Testimony10-24-19.pdf>.

²⁸ CAL. CIV CODE § 1798.120(c)-(d).

²⁹ 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>.

nonredacted personal information[.]”³⁰ The law allows businesses to quell private suits by “cur[ing]” an alleged violation.³¹ It was a mistake for the Attorney General not to address these statutory safe harbors in the draft rules, and that mistake should be remedied. The final rules should contain concrete guidance for organizations attempting to comply with the law. Doing so will provide needed regulatory certainty and protect businesses operating in good faith from abusive litigation.

Regulatory guidance is needed here given that the CCPA’s private right of action provision—absent clarification and strengthening of the safe harbor provisions—can result in substantial and unnecessary costs for businesses. The CCPA’s private right of action for certain security breaches authorizes consumers to sue for liquidated damages between \$100 and \$750 “per incident.”³² Moreover, the statute does not clearly require a showing of harm. This approach—which allows for uncapped statutory damages that are untethered from any real-world harm—is dangerous. As the U.S. Chamber of Commerce Institute for Legal Reform outlined in a July white paper, private rights of action in the privacy context can have disastrous consequences for businesses with little real benefit to consumers.³³ And those potential consequences are even more acute now, in light of the recently approved AB-1130, which broadens the categories of information for which businesses may be liable under the CCPA’s private right of action.³⁴

One way to partially alleviate the unintended consequences of private rights of action is to establish safe harbors—statutory or regulatory provisions that preclude liability if certain enumerated conditions have been met. Safe harbors benefit both businesses and consumers. *Businesses* are able to discern what their compliance obligations are and thus meet consumer protection mandates, without fear of undue liability or abusive litigation. *Consumers* reap the benefits of increased compliance, as businesses utilize the clear guidance to implement protections for personal information. For these reasons, among others, safe harbors are routinely used in consumer protection statutes in California and beyond.³⁵

³⁰ Cal. Civ. Code § 1798.150(a)(1); see also AB-1355, available at https://leginfo.ca.gov/faces/billCompareClient.xhtml?bill_id=201920200AB1355 (amending, *inter alia*, § 1798.150).

³¹ See *id.*, § 1798.150(b).

³² *Id.* § 1798.150(a)(1)(A).

³³ See *Ill-Suited: Private Rights of Action and Privacy Claims*, at 14, Chamber Institute for Legal Reform (July 2019), https://www.instituteforlegalreform.com/uploads/sites/1/Ill-Suited_-_Private_Rights_of_Action_and_Privacy_Claims_Report.pdf (“[P]rivate rights of action are routinely abused by plaintiffs’ attorneys, leading to grossly expensive litigation and staggeringly high settlements that disproportionately benefit plaintiffs’ lawyers rather than individuals whose privacy interests may have been infringed.”).

³⁴ See AB-1130, available at https://leginfo.ca.gov/faces/billCompareClient.xhtml?bill_id=201920200AB1130 (broadening definition of “personal information” in Cal. Civ. Code § 1798.81.5(d)(1)(A) to include additional identification numbers or biometric data, in combination with an individual’s first name or initial and last name); see also Cal. Civ. Code § 1798.150(a)(1) (incorporating definition of “personal information” from Cal. Civ. Code § 1798.81.5(d)(1)(A)).

³⁵ See Comments of the United States Chamber of Commerce re the California Consumer Privacy Act Rulemaking, at 9 n.41–46 (Mar. 8, 2019), available at https://www.uschamber.com/sites/default/files/ca_ag_privacy_comments_.pdf (“Chamber CCPA Comments”).

Given the plain text of the statute, which clearly establishes safe harbors,³⁶ the clear intent of its drafters,³⁷ and the numerous comments that the Attorney General received—including from the Chamber—urging for the regulations to include safe harbors,³⁸ the Attorney General should have clarified and strengthened the CCPA’s safe harbors in the draft regulations.³⁹ The Attorney General did not address this in the first drafts,⁴⁰ but can and should remedy this missed opportunity by adopting discrete safe harbor rules, including rules that:

- Clarify that a business that has implemented “reasonable security procedures and practices appropriate to the nature of the information” where it adopts information or data security practices recommended by an appropriate body, such as a standard-setting organization, a regulator, or a trade association, or when businesses can otherwise show that they have made good faith efforts to adopt compliance programs appropriate for the risks associated with the data they maintain;⁴¹ and
- Clarify that a business that implements “reasonable security procedures and practices”—as defined above—following a data breach will be found to have “cured” the breach within the meaning of the CCPA.⁴²

³⁶ Cal. Civ. Code § 1798.150(a)(1) (“Any consumer whose **nonencrypted and 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 . . .” (emphasis added)); *id.* § 1798.150(b) (“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.**” (emphasis added)).

³⁷ See *supra* note 28.

³⁸ See, e.g. *Chamber CCPA Comments* at 9–11; Comments of the California Chamber of Commerce at 34 (CCPA 00000112) (urging adoption of a “reasonable security” safe harbor consistent with the California Data Breach Report); Comments of the Toy Association at 7 (CCPA 00000191) (“We urge the Attorney General to consider a process to recognize [safe harbor] 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.”); Comments of Experian at 7 (CCPA00000259) (“[W]e 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.”); Comments of Okta, Inc. at 5 (CCPA 00000309) (requesting “safe harbor for reasonable security”); Comments of International Pharmaceutical & Medical Device Privacy Consortium at 2 (CCPA 00000417) (“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.”); Comments of the Los Angeles Area Chamber of Commerce at 1 (CCPA 00000553) (proposing safe harbor for implementing “recognized information security standard” (internal quotation omitted)); Comments of HITRUST at 1 (CCPA 00000604) (“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.”); Comments of Genetech at 8 (CCPA 00001364) (“The CCPA’s consumer private right of action enforcement mechanism should include a safe harbor for businesses that have implemented a data security program that is reasonable and consistent with recognized industry standards.”).

³⁹ See Cal. Civ. Code § 1798.185(a) (allowing for the Attorney General to engage in gap-filling and thus define safe harbors).

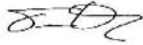
⁴⁰ See *generally* Proposed Text of California Consumer Privacy Act Regulations, available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf>.

⁴¹ See *Chamber CCPA Comments* at 10.

⁴² See *id.* at 10–11.

Clarifying and strengthening the statute's safe harbors in these ways will allow businesses to better operationalize and incorporate the CCPA's mandates. As a result, the safe harbors will provide certainty for businesses and better protect consumers.

Respectfully Submitted,



Tim Day
Senior Vice President
Chamber Technology Engagement Center



Harold Kim
Executive Vice President
U.S. Chamber Institute for Legal Reform

Message

From: Sarah Thompson [REDACTED]
Sent: 12/8/2019 10:37:16 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCPA questions/comments
Attachments: CCPA Questions for AG Open Session 12_3_2019.docx

Hello,

Attached are our questions/comments in regards to the CCPA. I apologize that this is a bit late. Unfortunately it got caught in my outbox Friday afternoon.

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

Regards,
Sarah Thompson
Chief Product Officer
Siemly Global, LLC
www.siemly.com
[REDACTED]

CCPA Implementation Guideline Questions

Submitted by Siemly Global, LLC

Contact: Sarah Thompson ([REDACTED])

www.siemly.com

General Questions

1. Can a consumer only submit 2 DSARs per year to the same company or only exercise a right twice per year with the same company? For example, if a consumer asks a company what data of theirs they have and then submits a second DSAR to the company to opt out of sale, would the company be required to respond to a third request by the consumer to delete all of their data during that same year?
2. What are the requirements for a business's third-party suppliers to delete data if the consumer does not ask them directly? Is this stated anywhere in the reg?
3. Are all companies that use google ads or analytics or the like subject to CCPA if they make more than 50% of their annual revenue from selling ad space? It seems like they would be regardless of annual revenue or whether they sell consumer's data in any other manner.
4. The regulations specifies that only for profit companies are subject to CCPA. However, there are many not of profit companies that collect large amounts of sensitive personal information from California consumers such as credit unions for example and religious organizations. Is there any case where they would need to comply with CCPA?

Sect 999.301

PG 2, Section (n)

1. Where is there a complete list of categories and their definitions?
 - a. Data categories
 - b. Source categories
 - c. 3rd party categories
2. If I collect IP addresses from website visitors do the business need to say that they collect IP addresses, or do I need to state the exact address they collected.
3. 999.301 (a) states that the parent of a minor must confirm their request for opt-in, after submission. If the consumer does not do this, what does the business do? Can it close the request after 45 days and simply out the user out?
4. Does the business have to remind the consumer to verify their submission during this 45-day period?

Sect 999.305 Notice at collection of personal information

PG 4, Section (a)(3)

1. How does a company inform change of use for consumer's they have no contact information for such as website visitors?

2. If a business did not have a “opt-in” button on their website after Jan.1, 2019, do they need to send privacy policy notices to anyone whom they collected data from in 2019?

Sect.999.313 Responding to Requests to Know and Requests to Delete

1. Does a consumer have to submit a separate request for deletion to all companies a business shares/sells their data to?
2. Does the business have to notify third parties of deletion requests at all?

PG 11, Section(b)

1. 999.308 (d)states that the consumer must confirm their request for deletion, after submission. If the consumer does not do this, what does the business do?
2. Can it close the request after 45 days and simply out the user out?
3. Does the business have to remind the consumer to verify their submission during this 45-day period?

PG 12, Section(c)(6)

1. What are reasonable security measures? Is email reasonable?
2. If not, can you require that the user creates an account on a third-party system to handle secure communication?

PG 12, Section(c)(7)

1. In the interest of security, can a business require that the user creates an account on a third-party system to handle secure communication if the user does not possess or the business does not offer existing password protected portal access?

PG 14, Section(3)

1. In reference to archived or backup systems, what does “next accessed or used” mean? If the backup runs nightly, is that “used” or does it refer to when a backup schedule is modified? If the business does not modify the schedule wouldn’t that mean the data may never be deleted?

PG 14, Section(4)

1. What does it mean to specify the manner in which data is deleted? Does the business need to disclose specific systems they use and how they are accessed?

Sect 999.314 SERVICE PROVIDERS

PG 15, Section(d)

1. On what basis can/must a service provider deny a consumer request?)

Sect 999.315 Requests to Opt-Out

Pg 16 (f)

1. Can a consumer opt-out of data sharing, not just selling?
2. Why do they only have to inform third parties they sold data within the past 90 days? Doesn’t the request apply to the preceding 12-month period?

3. Does the business have to specify the company names and data categories sold to those third parties or just the 3rd party's category?
4. Does the business need to be explicit about what data they have collected prior to opt out?
5. What are the guidelines for the business to send this request to the third party in order for it to be secure and auditable?
6. What does the third party need to do on receipt of this notice from the business?
 - a. What proof do they need to provide that they have complied with the request?
 - b. How long do they have to comply with the request?
7. Does the business require any proof of compliance from the third party before they can close/respond to the request?

Sect 999.317 Training; Record-Keeping

Pg 16 (a)

1. Are there certified training programs that trainers can attend? If not, how does a business find qualified trainers?

Pg 16 (b)

2.
Can the consumer make a request for deletion of the request record data since it can include very sensitive information?
3. What if the company keeps the request data for longer than 24 months?

Sect 999.318 Requests to Access or Delete Household Info

Pg 18 (b)

1. How can a business verify household members in order to comply with DSARs? How are they to know who lives in the household and their contact information to obtain opt-in?

Sect 999.323 General Rules Regarding Verification

Pg 219 (e)

1. If a business does anonymize the request data in the interest of security, how can a business prove that they have complied with a specific request or track who has submitted requests within a 12-month period?

Sect 999.325 General Rules Regarding Verification

Pg 20 (b)

1. What is a reasonable degree of certainty? 60% certain? 80%?

Pg 20 (c)

1. What constitutes "a signed declaration".
 - a. Does it need to be an actual signature?
 - i. If so, doesn't this increase the risk to the requestor?
 - b. Can it be an electronic signature?
 - c. Can it be an acknowledgement button in an email?

Sect 999.330 Minors Under 13 Years of Age

Pg 21(c)

1. What is sufficient proof of age? Age verification tool which can perform document verification for example or simply a checkbox "Are you over 18"?
2. If opt-in is required for minors under 16, does that not mean that everyone must opt-in unless the company employs a third-party identity verification tool to confirm a person's age?

Pg 22(c)

3. How is a phone or video call a verification method of guardianship? Is ID required to be submitted?

Message

From: Tonsager, Lindsey [REDACTED]
Sent: 12/6/2019 5:28:54 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCPA Rulemaking - Written Comments of the Entertainment Software Association
Attachments: Written Comments of the ESA.pdf

Dear Privacy Regulations Coordinator:

Please find attached the comments of the Entertainment Software Association in connection with the Attorney General Office's rulemaking on the California Consumer Privacy Act of 2018.

Respectfully submitted,
Lindsey Tonsager
Counsel for the Entertainment Software Association

Lindsey Tonsager

Covington & Burling LLP
Salesforce Tower, 415 Mission Street, Suite 5400
San Francisco, CA 94105-2533
[REDACTED]

www.cov.com

COVINGTON

This message is from a law firm and may contain information that is confidential or legally privileged. If you are not the intended recipient, please immediately advise the sender by reply e-mail that this message has been inadvertently transmitted to you and delete this e-mail from your system. Thank you for your cooperation.



December 6, 2019

Via Email

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

RE: Written Comments on the Proposed CCPA Regulations

To Whom It May Concern:

The Entertainment Software Association (“ESA”)¹ submits these comments in response to the Attorney General’s Notice of Proposed Rulemaking implementing the California Consumer Privacy Act (“CCPA” or “Act”).² ESA’s members share the Attorney General’s goal of protecting the privacy and security of consumers’ personal information, and we appreciate the significant efforts of the Attorney General’s Office to provide industry guidance on the scope and application of the Act’s requirements.

In particular, ESA appreciates the Attorney General’s clarification that a business has the option of permanently and completely erasing, de-identifying, or aggregating personal information in response to a verifiable deletion request.³ This proposed approach should be retained in the final regulation. Together with the cure period, these options serve as important

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 California Department of Justice, Notice of Proposed Rulemaking Action (Oct. 11, 2019), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf>.

³ California Department of Justice, Proposed Text of Regulations, § 999.313(d)(2) [hereafter, “Proposed Regulations”]. As explained in the comments we filed in connection with the Attorney General’s hearings on the CCPA, ESA requests that the Attorney General clarify that imprecise location information (such as zip code) is not “personal information” under the CCPA.

safety valves to protect consumers' rights while also avoiding "gotcha"-style enforcement and encouraging innovation in automated systems and processes to comply with consumer requests.

A number of areas remain, however, that create unnecessary uncertainty or require further clarification. Specifically, ESA requests that the Attorney General further revises its CCPA regulations to address the following issues:

- Explicitly permit businesses to protect the security and integrity of their systems and networks;
- Permit service providers to process personal information consistent with the statutory text;
- Delete the requirement to publish compliance metrics;
- Align the requirement to obtain explicit consent for privacy policy updates with the Federal Trade Commission's longstanding precedent for material retroactive changes;
- Clarify that providing a website address where a printable version of the privacy policy is available is sufficient to satisfy the requirement that the policy be printable;
- Clarify the requirements related to the opt out of "sale" by (a) specifying that personal information is not "sold" where it is not exchanged for "monetary or other valuable consideration"; (b) aligning the Proposed Regulations with the verifiable parental consent mechanisms recognized under the Children's Online Privacy Protection Act ("COPPA")⁴; (c) reducing the burden required for consumers who want to opt in; (d) eliminating the new requirement that businesses treat unverified deletion requests as requests to opt out; and (e) striking the new requirement that businesses pass through opt-out requests to third parties.

Each of these requests is considered in more detail below.

I. The regulations should explicitly recognize that businesses may take steps necessary to protect the security and integrity of their systems and networks.

As currently drafted, the CCPA's access, deletion, and portability rights⁵ are vulnerable to abuse by malicious actors. Research involving similar consumer rights under the European Union's General Data Protection Regulation demonstrates how identity thieves, fraudsters, and other criminals can abuse such rights.⁶ ESA and its members appreciate the Attorney General's recognition that measures to detect and prevent security incidents, fraud, and other unlawful

⁴ 15 U.S.C. § 6501, *et seq.*

⁵ As drafted, the Proposed Regulations do not appear to incorporate all of the statutory amendments that the California Governor signed into law in October 2019. For example, the statute, as amended, no longer requires all businesses to maintain a toll-free telephone number to receive consumer requests. ESA requests that the Attorney General harmonize the final regulations with all of the statutory amendments and apply the same methods for access, portability, and deletion requests.

⁶ See, e.g., Andrew Ross, "How Cyber Threats Could Grow Under GDPR," *Information Age* (May 14, 2018), available at <https://www.information-age.com/cyber-threats-gdpr-123472491/>; Martino et al., "Personal Information Leakage by Abusing the GDPR 'Right of Access,'" available at "<https://marianodimartino.com/dimartino2019.pdf>".

activity are important and permitted under the CCPA.⁷ ESA's members urge the Attorney General to further clarify the scope of the regulations to further prevent malicious actors from abusing the CCPA rights.

Our members have implemented a number of important controls to help ensure that video game players have a fun and fair gameplay experience. For example, members may use proprietary technologies to determine when a player is using illegal software that infringes intellectual property, is attempting to engage in fraud in connection with in-game purchases, is harassing or bullying other players through an in-game chat, or is cheating or otherwise engaging in behavior that violates the game rules. Once this malicious activity is detected, an ESA member may take a range of actions including to suspend or block the account from using online game services or other action consistent with the game's terms of use. The malicious actor may then try to use the CCPA's access or portability rights to try to reverse engineer what specific information or action resulted in the suspension or termination of the account in order to try to circumvent the controls and evade detection in the future.

Moreover, individuals might try to use the portability right in ways that could violate a game publisher's trade secrets or intellectual property rights. For example, a person's raw gameplay and game character information may contain creative elements that cannot be technically transposed into another game or that could infringe the copyrights and other intellectual property rights that the game publisher has in such elements if ported to another game. The statutory text expressly directs the Attorney General to protect these rights and avoid having portability be used as a tool of infringement.⁸

The statutory text of the CCPA and the proposed regulations already appear to generally permit video game companies to deny consumer access, deletion, or portability requests where the company has a good faith belief that the request is fraudulent, malicious, or would facilitate unlawful activity. This would include rejecting requests for data sets that could be used to draw insights into system architecture (which could then be used to try to compromise those systems). However, to avoid any ambiguity and send a strong message to fraudsters and other bad actors that the state of California will not tolerate any abuse, we strongly urge the Attorney General to clarify the Proposed Regulations as follows:

Nothing in the statute or these regulations shall restrict a business's ability to ensure security and integrity.

In addition, the regulations should add a new definition of "security and integrity":

"Security and integrity" means the ability: (1) of a network or an information system to detect security incidents that compromise the availability, authenticity, integrity, and

⁷ See, e.g., Proposed Regulations, §§ 999.314(c) (permitting service providers to broadly use personal information for security and anti-fraud purposes), 999.315(h) (allowing a business to refuse fraudulent opt-out requests); 999.323(c) (authorizing the collection of additional information during the verification process for security and fraud-prevention purposes). ESA requests that the Attorney General further clarify that the explanation that a business believes an opt-out request is fraudulent may be provided at a high enough level of generality to avoid making it easier for malicious actors to reverse-engineer or otherwise circumvent fraud detection mechanisms.

⁸ Cal. Civ. Code § 1798.185(a)(3).

confidentiality of stored or transmitted personal information; (2) to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions, and to help prosecute those responsible for such actions; (3) to protect trade secrets and intellectual property rights; and (4) to ensure the safety of natural persons.

This revision not only furthers the purposes of the CCPA by taking into consideration security concerns and upholding legal rights (including those relating to trade secrets and intellectual property),⁹ but also is consistent with clarifications recently sought by consumer advocates.¹⁰

II. The regulations should be clarified to avoid unduly restricting service providers' lawful data processing.

Section 999.314(c) of the Proposed Regulations states that a service provider cannot “use personal information received either from a person or entity it services or from a consumer’s direct interaction with the service provider for the purpose of providing services to another person or entity” unless it is “necessary to detect data security incidents, or protect against fraudulent or illegal activity.”¹¹ The ISOR notes that this provision

clarifies that a service provider’s use of personal information collected from one business to provide services to another business would be outside the bounds of a “necessary and proportionate” use of personal information. Doing so would be advancing the “commercial purposes” of the service provider rather than the “business purpose” of the business.

ISOR at 22.

ESA and its members request that the Attorney General clarify this language to explain that service providers also can, consistent with the statutory text, use the information they receive from one business for the service provider’s own operational purposes (including to provide services to other businesses) *as long as* the use is part of the services specified in the written contract with the business.

This clarification is necessary to avoid treating the statutory text in the “business purposes” definition as surplusage. The CCPA defines a “business purpose” to include the use of personal information for the “service provider’s operational purposes.”¹² In addition to detecting security incidents and protecting against fraudulent or illegal activity,¹³ the statute expressly includes a number of other “operational purposes” that constitute “business purposes”

⁹ Cal. Civ. Code §§ 1798.185(a)(3), (7).

¹⁰ See, e.g., Alastair Mactaggart, Letter to the Office of the Attorney General (Nov. 4, 2019) (regarding submission of amendments to the California Privacy Rights and Enforcement Act of 2020), https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

¹¹ Proposed Regulations, § 999.314.

¹² Cal. Civ. Code § 1798.140(d).

¹³ Cal. Civ. Code § 1798.140(d)(2).

when performed by the service provider. These activities include (for example) providing analytic services, debugging to identify and repair errors, verifying customer information, and providing advertising or marketing services.

Importantly, these “business purpose” activities often require the service provider to combine and process personal information received from multiple businesses in order to provide the contracted-for services back to these businesses. For example, a mobile game developer may use a third-party debugging service that receives personal data (such as device and other unique identifiers) any time the game crashes. To effectively detect patterns (e.g., that a specific version of a mobile operating system is causing crashes on a specific type of device) and troubleshoot the problem, the debugging service may need to combine and analyze the information it receives from all of its business customers. If it is restricted to analyzing the data it receives from a single customer alone, it might not be able to detect the issue and the issue would remain unresolved. Similarly, an analytics service provider must combine and analyze the personal information that it receives from all of its business customers in order to derive the analytics reports and business insights that make up the contracted-for analytics services.

As drafted, Section 999.314(c) of the Proposed Regulations is ambiguous because it could be interpreted as prohibiting the service provider from combining and analyzing the information it receives from multiple business customers for these contracted-for business purposes. Such a reading would, in effect, convert all of the examples of “business purposes” contained in Section 1798.140(d) of the statute — except for the small subset of security and fraud purposes contained in Section 1798.140(d)(2) — into surplusage, which the California Supreme Court expressly disfavors.¹⁴

To avoid this result, the Attorney General should clarify that Section 999.314(c) of the CCPA regulations are not so narrow. Specifically, the Attorney General should specify that a service provider’s data processing is “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” as long as the processing is to provide the services specified in the contract with the business.

This alternative interpretation resolves the relationship between the three definitions that the Attorney General considered in its ISOR (i.e., “service provider,” “business purpose,” and “commercial purpose”) in a manner that is more consistent with the statutory text and avoids treating any statutory language as superfluous. Importantly, it aligns the “business purpose” definition with the language in the “service provider” definition prohibiting the service provider from “retaining, using, or disclosing the personal information for a commercial purpose *other than* providing the services specified in the contract with the business” or for “any purpose other than for the specific purpose of performing the services specified in the contract for the business.”¹⁵ It also tethers the permitted service provider activities to the context in which the service provider collects the information — i.e., to provide the contracted-for services (e.g., fraud

¹⁴ *Copley Press, Inc. v. Superior Court*, 39 Cal. 4th 1272, 1286, 141 P.3d 288, 296 (2006).

¹⁵ Cal. Civ. Code § 1798.140(v) (emphasis added).

detection, preventing security incidents, analytics, or debugging to identify and repair errors) to the business.

For these reasons, ESA requests that the Attorney General revise Section 999.314(c) as follows:

A service provider shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose of providing services to another person or entity, except as *reasonably necessary and proportionate to perform the services specified in the contract for the business*. ~~A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary detect data security incidents, or protect against fraudulent or illegal activity.~~

III. Publishing compliance metrics in a company's privacy policy does not further any statutory purpose and could create consumer confusion.

The Proposed Regulations impose certain reporting obligations on companies that alone or in combination, annually buy, receive for the business's commercial purposes, sell, or share for commercial purposes, the personal information of 4,000,000 or more consumers. Specifically, such businesses, must publish certain metrics regarding the number of requests they received, complied with, or denied, and the median number of days it took to respond to requests.¹⁶ The ISOR explains that these metrics are necessary to inform the Attorney General, policymakers, academics, and members of the public about businesses' compliance with the CCPA.

However, this requirement serves no statutory purpose. Importantly, academics and members of the public do not need this information to ensure compliance with the CCPA, because the California legislature already refused to provide a private right of action in the context of consumer access, deletion, and opt-out requests.¹⁷ The Proposed Regulations already require businesses to maintain a record of the requests they received and how they responded to those requests,¹⁸ and the Attorney General has adequate means at his disposal to seek access to this information in the ordinary course of his regulatory and enforcement activities.

Moreover, the requested metrics do not achieve the stated purpose of assessing legal compliance. The fact that a request was denied does not, alone, demonstrate noncompliance, as the business might have lawfully relied on an applicable exception or lawfully denied the request based on a reasonable determination that it was fraudulent. Similarly, publishing the median number of days taken to respond to requests does not reflect on compliance. A business might report a median number of days lower than 45 days even if it had multiple occasions where it

¹⁶ Proposed Regulations, § 999.317(g).

¹⁷ SB 561 would have granted consumers a private right of action for any violation of the CCPA. SB 561 was placed on the suspense file earlier this year.

¹⁸ Proposed Regulations, § 999.317(b).

unjustifiably responded *after* the statutory deadline had passed, and a business might report a median number of days higher than 45 days even if it had acted lawfully by properly seeking an extension under the statute.¹⁹ Consequently, the requirement would appear on its face to be arbitrary and capricious.

Compiling the required metrics also might not be practically feasible. In many cases, a business will not be able to determine whether a consumer is a California resident, but may respond to the individual's request regardless as a voluntary best practice. The regulations do not appear to require these individuals to be considered when determining whether the 4 million threshold (which also has no reasonable basis and appears to have been arbitrarily selected) has been met, since "consumers" are defined to include only California residents. But this variability could significantly skew the metrics and make them less reliable.

Unfortunately, the most likely result of publishing these metrics is to create consumer confusion around their meaning and import.²⁰ In responding to consumer requests under the European Union General Data Protection Regulation, it is the experience of ESA members that each consumer request to exercise access or deletion of personal information is unique. However, a California consumer might compare his or her own experience against these metrics and become frustrated if their specific request is taking longer than the average or is denied, even though there may be entirely legitimate reasons for the delay or the denial. The consumer might also have the misimpression that these metrics represent legal standards, and that any delay or denial is unlawful, when this clearly is not the case for the reasons described above.

Consequently, we respectfully request that the Attorney General strike Section 999.317(g) of the Proposed Regulations and instead seek this information as needed in the ordinary course of regulatory and enforcement activities.

¹⁹ The draft regulations require businesses to respond to requests to know and to delete personal information within 45 days, "regardless of time required to verify the request." Proposed Regulations, § 999.313(b). Forcing businesses to hurry through verification procedures to meet arbitrary and capricious deadlines significantly jeopardizes the security of consumers' personal information and compliance with other laws that may require the business to withhold the data from the consumer or to retain the data. *See, e.g.*, Cal. Civ. Code § 1798.81.5 (West). It also overlooks the statutory text in Section 1798.145(j)(1) that plainly states that a "time period for a business to respond to any verified consumer request may be extended by up to 90 *additional* days where necessary," such as where the consumer delayed the business's reasonable efforts to verify the request (emphasis added). To better protect consumers and facilitate legal compliance, we request that the Attorney General clarify that businesses can seek an additional 90-day extension where a consumer does not promptly verify their request.

²⁰ The requirement in the draft regulations that businesses disclose the value of the consumer's data and the results and methods of calculating that value also are likely to be impractical and encourage competitors to seek access to sensitive proprietary information. Proposed Regulations, § 999.307. In addition, this requirement runs contrary to established California case law that assigns no value to personal information. *See In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at *14 (N.D. Cal. Sept. 20, 2011) ("Numerous courts have held that a plaintiff's 'personal information' does not constitute money or property under the [Unfair Competition Law]."). Accordingly, we propose striking sections 999.307(b)(5) and 999.337 of the Proposed Regulations.

IV. Any requirement to obtain explicit consent for privacy policy updates should align with longstanding Federal Trade Commission precedent.

Under the proposed regulations, a business must notify the consumer and obtain explicit consent before processing personal information for a purpose that was not previously disclosed to the consumer in the notice provided at or before collection.²¹ ESA appreciates the Attorney General's concern that a "consumer could have reasonably relied on the information provided in the notice at collection when interacting with the business,"²² and encourages the Attorney General to align the regulations with the more than fifteen years of Federal Trade Commission ("FTC") precedent on this issue.

The FTC has long held that *retroactive* application of *material* changes in a business's data practices may be deceptive or cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition.²³ In such circumstances, the FTC requires the business to provide prominent disclosures and obtain opt-in consent before using the consumer's data in a materially different manner than claimed when the data was obtained.²⁴

This approach, which is based on whether the change is material (i.e., is likely to affect the consumer's conduct or decision with regard to a product or service²⁵) and retroactive (i.e., applies to information collected prior to the effective date of the new policy), strikes the right balance of getting consumers the information they need and providing consumers appropriate choices, without unduly overwhelming consumers or interrupting the consumer experience when the changes have minimal impact on the consumer's privacy interests. As former FTC Chief Technologist Ashkan Soltani explained in his testimony before the California Senate Judiciary Committee's hearing on the CCPA, there is a significant risk that consumers will begin to get notice fatigue if they are asked to affirmatively assent to *every* new purpose for which a business processes data, regardless of whether that new purpose is materially different than those previously disclosed or is retroactive. In such circumstances, the Proposed Regulations could have the unintended effect of making consumers less likely to read notices before opting in to the changes.

To avoid this result, and to bring the CCPA into alignment with established legal precedent, ESA recommends that the Attorney General make the following changes in bold to Section 999.305(a)(3) of the Proposed Regulations:

²¹ Proposed Regulations, § 999.305(a)(3).

²² California Department of Justice, Initial Statement of Reasons, at 8-9, <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf> [hereafter, "ISOR"].

²³ Federal Trade Commission, Complaint, *In Re Gateway Learning Corp.*, No. C-4120, 2004 WL 2618647, at 5 (F.T.C. Sept. 10, 2004), <https://www.ftc.gov/sites/default/files/documents/cases/2004/09/040917comp0423047.pdf>.

²⁴ *Id.* at 3; see also Federal Trade Commission Report, *Protecting Consumer Privacy in an Era of Rapid Change*, at 58, <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

²⁵ Federal Trade Commission, *FTC Policy Statement on Deception* (Oct. 14, 1983), appended to *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984).

~~*A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection. If the business intends to retroactively use a consumer's personal information for a purpose that was not is materially different than what was previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of prominently disclose this new use to the consumer and obtain express affirmative consent explicit consent from the consumer to use it for this new purpose.*~~

V. The regulations should clarify that providing the website address for a printable version of the privacy policy is an acceptable way to enable print functionality.

Under the Proposed Regulations, businesses must make their privacy policies available in a printable format.²⁶ ESA and its members support the CCPA's goal of making privacy policies accessible for all consumers. As the "Internet of Everything" expands beyond desktop computers and laptops to include devices that have no reason to connect to a printer, ESA encourages the Attorney General to provide companies flexible alternatives to ensure consumers can access printable copies of privacy policies.

For example, video game consoles and handheld gaming devices do not have print functionality given that they are designed for gaming and entertainment purposes and not, for example, document processing. ESA's members take steps to ensure that consumers can access privacy notices through these devices and provide the website URL where a consumer can access a printable version of the privacy notice through a web browser on a printer-connected device. We believe providing the website URL qualifies as an "additional format" under the Proposed Regulations, but ask the Attorney General to clarify by revising the Proposed Regulations as follows:

Be available in an additional format that allows a consumer to print it out as a separate document, such as a website address where the consumer can access a printable version of the privacy policy.

This approach is consistent with Section 999.306(c)(5) of the Proposed Regulations, which similarly permits businesses to include a website address for a business's privacy policies in the case of a printed form containing the notice of a right to opt-out.

VI. The Attorney General should clarify the "sale" opt-out requirements.

As explained further below, ESA requests that the Attorney General clarify the requirements related to the opt out of "sale" by (a) specifying that personal information is not "sold" where it is not exchanged for "monetary or other valuable consideration"; (b) aligning the Proposed Regulations with the verifiable parental consent mechanisms recognized under the Children's Online Privacy Protection Act ("COPPA")²⁷; (c) reducing the burden required for consumers who want to opt in; (d) eliminating the new requirement that businesses treat

²⁶ Proposed Regulations, § 999.308(a)(2)(e).

²⁷ 15 U.S.C. sections 6501, *et seq.*

unverified deletion requests as requests to opt out; and (e) striking the new requirement that businesses pass through opt-out requests to third parties.

A. Specify that personal information is not “sold” if the exchange of data is not “for monetary or other valuable consideration.”

ESA’s members are focused on creating dynamic interactive experiences that challenge the boundaries of storytelling, competition, and social interaction. They are not in the business of selling data for commercial purposes or profit. Personal information often *does* need to be disclosed, however, between the operator of the gaming console or handheld device and the video game publisher in order to offer a wide range of video game services to players. In addition, ESA’s members contract with a wide range of business partners who need personal information in order to provide important services that promote game development, enable game functionality, detect fraud and intellectual property infringement, and facilitate more effective promotion and advertising of game services to existing and prospective players. While some of these business partners are service providers, others may be considered third parties who use personal information to provide the contracted-for services but who do not receive such data for monetary or other valuable consideration.

Because there is significant confusion and uncertainty regarding the scope of the CCPA’s “sale” definition, ESA requests that the Attorney General clarify that disclosures of personal information do not constitute a “sale” unless the personal information is disclosed “for monetary or other valuable consideration.” This interpretation is supported by the plain text and legislative history of the statute, which require that personal information be exchanged for monetary or other valuable consideration.²⁸ An interpretation of the statute that treats *any* disclosure of personal information to another business or third party as a sale would impermissibly read the words “for monetary or other valuable consideration” out of the statute.²⁹

Permitting disclosures of personal information to third parties who receive personal information to provide or facilitate video game services to players also is consistent with case law interpreting the meaning of “other valuable consideration.” The Supreme Court of California has adopted the “bargained-for exchange” test for determining what constitutes

²⁸ Cal. Civ. Code § 1798.140(t); *see also* California Senate Judiciary Committee Bill Analysis (AB 375) at 17–18 (June 26, 2018) (“‘Sell’ as used in this bill would essentially delete this second section of the definition [contained in the preceding ballot initiative, which would have included] importantly the sharing of the information for no consideration to a third party for that party’s commercial use. It is unclear why this change was made, but its effect would be that a consumer could not opt out of the sharing of their personal information with third parties, so long as there is not valuable consideration received.”); California Assembly Floor Analysis (AB 375) at 7 (June 25, 2018) (referring to a “narrowing of the definition of ‘sell’ to remove reference to situations that do not involve valuable consideration”).

²⁹ *Corley v. United States*, 556 U.S. 303, 314 (2009); *Smith v. Superior Court*, 137 P.3d 218, 221 (Cal. 2006) (“[W]e give significance to every word, phrase, sentence, and part of an act in pursuance of the legislative purpose.”) (citing *People v. Canty*, 90 P.3d 1168, 1172 (Cal. 2004)) (internal quotation marks omitted); *Shoemaker v. Myers*, 801 P.2d 1054, 1067 (Cal. 1990) (“We do not presume that the Legislature performs idle acts, nor do we construe statutory provisions so as to render them superfluous.”).

“valuable consideration.”³⁰ In the typical scenario where personal information is disclosed to provide or facilitate video game services to players, the business promises to pay the third party money to induce or motivate the third party to perform the contracted-for services to players. In exchange, the third party promises to perform such services to induce or motivate the business to remit payment. Although personal information may need to be exchanged so that the third party can perform the contracted-for services, both parties have not “so understood and intended” the exchange of data to be the “plan and purpose for which the consideration was paid” or provided.³¹ In such circumstances, personal information is not exchanged for “monetary or other valuable consideration” and, accordingly, there is no “sale” for CCPA purposes.³²

B. *The parental consent mechanisms permitted under the regulations should align with the verifiable parental consent mechanisms recognized under COPPA.*

As drafted, Section 999.330(a) creates ambiguity regarding whether businesses can rely on existing processes for obtaining verifiable parental consent under COPPA to comply with the CCPA’s parental consent requirements. Specifically, Section 999.330(a) states:

A business that has actual knowledge that it collects or maintains the personal information of children under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. This affirmative authorization is in addition to any verifiable parental consent required under the Children’s Online Privacy Protection Act, 15 U.S.C. sections 6501, *et seq.*

³⁰ See, e.g., *Jara v. Suprema Meats, Inc.*, 121 Cal. App. 4th 1238, 1248–49 (Cal. Ct. App. 2004) (explaining that “[t]o constitute 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” (quoting Restmt. 2d of Contracts § 71)); *Stern v. Franks*, 35 Cal. App. 2d 676, 678 (Cal. Dist. Ct. App. 1939) (“Nothing is consideration that is not regarded as such by both parties” (quoting *Philpot v. Gruninger*, 81 U.S. 570, 577 (1871))); *People v. Cardas*, 137 Cal. App. Supp. 788, 791 (Cal. App. Dep’t 1933 (although participants in a sweepstakes gave the promotor something of value, that gift was not a condition upon which the chance to participate in the sweepstakes was delivered; therefore, no consideration was exchanged); see also *Colorado Nat. Bank of Denver v. Bohm*, 286 F.2d 494, 496 (9th Cir. 1961) (In determining whether consideration was exchanged, the Ninth Circuit identified a fundamental common law principle “that consideration must be bargained for- it must be the thing which the parties agree shall be given in exchange for the promise”).

³¹ *People v. Gonzales*, 62 Cal. App. 2d 274, 282–283 (Cal. Dist. Ct. App. 1944) (quoting *State v. Danz*, 250 P. 37 (Wash. 1926)) (internal quotation marks omitted).

³² ESA appreciates that, consistent with the statutory text of the CCPA, the draft regulations do *not* require businesses to honor do-not-track signals as opt-out-of-sale requests. The draft regulations appear to appropriately recognize that “do not sell” is not equivalent to “do not track” by requiring businesses to honor user-enabled privacy controls only for *sales* of personal information, rather than for online *tracking*. Compare Cal. Bus. Prof. Code Section 22575(b)(5) (defining “do not track” signals as communicating a consumer’s “choice regarding the collection of personally identifiable information about an individual consumer’s online activities over time and across third-party Web sites or online services”), with Proposed Regulations Section 999.315(c) and Cal. Civ. Code § 1798.140(t) (defining “sale” as the exchange of personal information “for monetary or other valuable consideration”). To avoid requiring technical compatibility with every “do not sell” plugin or setting that could emerge (which is not practically possible), ESA encourages the Attorney General to clarify in the final regulations that this requirement applies only to commonly-accepted and industry standard user-enabled privacy controls.

Section 999.330(a)(2) lists six specific methods that the Attorney General characterizes as “reasonably calculated to ensure that the person providing consent is the child’s parent or guardian.” However, it is not clear whether this list is exhaustive, and the list notably departs in some significant respects from FTC guidance.³³

ESA requests that the Attorney General permit businesses to repurpose their existing verifiable parental consent processes under COPPA by, for example, expanding this process to include offline data that is sold for CCPA purposes. More specifically, the Attorney General should clarify the Proposed Regulations to align the permitted parental consent mechanisms under the CCPA with parental consent methods permitted under COPPA by making the following changes to Section 999.330(a):

(1) A business that has actual knowledge that it ~~collects or maintains~~ *sells* the personal information of children under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. ~~This affirmative authorization is in addition to any~~ *The business may utilize the same procedures used to obtain the* verifiable parental consent required under the Children’s Online Privacy Protection Act, 15 U.S.C. sections 6501, *et seq.; provided, however, that such consent is appropriately scoped to cover the sale of any personal information the business collects (whether online or offline).*

(2) Methods that are reasonably calculated to ensure that the person providing consent is the child’s parent or guardian include, *but are not limited to*:

- a. Providing a consent form to be signed by the parent or guardian ~~under penalty of perjury~~ and returned to the business by postal mail, facsimile, or electronic scan;
...
- C. *Consumers should not be required to go through an unduly burdensome two-step process in order to exercise their opt-in choice.*

Section 999.316(a) requires all consumers who wish to opt in to sales to undergo a two-step process through which they submit a request to opt in to the sale of personal information and then submit a subsequent confirmation of that request.

The CCPA was built on the recognition that “California consumers should be able to exercise control over their personal information.” Requiring consumers to confirm their request to exercise a CCPA right detracts from that goal by introducing unnecessary steps that may unduly discourage the consumer from completing his or her request.

Additionally, the stated policy concerns underlying the two-step requirement for opt-in consent (including for minors between the ages of 13 and 16) are already addressed through the statute. The ISOR suggests that the new two-step requirement for opt-in requests is needed to

³³ For example, the first mechanism listed in the Proposed Regulations would require that a parent or legal guardian sign and return a consent form “under penalty of perjury,” which is not required under COPPA. Compare Proposed Regulations, § 999.330(a)(2)(a), with 16 C.F.R. § 312.5(b)(i).

give “consumers the opportunity to correct an accidental choice to opt back into the sale of their personal information,” and to provide “businesses additional assurance that the consumer has made a clear choice to exercise their right to opt-in.” ISOR at 26. However, there is no evidence that opt-in requests are likely to be “accidental” and consumers, of course, retain the ability to opt out again at any time if their opt-in request was a mistake.³⁴ Requiring a double opt-in is especially disproportionate given that opt-out requests need not be verified. This discrepancy is likely only to confuse and frustrate the consumer.

Consequently, the double opt-in requirement should be removed from Section 999.316(a) and from the definition of “affirmative authorization” for consumers 13 years old and older. If the Attorney General rejects this request and retains the double opt-in requirement, then the regulations should at minimum similarly require the consumer to confirm his or her opt out request (i.e., double opt-out) before the business is required to comply with the request.

D. Requiring businesses to treat unverified deletion requests as opt-out requests diminishes consumer choice and creates practical challenges.

The Proposed Regulations introduce a new requirement that businesses must treat deletion requests that they cannot verify as requests to opt out of sales.³⁵ This requirement is not necessary to further any purpose of the CCPA. To the contrary, Section 999.313(d)(1) meaningfully *diminishes* the consumers’ ability to control his or her own information.³⁶ The fact that a consumer chooses to submit only a deletion request and not also simultaneously opt out is significant, and is strong evidence that the consumer affirmatively chooses *not* to exercise the opt-out right.

Moreover, automatically converting the deletion request into an opt-out request does not provide the consumer any additional benefit. A business that denies the deletion request already must inform the consumer that the request is denied, at which point the consumer would be free to choose to submit a request to opt out of the sale of the information if she so desired.

Finally, this requirement may prove unworkable in practice. Consistent with the Proposed Regulations, a business may have one method for consumers to submit requests to delete data that requires a certain subset of the data the business maintains about the consumer, so the business can match the data provided with the particular requesting individual.³⁷ In contrast, the business may use a different mechanism for consumers to submit opt out of sales requests. If the two mechanisms used are different and collect different types of information (e.g., a webform request and user-enabled privacy settings), it might not be possible to convert the deletion request into an actionable opt-out request based on the data available to the business.

³⁴ Cal. Civ. Code § 1798.120.

³⁵ Proposed Regulations, § 999.313(d)(1).

³⁶ CCPA §§ 1798.105(b), 1798.120(b); Proposed Regulations §§ 999.306, 999.308.

³⁷ Proposed Regulations, § 999.323(b)(1).

For these reasons, ESA requests that the Attorney General strike Section 999.313(d)(1) from the final regulations.

E. Requiring businesses to pass through opt-out requests inadvertently would undermine consumer choice.

The Proposed Regulations require a business that receives an opt-out request not only to stop selling that consumer's personal information, but also to communicate that consumer's request to any third party to whom the business sold that consumer's data in the prior 90 days.³⁸ This new requirement does not advance any statutory purpose and, to the contrary, undermines consumers' ability to freely exercise control over their personal information.

This new requirement is unnecessary, because the statute already requires consumers to receive explicit notice before a third party may resell personal information.³⁹ This provision enables consumers to effectively exercise their opt out of sale rights with respect to the entire universe of parties who sell their data.

The new requirement also could have the unintended consequence of undermining the consumer's preferred choices. For example, a consumer may desire to terminate her relationship with video game publisher X, who may disclose personal information to third party Y to provide certain game services across a number of different video games. If the consumer continues to play a different game published by video game publisher Z, who also discloses the consumer's personal information to third party Y, then Y might be unable to continue to provide the game services when the consumer plays publisher Z's game title due to the opt-out request that it received in connection with publisher X's game. This might surprise and frustrate the consumer, who believed her opt-out request would apply only to publisher X.

In addition to creating consumer confusion, adding a new pass-through obligation for "sale" opt outs would be inconsistent with the statutory text and longstanding canons of statutory interpretation. The CCPA contains a single pass-through obligation, requiring businesses to pass deletion requests on to service providers.⁴⁰ The California Supreme Court has held that "the expression of some things in a statute necessarily means the exclusion of other things not expressed."⁴¹ Consequently, the inclusion of the deletion pass through means the exclusion of the pass-through requirement in the opt-out right must be given effect.

³⁸ Proposed Regulations, § 999.315(f).

³⁹ Section 999.305(d) of the Proposed Regulations requires companies that collect a consumer's data, but do not collect the data directly from the consumer, to (1) notify the consumer of that business's sale of their data, or (2) obtain a signed attestation from the source of the data that the source gave the consumer the relevant notice and obtain a copy of that notice. Both of these options are unlikely to be workable given the number of intermediaries that can be involved in a particular product or service offering. Instead, ESA encourages the Attorney General to permit the third party to obtain a broad confirmation by consumer type and contractual commitments that the source of the data has the right to share the personal information.

⁴⁰ Cal. Civ. Code § 1798.105(d).

⁴¹ *Gikas v. Zolin*, 6 Cal. 4th 841, 852, 863 P.2d 745, 752 (1993).

For these reasons, ESA asks the Attorney General to remove Section 999.315(f) from the final regulations.

* * *

ESA appreciates the Attorney General's consideration of these comments, and we hope to continue working with the Attorney General and his staff on these critically important issues.

Sincerely,

A handwritten signature in black ink that reads "Gina Vetere". The signature is written in a cursive, flowing style.

Gina Vetere
Senior Vice President & General Counsel
Entertainment Software Association

Message

From: Robert Rutkowski [REDACTED]
Sent: 12/6/2019 12:47:22 PM
To: Xavier Becerra [Xavier.Becerra@doj.ca.gov]
Subject: Strengthen California's Consumer Data Privacy Regulations

Xavier Becerra, Attorney General
Attorney General's Office
California Department of Justice
Attn: Public Inquiry Unit
P.O. Box 944255
1300 I Street, Suite 1740
Sacramento, CA 94244-2550
xavier.becerra@doj.ca.gov
Phone: 916-445-9555 Fax: 916-323-5341

Re: Strengthen California's Consumer Data Privacy Regulations

Dear Attorney General:

A coalition of privacy advocates have filed comments seeking strong regulations to protect consumer data privacy. The draft regulations are a good step forward, but the final regulations should go further.

The California Consumer Privacy Act of 2018 (CCPA) created new ways for the state's residents to protect themselves from corporations that invade their privacy by harvesting and monetizing their personal information. Specifically, CCPA gives each Californian the right to know exactly what pieces of personal information a company has collected about them; the right to delete that information; and the right to opt-out of the sale of that information. CCPA is a good start, but they want more privacy protection from the California Legislature.

CCPA also requires the California Attorney General to adopt regulations by July 2020 to further the law's purposes. In March 2019, EFF submitted comments with suggestions for CCPA regulations. In October 2019, you published draft regulations and again invited public comment.

In the new comments, the coalition wrote:

The undersigned group of privacy and consumer-advocacy organizations thank the Office of the Attorney General for its work on the proposed California Consumer Privacy Act regulations. The draft regulations bring a measure of clarity and practical guidance to the CCPA's provisions entitling consumers to access, delete, and opt-out of the sale of their personal information. The draft regulations overall represent a step forward for consumer privacy, but some specific draft regulations are bad for consumers and should be eliminated. Others require revision.

The coalition made dozens of suggestions. Noted are two here.

First, to implement CCPA's right to opt-out of the sale of one's personal information, the draft regulations at Section 315(c) would require online businesses to comply with user-enabled privacy controls, such as browser plugins, that signal a consumer's choice to opt-out of such sales. EFF suggested such an approach in the March 2019 comments. The coalition comments now seek a clarification to this draft regulation: that "do not track" browser headers, which thousands of Californians have already adopted, are among the kinds of signals that online businesses must treat as an opt-out from data sale.

Second, the coalition urges issuing clarifying regulations that bar misguided efforts announced by some members of the adtech industry to evade CCPA's right to opt-out of sales. Adtech is one of the greatest threats to consumer data privacy, as explained in a new EFF report on third-party tracking. The broad dissemination of personal information

throughout the adtech ecology is a form of “sale” plainly subject to CCPA’s right to opt-out. Regulations should now lay to rest the crabbed arguments to the contrary.

Yours sincerely,
Robert E. Rutkowski

cc:

Representative Steny Hoyer
House Majority Leader
Legislative Correspondence Team
1705 Longworth House Office Building
Washington DC 20515
Office: (202) 225-4131
Fax: (202) 225-4300
https://urldefense.proofpoint.com/v2/url?u=https-3A__www.majorityleader.gov_content_email-2Dwhip&d=DwIDaQ&c=uASjV29gZuJt5_5J5CPRuQ&r=pjnDzEEbcy-Gofg9cc8KuOxxQt4kIkqvQtb6_GugvPg&m=vfjxB1lqKP2PsUtb7VcJUnCKomUMok1LFM_QlJMBD9s&s=pt3Ppo81ebYb2hzOgBYMrQZAWNfs_ilvmpmdQropjKY&e=



Re: Comments:

https://urldefense.proofpoint.com/v2/url?u=https-3A__www.eff.org_document_2019-2D12-2D06-2Dprivacy-2Dcoalition-2Dcomments-2Dre-2Dcag-2Ddraft-2Dccpa-2Dregspdf-2D0&d=DwIDaQ&c=uASjV29gZuJt5_5J5CPRuQ&r=pjnDzEEbcy-Gofg9cc8KuOxxQt4kIkqvQtb6_GugvPg&m=vfjxB1lqKP2PsUtb7VcJUnCKomUMok1LFM_QlJMBD9s&s=sj7gzn0FBst3D2cG41RqEsbghectnC5EsMmJl_p1A&e=

Message

From: Friel, Alan L. [REDACTED]
Sent: 12/6/2019 7:18:51 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]; Sweeney, Margaret [REDACTED]
Subject: RE: Proposed Regulations Implementing the California Consumer Privacy Act
Attachments: 20191206191224441.pdf

Thank you for your reply. Please kindly discard our submission of 5:14 pm and replace it with the attached. The prior submission was inadvertently sent and is version 4 of the document. This is the final version 5, as indicated in the document footer number on each page after the cover page.

Best regards,

Alan L. Friel | Partner | **BakerHostetler**

11601 Wilshire Blvd. | Suite 1400
Los Angeles, CA 90025-0509
[REDACTED] F +1.310.820.8859

600 Anton Blvd. | Suite 900
Costa Mesa, CA 92626-7221
[REDACTED] F +1.714.754.6611

[REDACTED]
bakerlaw.com



From: Privacy Regulations <PrivacyRegulations@doj.ca.gov>
Sent: Friday, December 6, 2019 5:20 PM
To: Sweeney, Margaret [REDACTED]
Cc: Friel, Alan L. [REDACTED]
Subject: RE: Proposed Regulations Implementing the California Consumer Privacy Act

Thank you for submitting a public comment on the CCPA proposed regulations. Your email has been received.

Sincerely,
California Department of Justice

From: Sweeney, Margaret [REDACTED]
Sent: Friday, December 06, 2019 5:14 PM
To: Privacy Regulations <PrivacyRegulations@doj.ca.gov>
Cc: Friel, Alan L. [REDACTED]
Subject: Proposed Regulations Implementing the California Consumer Privacy Act

Good Afternoon,


On behalf of Baker Hostetler please see attached letter.

Thank you

Margaret Sweeney
Legal Secretary

BakerHostetler

11601 Wilshire Boulevard | Suite 1400
Los Angeles, CA 90025-0509


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.

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.

BakerHostetler

Baker & Hostetler LLP

11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509
T 310.820.8800
F 310.820.8859
www.bakerlaw.com

Alan L. Friel

December 6, 2019

VIA E-MAIL (PrivacyRegulations@doj.ca.gov)

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: Proposed Regulations Implementing the California Consumer Privacy Act

Dear Privacy Regulations Coordinator:

BakerHostetler, one of the nation's largest law firms, represents clients around the globe. With offices coast to coast, three of which are in California, our nearly 1,000 attorneys counsel businesses of all sizes and in all industries. For the last year our highly ranked and awarded, 70+ member, Privacy and Data Protection practice has been counseling clients on how to interpret, and prepare for the effectiveness of, the California Consumer Privacy Protection Act ("CCPA" or "Title"). These comments are an aggregation of comments that some of our clients have asked us to submit to you. They do not reflect the position of all of our clients, or of the firm itself. However, we believe that the issues noted are ones ripe for further change or clarification, and within the authority of Attorney General to adopt. Accordingly, we respectfully submit the following for your consideration:

I. Safe Harbors

- **The enforcement delay under Section .185(c) of the Title should be a safe harbor period for any business that is making good faith efforts to come into compliance by the end of that period, and having done so should be deemed a cure under Section .155(b) of the Title.**

The delay in the issuance of a first set of proposed regulations has created an undue burden on businesses. The lack of clarity on issues such as the meaning and scope of terms and how to give requisite notice, verify consumers and fulfill their rights left business with little to do

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

until recently other than inventory their data and develop general compliance programs. It is clear that the Title will become effective before the regulations are final. The rush to try to implement details even based on the October 2019 first draft regulations has left businesses and their advisors with too much to accomplish in too little time, and many companies are already, or will soon be, in code lock. Mobile apps cannot be revised without submitting a new update to Google or Android for approval. As of today, the regulation on the “Do Not Sell” button has not even been proposed for consideration.

Further, many vexing questions remain unanswered by the first draft of the regulations, and those draft regulations (“Regs”) provide, for many unexpected and difficult to implement compliance obligations. It will take considerable time for even companies that have staffed entire teams to work full-time for the last year or more to prepare to do what will be ultimately necessary to launch a fully compliant program.

- **A good faith belief that a business is in compliance, where that conclusion is not expressly contradicted by the Title or the final regulations, should be a complete defense to non-compliance, if the business commits to cure upon being instructed by the AG that its position is mistaken.**

The proposed regulations leave much unanswered and there is sparse legislative history to guide interpretation of the Title. Further, the Title is in many ways ambiguous and subject to entirely reasonable, but conflicting, interpretations simultaneously. The right to cure in Section .155(b) of the Title should be a real and meaningful right to prospectively cure.

- **A Business should not be liable for providing personal information to a person who is not the consumer in response to a consumer request if it can show that it met the verification standards set forth in the final regulations and/or a business should be provided ultimate discretion to determine that it cannot sufficiently verify a Consumer when specific pieces of personal information are requested.**

Article 4 of the Regs reflect the principle that security is paramount to consumer access to specific pieces. This approach should be further incented by providing a safe harbor for a business declining to provide specific pieces in a good faith attempt to protect the security of the applicable consumer.

II. Requirements Relating to Offline Collection.

The Regs place significant, and sometimes impossible, burdens on retail businesses and other businesses that substantially interact with consumers offline.

- Offline Notices.
 - **The AG should revise the Regs to state that the notices required by Sections .305(a)(2)(e) (notice at collection) and .306(b)(2) (notice of the right to opt-out) can be satisfied by providing a single link to the business' California-specific privacy notice, or the California-specific section of a business' privacy notice, in the offline methods currently permitted in the Regs.**
 - The regulations currently arguably require businesses that collect personal information offline to post two additional, separate notices, in addition to the numerous notices that are already presented to individuals who visit retail and other offline business locations in California (e.g., Prop 65 and many others) – the notice at collection pursuant to Section 999.305(a)(2)(e) and the notice of the right to opt-out pursuant to Section 999.305(b)(3) and .306(b)(2).
 - Because of the foregoing, and for the additional reasons discussed below, the AG should clarify that both the Notice of Collection and the Notice of the Right to Opt-Out may be given by providing a link to the business' California-specific privacy notice or the California-specific section of a business' privacy notice in the offline methods currently permitted in the regulations¹.
 - Consumers will be confused and misled if presented with more specific information regarding their right to opt out of sales of personal information. Most retailers do not sell information in the colloquial sense, and especially not information collected in person at a retail location. Presenting the Notice of the Right to Opt-Out and explaining that a business sells information, such as only in the context of interest-based advertising (in the event that is ultimately determined to be a sale, which remains far from clear), will only confuse and mislead a consumer. This is, in part, because to the extent that retailers and other offline businesses do sell as defined in the CCPA, such sales are often limited to their online retailers' activities (though that is currently not settled in the digital advertising industry). Explaining this in the context of an in-person notice in a clear and concise manner in a way that the average consumer will actually read and understand is an impossible task and will not further the purposes of the CCPA.
 - Multiple or complex notices are contrary to the principle of simplicity and understandability that are woven elsewhere throughout the Regs.

¹ Section 999.305(a)(2)(e) states that businesses “may, for example, include the [Notice at Collection] on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to the web address where the notice can be found.” Section 999.306(b)(2) allows the Notice of the Right to Opt-Out to be given on methods that “include, but are not limited to, printing the notice on paper forms that collect personal information, providing the consumer with a paper version of the notice, and posting signage directing consumers to a website where the notice can be found.”

- Handling Offline Consumer Requests.
 - The AG should revise the Regs to clarify that there is no requirement that businesses must accept paper forms submitted in person for consumer requests, and allow for businesses to merely ensure that in-store inquiries are directed to a way to submit the inquiry, such as by pointing consumers to the business' privacy policy, where the information can be found, or to a 1-800 number program.²
 - The Regs require that retail businesses offer at least three methods to submit requests to know: a toll-free telephone number, an interactive webform accessible through the business's website, and an in-store method, an example of which is said to be a form that can be submitted in person at the retail location. See Section 999.312(a).
 - Requiring businesses to allow consumers to submit a form in person at a retail location detracts from the purposes of the CCPA and also presents a litany of operational issues for businesses.
 - Personal information, such as name, email and phone number, submitted on a form could be exposed to any number of retail employees where the form was submitted. On the other hand, a request via email, phone call or on an interactive webform may be made in the privacy of the consumer's use of a computer or phone.
 - Businesses cannot feasibly verify the identity of an individual at a retail location for a variety of reasons. Therefore, although the in-person receipt of requests should not be required as discussed above, if the AG does require businesses to do so, the regulations should specify that the businesses' submission of a form in person does not require in person verification.
 - It is not clear how a retail location would verify identity in-person anyway. In the practice of privacy-by-design, point of sale systems do not (and should not) have access to information that would allow businesses to verify. Alternatives like check multiple IDs is overly intrusive.
 - Businesses will have to rely on retail-level employees, often part-time or actually employees of a franchisee and not the brand, to distribute and intake the forms and see to it that they are sent to the corporate office location where the process will be carried out. These personnel are not appropriately equipped to perform such tasks.

² As discussed above, this information already must be posted on prominent signage.

- As a result, the submission of forms in-person will require more communication, risk of data loss or seepage, and follow-up from both the consumer and the business than would otherwise occur in an electronic (e.g., email or interactive webform context) or oral (phone) context, and would detract from privacy and thus the purposes of the CCPA.
- Training Employees in Retail/Hospitality/Other Offline Collection Settings.
 - **The AG should include a provision in the Regs that Section 999.312(f) does not apply to a business' retail-level and similar employees.**
 - Due to the requirement that a business must assist a consumer who has provided a deficient request pursuant to Section 999.312(f)³ and Section 999.317(a)⁴ (i.e., that all individuals responsible for handling consumer inquiries must be informed “how to direct consumers to exercise their rights”), all retail-level employees must be trained on how to direct a consumer to exercise their CCPA rights. This is not realistic.

III. Consumer Requests

- **The AG should revise Section 999.312(a) of the Regs to state that a business that operates exclusively online, and has a direct relationship with a consumer from whom it collects personal information, shall only be required to provide an email address for submitting requests to know.**
- This is consistent with the amendments from Assembly Bill 25, which was signed into law on October 11, 2019 as Section .130(a)(1)(A) of the Title.

IV. Notice at Collection

- **The AG should revise Section 999.305 of the Regs to state that the notice at collection to be given to parties who are subject to the exemption in CA Civ. Code §1798.140(h)(1)⁵ (i.e., job applicants, employees, owners, directors, officers, medical staff members, or contractors of a business) need not include a link to the business' privacy policy as required in Section 999.305(b)(4) of the Regs.**

³ “If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either: (1) Treat the request as if it had been submitted in accordance with the business’s designated manner, or (2) Provide the consumer with specific directions on how to submit the request or remedy any deficiencies with the request, if applicable.”

⁴ “All individuals responsible for handling consumer inquiries about the business’s privacy practices or the business’s compliance with the CCPA shall be informed of all the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.”

⁵ As included in Assembly Bill 25, signed into law on October 11, 2019.

- This is consistent with the amendments from Assembly Bill 25, which was signed into law on October 11, 2019 as Section .140(n)(1)(excluding HR data for one year), because the full privacy notice will no longer include this type of HR data.

V. Scope of regulatory coverage.

- **The Regs should clarify that CCPA rights only apply to California consumers, and that a business may decline to provide CCPA rights where it cannot reasonably verify residency.**
 - In multiple contexts, the Regs arguably do not allow businesses, service providers, and third parties to limit the application of the CCPA to only personal information of California consumers. Similarly, in some contexts the Regs appear to confer rights under the CCPA upon individuals regardless of their status as a California Consumer. The AG must provide a regulatory scheme which provides obligations on businesses, service providers, and third parties relating only to personal information of California consumers, and corresponding rights to only California consumers.
 - The AG should state in the Regs that “reasonable steps” as set forth in CA Civ. Code §1798.135(b) include, but are not limited to, detecting and utilizing internet protocol (IP) address to determine a person’s status as a California consumer.
 - The AG should state in the Regs that businesses, service providers, and third parties are permitted take the “reasonable steps” referred to in Section .135(b) of the Title to determine a person’s status as a California consumer in contexts outside of those set forth in Section .135(b), including, without limitation, a business’ verification of identity.
 - Section .135(b) states: “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.*” An example of “reasonable steps” would be to detect the IP address of a website visitor and to make a decision to direct them to the California-specific homepage based on the detection. It is otherwise unclear how a business would detect that someone visiting a website is, in fact, a California consumer visitor to the website.

- In other online contexts, such as digital advertising, businesses, service providers, and third parties will have to make decisions whether and how to afford rights to a visitor to a website, mobile application, or online service. Often the only information the website publisher and advertising vendors providing the publisher services have on visitors is IP address and information collected by cookies and other tracking technologies. The only feasible way of understanding if such visitor should be afforded the rights of a California consumer is to understand the location of such visitor.
- **Accordingly IP address lookup, reference to address on file and other reasonable methods of establishing location should be deemed reasonable methods to verify that a consumer is a California consumer, and nothing more exacting should be required. However, if a business wants to require more exacting residency verification, it should be free to be able to do so.**
 - In the context where a business is interacting with a consumer online, the AG should clarify that the “reasonable steps” a business may take pursuant to CA. Civ. Code §1798.135(a)(6) may also be taken by businesses in the context of verification.

VI. Service Providers

- **The AG should revise Section 999.314 of the Regs to state that a service provider shall retain its status as a service provider so long as the purposes for which it is permitted to process personal information under the contract with the business meets the definition of “business purpose” under CA Civ. Code § 1798.140(d).**
 - Section 999.314(c), as currently written, provides a bright line as to the permissible purposes for which a service provider can process personal information. In view of the balancing test provided in the statute, this bright line is not necessary, conflicts with the plain statutory language and misses the reality of the provision of services by vendors, in which virtually all vendors that process personal information do so for their own business purposes, frequently for the benefit of all of their customers, and not to the detriment of consumers.
 - Section 999.314(c) of the Regs puts businesses and service providers alike in an impossible position to comply with the statute. Section 314(c) as currently written would prevent service providers from carrying out routine operational activities (i.e., business purposes), including, but not limited to:
 - Deidentifying and aggregating personal information, which is necessary to use deidentified and aggregate personal information in the first place (e.g., the use of which is provided for in the vast majority of services agreements between vendors and customers, and which notably allows for

- data minimization and furtherance of privacy and security of such information);
- Appointing subcontractors (e.g. sub-service providers);
- Disclosing information to comply with law, or complying with a legal inquiry, investigation, subpoena or similar from authorities (See CA Civ. Code Section 1798.145(a), which only affords exceptions like these to businesses and not service providers or third parties).
- In addition to the seven enumerated business purposes in CA Civ. Code §1798.140(d)(1)-(7), the definition of business purpose allows for “operational purposes, or other notified purposes.” Businesses should be free to direct their service providers to process for such purposes, and in particular the “other notified purposes” – which necessarily entails that the business has notified consumers of such purposes. This could include appointment of subcontractors and compliance with law and legal process or other specific disclosures not inconsistent with the collection purpose since the purposes are notified.
- Because of Section .314(c) of the Regs, the moment that the regulations are promulgated, service providers providing services under existing contracts will immediately be in violation of the CCPA and businesses will immediately be shed of the immunity afforded to them under CA Civ. Code §1798.140(k). “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.” This is because by continuing to provide services and process personal information for purposes which are not permitted, the service provider would be in violation of the CCPA, and businesses would have actual knowledge, because of the permissions granted in a contract with the service provider, “that the service provider intends to commit such a violation.” While it is unclear what the liability would be for such violation by the service provider, what is clear is that innumerable businesses would immediately lose immunity afforded to it by CA Civ. Code §1798.140(k) because of §999.314(c) of the Regs.
- The Statement of Reasons in connection with the Regs indicate that the AG’s reason for drawing the bright line of limited permitted service provider business purposes was to prevent business purposes from bleeding into commercial purposes. This confuses the distinction between the definition of business purposes and commercial purposes. If the test in the definition of business purpose, in Section .140 (d) of the Title, that the “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 arose that is compatible with the context in which the personal information was collected” is met, then the purpose is by that measure a business

and not a commercial purpose. The Regs propose to upend that statutory distinction between the two definitions by rewriting the CCPA with a bright line the legislature did not draw, and in doing so would eviscerate the test the law requires be applied to establish what purposes qualify as a business' or a service provider's business purposes.

VII. Financial Incentive and Non-Discrimination

- The Regs should establish that “Loyalty program benefits are reasonably related to the value of a consumer’s data to the business offering the program arising out of the business’ use and disclosure of that personal information as set forth in the program terms, as a condition of ongoing loyalty program participation, if the terms and benefits of the loyalty program, and the scope of the business’ potential use and disclosure of the personal information, and any related waivers of consumer rights under the Title, are clearly stated in the program terms, the consumer affirmatively accepts the program terms and the consumer can prospectively withdraw from the program and upon doing so prospectively regain the consumer's full rights under the Title regarding that personal information (including right to know, right to delete and opt-out).”
- The Regs impose restrictions on any “financial incentive,” the definition of which hinges on the collection of personal information.
- Loyalty programs by their nature are financial incentives that require personal information.
- Many consumers want to keep their loyalty programs, which are entirely voluntary in nature.
- As part of a loyalty program, consumers choose to give their information to a company so that it can provide them with certain benefits, including marketing, sometimes from third parties.
- Under the Regs, a “financial incentive” is not only subject to various regulatory requirements, but it is prohibited outright.
- An exception to this prohibition is if the value received by a consumer from the financial incentive is reasonably related to the value to the business of the of the consumer’s data. The Regs enumerate eight methods for determining the value of a consumer’s data. This presents several issues.
 - Most significantly, the language is unclear and confusing.
 - This confusion creates a high regulatory burden for a company simply to determine if it qualifies for the exception.
 - Additionally, while the complicated nature of the law makes compliance difficult, there are many methods by which a company can calculate the value of consumers’ data in order to fit within the exception.
 - The practical effect is that if a company spends enough money on its calculations, then, and only then, can it offer a loyalty program.

- These compliance costs do not work to protect consumers' data, instead it is spent manipulating a company's data in myriad ways until it fits one of the prescribed methods.
 - The Regs thereby create a barrier to entry for offering loyalty programs that excludes smaller businesses and generally adds unnecessary costs.
- In reality, a bargained for exchange occurs when a consumer knowingly accepts loyalty program benefits in exchange for providing a business certain specified uses of the consumer's data. That fully-informed, free market exchange is, alone, an adequate measure of the value to each party. There is no need for any more complex analysis.

VIII. Business-to-Business Exception

- **The Regs should clarify that the Do Not Sell Right does not apply to personal information covered by Section .145(n)(1) of the Title.**
- Assembly Bill 1135, which was signed by the Governor on October 11, 2019, adds Section .145(n)(1) to the Title to exempt, for one year, certain business-to-business communications data, from Sections .100, .105, .110, .115, .130 and .135 of the Title.
- Not specifically excepted are Sections .120 or .125 of the Title, which at first blush suggests that the Do Not Sell opt-out rights and non-discrimination rights are not included in the exclusion.
- However, a more careful reading indicates that the inclusion of Sections .100, .105, .110, .115, .130 and .135 of the Title as excluded is sufficient to exclude Sections .120 and .125 without the need to name them, because:
 - Section .135, which is where a business' obligations corresponding to .120 exist, is excluded and without Section .135 Section .120 is rendered is meaningless.
 - And, as to Section .125, with all the consumer rights provisions excluded what would be left that the exercise or non-exercise of which could be the basis for discrimination? Nothing.

Thus, the AG should clarify that .120 and .125 do not apply given that the exclusion of the rest of the consumer privacy rights makes them moot.

Thank you for your consideration of these comments.

Respectfully submitted,



BAKER & HOSTETLER, LLP

**Statement of the Association of National Advertisers
(ANA) to the California Attorney General on the
Proposed Regulations Implementing the California
Consumer Privacy Act**

*San Francisco, CA
December 4, 2019*

Good morning/afternoon and thank you for the opportunity to provide comments regarding the content of the proposed regulations implementing the California Consumer Privacy Act. My name is Dan Jaffe, and I am the Group Executive Vice President of Government Relations at the Association of National Advertisers -- the "ANA."

The ANA's mission is to drive growth for marketing professionals, for brands and businesses, and for the industry. Growth is foundational for all participants in the ecosystem. ANA protects the legitimate First Amendment rights of advertisers to effectively reach consumers and support a competitive and fair marketplace. The ANA's membership consists of more than 1,600 domestic and international companies, including more than 1,000 client-side marketers and nonprofit fundraisers and 600 marketing solutions providers (data science and technology companies, ad agencies, publishers, media companies, suppliers, and

vendors). Collectively, ANA member companies represent 20,000 brands, engage 50,000 industry professionals, and invest more than \$400 billion in marketing and advertising annually. The vast majority of them are either headquartered or do substantial business in California.

Because the ANA strongly supports the importance of protecting consumer privacy, our members have long had in place vigorous codes of conduct and self-regulatory programs that permit consumers to control access to and use of their information.

The CCPA represents a highly complex and in many respects ambiguous law, and without final rules to sufficiently clarify its terms in advance of its effective date, the CCPA will prove to be extremely disruptive to consumers and business alike. ANA strongly urges you to work diligently to reduce the economic and general burdens of the CCPA while maintaining protections for consumers. It is simply impractical and unfair to raise consumers' expectations about their rights and to require businesses to comply with obligations that are still unknown.

We recognize that the proposed regulations to implement the CCPA are well-intentioned, but we are very concerned that they will not effectuate the law's stated

goals. In some cases, they do not reflect the CCPA's language and scope as enacted by the Legislature; they also could decrease consumer choice and privacy rather than advance it; and they will dramatically impact the cost of doing business.

We believe they will:

1. limit important programs and services that California consumers now enjoy and expect;
2. place requirements on businesses that will ultimately substantially restrict rather than enhance consumer choice and control; and
3. impose significant costs and burdens on the California economy, as evidenced by the estimated up to 16.454 billion dollar cost of the regulations over the next ten years set forth in the Standardized Regulatory Impact Assessment on the CCPA published by your office.

We urge that the proposed regulations be improved in a number of ways, and we will be submitting more extensive suggestions on these improvements shortly. But today we highlight three important issues regarding:

1. loyalty programs;

2. browser signals that communicate opt-out choices;
and

3. requiring businesses to pass opt-outs to third parties.

First, Section 999.336 of the proposed regulations repeats the statutory language that a business may offer financial incentive or a price or service difference to a consumer if the difference is reasonably related to “the value provided to the business by the consumer’s data.” If a business offers such an incentive, Section 999.307 requires the business to provide a notice of the incentive that lists a good-faith estimate of the value of the consumer’s data and a description of the method the business used to calculate the value of the consumer’s data. This provision will significantly impact numerous loyalty programs with which we are all familiar, such as gas dollar programs, frequent flyer programs, or grocery “valued customer” rewards.

Consumers provide data to participate in loyalty programs because they obtain major value through lower prices and special offers. In order to provide this value to consumers, loyalty programs depend on data; but deletion or opt-out requests restrict that data. The proposed regulations’ requirement regarding the relationship of the value received from data to the price or service difference offered to consumers could well create requirements that many businesses cannot meet, thereby prohibiting

businesses from offering these rewards programs that consumers enjoy and expect. And the proposed regulations' directive to provide an estimate of the value of that data and a description of the method used to calculate such value is unworkable and risks exposing businesses' proprietary processes and confidential information to the public. Although the proposed regulations provide certain acceptable methods for calculating the value of data, it will be difficult for a business to calculate the value of such data on an individual consumer basis rather than an aggregate consumer value, making these calculations complex.

Making disclosures about the value of data therefore could confuse consumers rather than provide helpful transparency into business practices. Loyalty programs should not be jeopardized because unreasonable burdens are imposed due to some consumers choosing to exercise their CCPA rights.

Harming loyalty programs valued by consumers could well undermine their confidence in privacy protection in general and impose additional costs on them.

Accordingly, the ANA urges that the regulations clarify sufficiently how a business may justify that a price or service difference is reasonably related to “the value provided to the business by the consumer’s data” and remove the requirement to provide an estimate of the

value and the method of calculating such value in a notice so that consumers can continue to receive these loyalty programs that they appreciate and desire.

Second, Section 999.315(c) of the proposed regulations states that a business that collects personal information from consumers online must treat user-enabled privacy controls (such as a browser plug-in, privacy setting or other mechanism) that communicate or signal the consumer's choice to opt out of the sale of their personal information as a valid request submitted for that browser or device, or -- if known -- for the consumer. This mandate will harm consumers, as it could be interpreted to remove their ability to set granular preferences and choose which businesses can and cannot sell personal information. This would deprive consumers of the opportunity to exercise meaningful choices and make business-by-business decisions about different entities that may transfer or use data. A consumer very well may want to restrict a specific business's ability to sell personal information -- say, a car dealership -- but allow another, different business -- for example, a grocery store -- to transfer or sell personal information. The overly broad requirement to honor browser settings on an across-the-board basis would destroy this ability to make granular choices based on individual preferences, since they would apply across the

entire marketplace. Furthermore, this requirement goes far beyond the scope of the CCPA because this new business duty is not included in the statute. Therefore, at the least, this requirement should be removed or the proposed rules should be revised so that a business engaged in the sale of personal information has the option either to honor browser plug-ins, privacy settings or mechanisms, or not be required to honor them if the business includes a “Do Not Sell My Info” link and offers another mechanism or protocol for consumers to opt out of the sale of personal information.

Third, Section 999.315(f) of the proposed regulations states that, upon receipt of an opt-out request, a business must notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the request that the consumer has exercised the right to opt out, and instruct such third parties not to further sell the information. This represents a significant new and sweeping requirement not contemplated by the CCPA’s language. The new requirement to pass opt-out requests along to a potentially broad range of other businesses would take the consumer’s expressed choice with respect to one business – like a retail holiday-themed store -- and apply that choice across the marketplace to others, such as those less seasonal in nature. If third parties act on opt-out requests

originally directed to just that business alone, consumers may lose access to other valued products, services, and content that they did not intend to limit. ANA therefore suggests that the proposed rules be revised so businesses are not required to pass opt-out requests along to third parties for when data has been provided in the last 90 days.

The proposed regulations run the risk of significantly reducing the use and value of consumer data, depriving consumers of benefits and advantages they currently receive. Consumers will certainly feel the effects of the regulations, which will raise the cost of doing business in California. And business operations should not be stymied or rendered ineffective because the “rules of the road” are not clear. We will be submitting detailed written comments shortly, setting forth more information about these and a number of other important concerns, and we look forward to working with you as the regulations to implement the CCPA are finalized.

Thank you for the opportunity to speak to you today.

ABOUT THE WITNESS

John William Templeton is a San Francisco-based newspaper, book and television publisher and producer with 45 years experience who has been in management for 40 years. An expert in the MDL Microsoft anti-trust case and Moore v. Lightstorm copyright infringement case, he is plaintiff in the anti-trust and trademark case Templeton v. Amazon, Google, Thriftbooks, et.al.

He has testified to the Senate and House Judiciary Committees, the House Energy and Commerce Committee and House Small Business Committee.

Author of the four-volume history of African-Americans in California in 1991 and curator of the first black history exhibit in the Historic State Capitol, he was editor of the *San Jose Business Journal* and director of employee communications for FMC Defense Systems Group before forming his own imprint in 1989.

In 2017, he was presented the Community Activist Award by the San Francisco branch of the NAACP. The California Black Chamber of Commerce presented the Visionary Award to him in 2016. KGO-7 awarded the Circle 7 Award in 2011 for his development of the 6,000 site California African-American Freedom Trail.

He has presented to the California Council for the Promotion of History, California Council for the Social Studies, Association for the Study of African-American Life and History, American Library Association, American Bar Association, American Educational Research Association and American Historical Association-Pacific Coast Branch.

A fourth generation Presbyterian ruling elder, he served as a Commissioner to the five-state Synod of the Pacific and was Overture Advocate to the 2018 General Assembly of the Presbyterian Church USA achieving a 485-9 vote in favor of a measure originated in the Presbytery of San Francisco.

Since 1995, he has published the online business newspaper blackmoney.com and published the *Journal of Black Innovation* scholarly scientific magazine.

ABSTRACT

Dear General Becerra and Staff,

The Honorable Malia Cohen, Chair of the State Board of Equalization and former President of the San Francisco Board of Supervisors and San Francisco Retirement System, described technology as the “civil rights issue of the 21st Century” during the 2017 Innovation and Equity: 50 Most Important African-Americans in Technology symposium.

She was joined by then-Treasurer John Chiang, who discussed how he used his authority to act against racial discrimination by Wells Fargo Bank by preventing state agencies from using the bank.

Reps. Zoe Lofgren and Anna Eshoo, Silicon Valley Democrats have taken the lead to introduce a national online privacy protection bill, based in large part on the California Online Privacy Protection Act and the European Union’s General Data Protection Protocol.

We face a moment similar to the first two decades of the 20th century. California became the hub of the most important communications technology of the century.

The earliest technical innovators of the nascent motion picture industry included African-Americans Noble Johnson, Oscar Micheaux and Benjamin Franklin Spikes.

But the industry became dominated by a movie which was so divisive that it sparked the creation of the National Association for the Advancement of Colored People.

That movie "Birth of a Nation" accelerated the Jim Crow period of American history, reversing the impact of the 14th and 15th Amendments until the 1950s.

Eighty years before, the advent of the cotton gin reversed the abolition timetable anticipated by the Founders with the 20 year delay in Congress' ability to ban the slave trade.

As Chair Cohen and Treasurer Chiang noted, the actions of public officials can have consequences for decades, most importantly locking in inequality.

In each of the past two centuries, African-Americans have had their quest for freedom reversed by technological changes supported by public policy.

The lesson of history is that technological change must be governed by the positive impact for those who have been excluded in the past.

As the subject matter expert on African-American history in the West and the abolition movement as well as the dean of Silicon Valley journalists, I see that lesson coming to fruition in the California Online Privacy Protection Act.

The most progressive civil rights act in American history, the Unruh Civil Rights Act, as amended since 1959, can be subverted, just as the 14th Amendment was by the movie industry,

As author of the authoritative history of the adoption of the 13th and 14th Amendments, the witness is able to insightfully observe the parallels in history for policy choices and failures in a similar time of political and economic upheaval.


He is further illuminated by the challenge of having to defend his own name from egregious violations of his California privacy rights, including the right of publicity, false advertising, phishing, unfair business practices and restraint of trade. Pursuing these matters has subjected him to retaliation, interference with religious practice, bullying and commercial disparagement.

john william templeton all things open

Web Images Videos News Settings


All Regions Safe Search: Moderate Any Time

Recent News



How liberals learned to love federalism

WP Washington P... 3h



Unexpected access: 18th-century Wren Building drain uncovered

VG Virginia Gazette 3d

McArthur delivers on space jam

R Robesonian 2h

→ More News

Are these links helpful? Yes No

John Templeton at Amazon AD

 Amazon.com  Report Ad

Buy John Templeton at Amazon! Free Shipping on Qualified Orders.

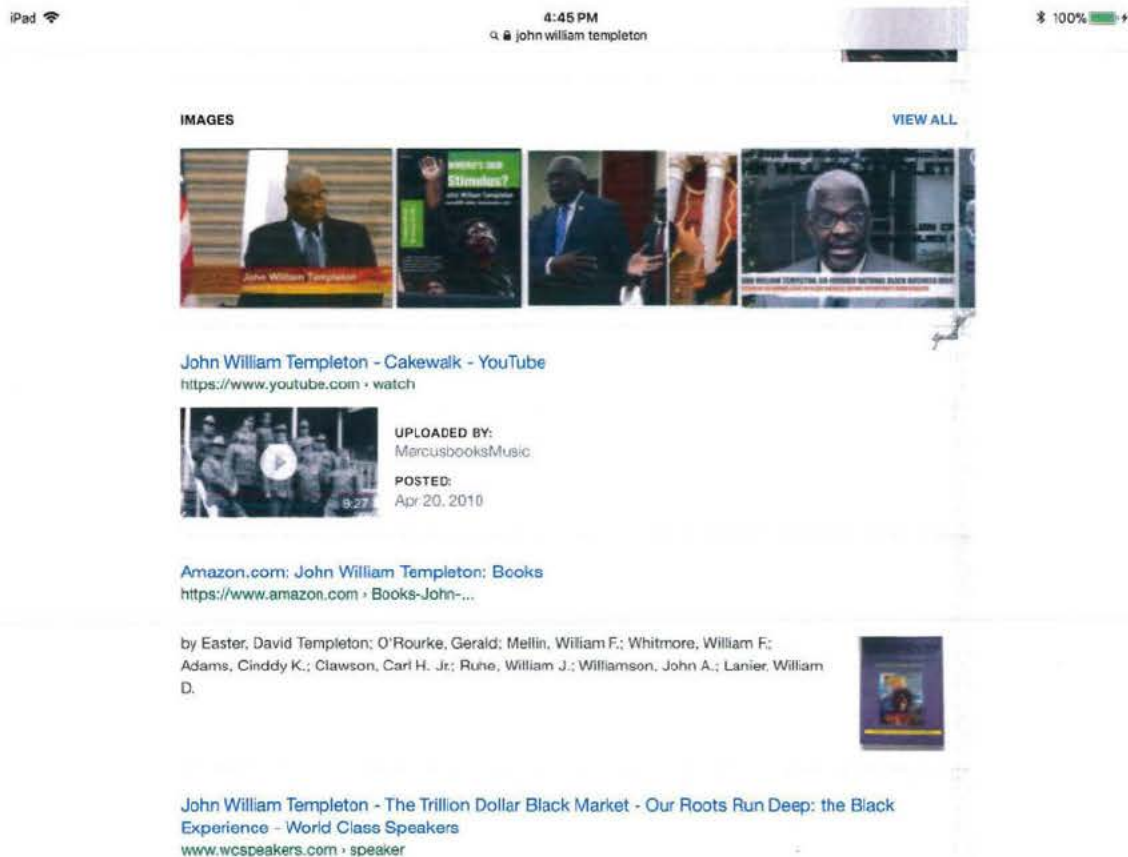
[Amazon Prime Benefits](#), [Shop Amazon Fire Tablets](#), [Explore Amazon Smart Home](#)

All Things Open 2015 | Keynote Panel hosted by Delisa ...

 <https://www.youtube.com/watch?v=HQRkgyArV5k>

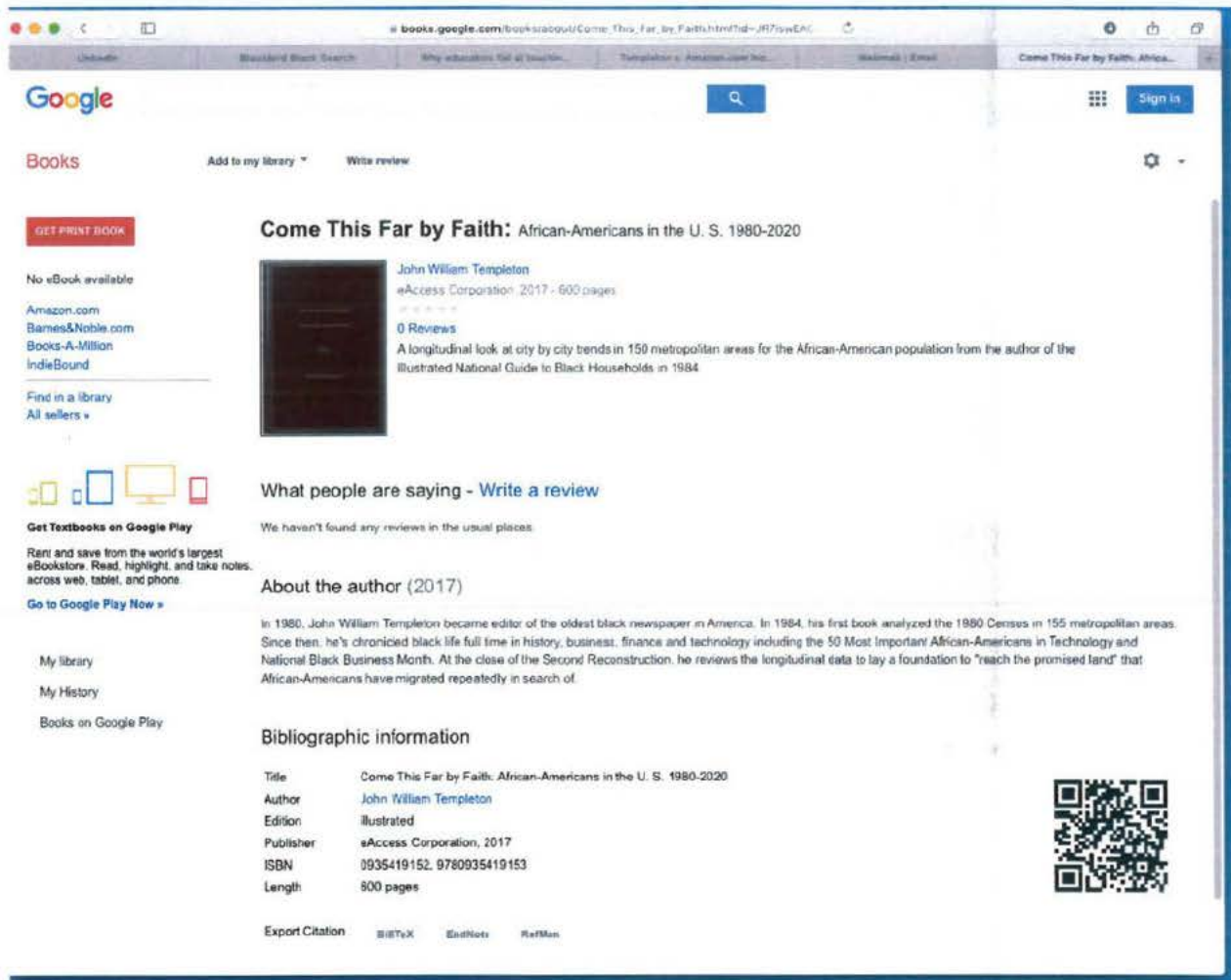
All Things Open 2015, October 19th and 20th, Raleigh NC. Hosted by DeLisa Alexander with special guests Carolina Simard, **John William Templeton**, and Nithya R...

Simply put, Google, Amazon and others place more than 130 pages of their own before his owned and earned media, favoring their own surreptitious capture of hundreds of facts about his customers.



In February, he was featured to the six million readers of California State Automobile Association and his nationwide promotion in August on Good Morning America. He didn't know about the latter for more than a month because his audience was diverted to these rigged pages. According to the *New York Times*, Amazon makes \$1,400 per year from each person it captures.

This seven year ordeal has been in recent weeks the subject of testimony to the House Energy and Commerce Committee and House Small Business Committee and a civil complaint in the Northern District of California, U.S District Court.



His stature as a journalist, historian, curator and religious leader is highjacked through these tactics in order to convince unsuspecting readers to give up their personal data.

Although most of these matters involve violations of California law, local and state prosecutors are not prepared to address these threats to the public. COPPA offers most of all the opportunity to engage current law in a systematic way to create a level playing field for African-American businesses and online users, who are the subject of racial profiling in a wide array of digital methodologies.

The Attorney General's regulation must see the COPPA as the newest addition to the state's civil rights legal framework and empower District Attorneys and the Department of Justice to understand the danger which individuals and small businesses have been placed under through several decades of an inadequate legal framework.

The State of California could be the last bulwark against a digital repetition of the Jim Crow era brought on through the movie industry.

The Risk to African-Americans from Privacy Violations

Baked-In Discrimination

"On August 13, 2018, the Assistant Secretary for Fair Housing and Equal Opportunity ("Assistant Secretary") filed a timely complaint with the Department of Housing and Urban Development ("HUD" or the "Department") alleging that Respondent violated subsections 804(a), 804(b), 804(c) and 804(f) of the Fair Housing Act, 42 U.S.C. §§ 3601-19 ("Act"), by discriminating because of race, color, religion, sex, familial status, national origin and disability.

“The Act authorizes the Secretary of HUD to issue a Charge of Discrimination (“Charge”) on behalf of aggrieved persons following an investigation and a determination that reasonable cause exists to believe that a discriminatory housing practice has occurred....

“It is unlawful to make, print, or publish, or cause to be made, printed, or published, any notice, statement, or advertisement with respect to the sale or rental of a dwelling that indicates any preference, limitation, or discrimination based on race, color, religion, sex, familial status, national origin or disability, or that indicates an intention to make such a distinction. 42 U.S.C. § 3604(c); 24 C.F.R. § 100.75(a), (b), (c)(1). Such unlawful activity includes “[s]electing media or locations for advertising the sale or rental of dwellings which deny a particular segment of the housing market information about housing opportunities because of race, color, religion, sex, handicap, familial status, or national origin.” 24 C.F.R. § 100.75(c)(3). Such unlawful activity also includes “[r]efusing to publish advertising for the sale or rental of dwellings or requiring different charges or terms for such advertising because of race, color, religion, sex, handicap, familial status, or national origin.” 24 C.F.R. § 100.75(c)(4). ...

“Respondent Facebook, Inc., is incorporated in Delaware with headquarters in Menlo Park, California. Respondent is the second largest online advertiser in the United States and is responsible for approximately twenty percent of all online advertising nationwide.

6. Respondent operates Facebook and Instagram, two of the most widely used social media platforms in the United States. Facebook has approximately 221 million active users in the United States and over two billion active users globally, while Instagram has approximately 114 million active users in the United States and over one billion active users globally, with active user defined as someone who uses the platform at least once per month. Respondent also operates Messenger, a messaging tool and platform that can be accessed from within Facebook or through a standalone website and mobile application. In addition, Respondent has created an “Audience Network,” which is comprised of thousands of websites and mobile applications that are operated by third parties but on which Respondent displays targeted ads.

C. Factual Allegations

7. Respondent collects millions of data points about its users, draws inferences about each user based on this data, and then charges advertisers for the ability to microtarget ads to users based on Respondent's inferences about them. These ads are then shown to users across the web and in mobile applications. Respondent promotes and distinguishes its advertising platform by proclaiming that "most online advertising tools have limited targeting options . . . like location, age, gender, interests and potentially a few others. . . . But Facebook is different. People on Facebook share their true identities, interests, life events and more."¹ As Respondent explains, its advertising platform enables advertisers to "[r]each people based on . . . zipcode . . . age and gender . . . specific languages . . . the interests they've shared, their activities, the Pages they've like[d] . . . [their] purchase behaviors or intents, device usage and more."² Thus, Respondent "use[s] location-related information—such as your current location, where you live, the places you like to go, and the businesses and people you're near to provide, personalize and improve our Products, including ads, for you and others."³
8. Advertisers pay Respondent to show targeted ads to users on Facebook, Instagram, and Messenger, and on Respondent's Audience Network. Targeted ads are generally placed through a single advertising platform called Ads Manager regardless of where the ads will be shown to users.
9. Respondent holds out its advertising platform as a powerful resource for advertisers in many industries, including housing and housing-related services. For example, Respondent promotes its advertising platform with "success stories," including stories from a housing developer, a real estate agency, a mortgage lender, a real-estate-focused marketing agency, and a search tool for rental housing.
10. Respondent's advertising platform is actively being used for housing-related ads. Such ads include ads for mortgages from large national lenders, ads for rental housing from large real estate listing services, and ads for specific houses for sale from real estate agents.
11. Because of the way Respondent designed its advertising platform, ads for housing and housing-related services are shown to large audiences that are severely biased based on characteristics protected by the Act, such as audiences of tens of thousands of users that are nearly all men or nearly all women."

This charge by the U.S. Department of Housing and Urban Development comes 55 years after Assemblyman Byron Rumford passed the California Fair Housing Act and 50 years after the passage of the national Fair Housing Act.

All of these issues would also be violations of the Unruh Civil Rights Act, the authorizing law for the California Department of Fair Employment and Housing. The state of California must understand this background of baked-in discrimination by online networks in order to enforce the California Online Privacy Protection Act, because customer data is being used not just to make money, but to actively discriminate.

This discrimination is confirmed in recent weeks from the inside. Black Facebook employees complain racism, discrimination have gotten worse

Jessica Guynn
USA TODAY

SAN FRANCISCO – An anonymous memo alleging Facebook still has a problem with racial bias is circulating inside the company one year after a former employee complained of racism and discrimination there.

The Medium post from 12 current and former employees, first reported by Business Insider, details a number of incidents, suggesting morale has sunk even lower since Mark Luckie published his Facebook post about discrimination on the company's Silicon Valley campus and on the social media giant's platform.

Both missives expose the racial fault lines in the mostly white tech industry and how the stubbornly persistent lack of representation and agency of African-Americans inside Facebook directly affects how black people on Facebook and its other platforms are treated.

“We may be smiling. We may post on Instagram with industry influencers and celebrities. We may use the IG ‘Share Black Stories’ filter and be featured on marketing pieces. We may embrace each other and share how happy we are to have the opportunity to work with a company that impacts nearly three billion people,” the anonymous memo says. “On the inside, we are sad. Angry. Oppressed. Depressed. And treated every day through the micro and macro aggressions as if we do not belong here.”

If computer programs do nothing but use existing literature and practice, particularly the motion picture industry which has systematized white supremacy since D.W. Griffith, it would lock in and accelerate

AI programs exhibit racial and gender biases, research reveals | Technology | The Guardian 6/2/19, 5:13 PM

An artificial intelligence tool that has revolutionised the ability of computers to interpret everyday language has been shown to exhibit striking gender and racial biases.

The findings raise the spectre of existing social inequalities and prejudices being reinforced in new and unpredictable ways as an increasing number of decisions affecting our everyday lives are ceded to automats.

In the past few years, the ability of programs such as Google Translate to interpret language has improved dramatically. These gains have been thanks to new machine learning techniques and the availability of vast amounts of online text data, on which the algorithms can be trained.

However, as machines are getting closer to acquiring human-like language abilities, they are also absorbing the deeply ingrained biases concealed within the patterns of language use, the latest research reveals.

Joanna Bryson, a computer scientist at the University of Bath and a co-author, said: "A lot of people are saying this is showing that AI is prejudiced. No. This is showing we're prejudiced and that AI is learning it."

But Bryson warned that AI has the potential to reinforce existing biases because, unlike humans, algorithms may be unequipped to consciously counteract learned biases. "A danger would be if you had an AI system that didn't have an explicit part that was driven by moral ideas, that would be bad," she said.

The research, published in the journal Science, focuses on a machine learning tool known as "word embedding", which is already transforming the way computers interpret speech and text. Some argue that the natural next step for the technology

may involve machines developing human-like abilities such as common sense and logic.

“A major reason we chose to study word embeddings is that they have been spectacularly successful in the last few years in helping computers make sense of language,” said Arvind Narayanan, a computer scientist at Princeton University and the paper’s senior author.

The approach, which is already used in web search and machine translation, works by building up a mathematical representation of language, in which the meaning of a word is distilled into a series of numbers (known as a word vector) based on which other words most frequently appear alongside it. Perhaps surprisingly, this purely statistical approach appears to capture the rich cultural and social context of what a word means in the way that a dictionary definition would be incapable of.

For instance, in the mathematical “language space”, words for flowers are clustered closer to words linked to pleasantness, while words for insects are closer to words linked to unpleasantness, reflecting common views on the relative merits of insects versus flowers.

The latest paper shows that some more troubling implicit biases seen in human psychology experiments are also readily acquired by algorithms. The words “female” and “woman” were more closely associated with arts and humanities occupations and with the home, while “male” and “man” were closer to maths and engineering professions.

And the AI system was more likely to associate European American names with pleasant words such as “gift” or “happy”, while African American names were more commonly associated with unpleasant words.

The findings suggest that algorithms have acquired the same biases that lead people (in the UK and US, at least) to match pleasant words and white faces in implicit association tests.

These biases can have a profound impact on human behaviour. One previous study showed that an identical CV is 50% more likely to result in an interview invitation if the candidate's name is European American than if it is African American. The latest results suggest that algorithms, unless explicitly programmed to address this, will be riddled with the same social prejudices.

"If you didn't believe that there was racism associated with people's names, this shows it's there," said Bryson.

The machine learning tool used in the study was trained on a dataset known as the "common crawl" corpus – a list of 840bn words that have been taken as they appear from material published online. Similar results were found when the same tools were trained on data from Google News.

Sandra Wachter, a researcher in data ethics and algorithms at the University of Oxford, said: "The world is biased, the historical data is biased, hence it is not surprising that we receive biased results."

Rather than algorithms representing a threat, they could present an opportunity to address bias and counteract it where appropriate, she added.

"At least with algorithms, we can potentially know when the algorithm is biased," she said. "Humans, for example, could lie about the reasons they did not hire someone. In contrast, we do not expect algorithms to lie or deceive us."

However, Wachter said the question of how to eliminate inappropriate bias from algorithms designed to understand language, without stripping away their powers of interpretation, would be challenging.

"We can, in principle, build systems that detect biased decision-making, and then act on it," said Wachter, who along with others has called for an AI watchdog to be established. "This is a very complicated task, but it is a responsibility that we as society should not shy away from."

How A.I. Can Be Weaponized to Spread Disinformation The New York Times 6/9/19, 9'03 AM

By CADE METZ and SCOTT BLUMENTHAL

In 2017, an online disinformation campaign spread against the “White Helmets,” claiming that the group of aid volunteers was serving as an arm of Western governments to sow unrest in Syria.

This false information was convincing. But the Russian organization behind the campaign ultimately gave itself away because it repeated the same text across many different fake news sites.

Now, researchers at the world's top artificial intelligence labs are honing technology that can mimic how humans write, which could potentially help disinformation campaigns go undetected by generating huge amounts of subtly different messages.

Tech giants like Facebook and governments around the world are struggling to deal with disinformation, from misleading posts about vaccines to incitement of sectarian violence. As artificial intelligence becomes more powerful, experts worry that disinformation generated by A.I. could make an already complex problem bigger and even more difficult to solve.

In recent months, two prominent labs — OpenAI in San Francisco and the Allen Institute for Artificial Intelligence in Seattle — have built particularly powerful examples of this technology. Both have warned that it could become increasingly dangerous.

Alec Radford, a researcher at OpenAI, argued that this technology could help governments, companies and other organizations spread disinformation far more efficiently: Rather than hire human workers to write and distribute propaganda, these

<https://www.nytimes.com/interactive/2019/06/07/technology/ai-text-disinformation.html>

Page 2 of 4

How A.I. Could Be Weaponized to Spread Disinformation - The New York Times 6/9/19, 9'03 AM

organizations could lean on machines to compose believable and varied content at tremendous scale.

A fake Facebook post seen by millions could, in effect, be tailored to political leanings with a simple tweak.

“The level of information pollution that could happen with systems like this a few years from now could just get bizarre,” Mr. Radford said.

This type of technology learns about the vagaries of language by analyzing vast amounts of text written by humans, including thousands of self-published books, Wikipedia articles and other internet content. After “training” on all this data, it can examine a short string of text and guess what comes next.

We wanted to see what kind of text each of the labs’ systems would generate with a simple sentence as a starting point. How would the results change if we changed the subject of the sentence and the assertion being made?

OpenAI and the Allen Institute made prototypes of their tools available to us to experiment with. We fed four different prompts into each system five times.

What we got back was far from flawless: The results ranged from nonsensical to moderately believable, but it’s easy to imagine that the systems will quickly improve.

“The level of information pollution that could happen with systems like this a few years from now could just get bizarre,” said Alec Radford, an artificial intelligence researcher in San Francisco. Carlos Chavarría for The New York Times

Researchers have already shown that machines can generate images and sounds that are indistinguishable from the real thing, which could accelerate the creation of false and misleading information. Last month, researchers at a Canadian company, Desso, built a system that learned to imitate the voice of the podcaster Joe Rogan by analyzing audio from his old podcasts. It was a shockingly accurate imitation.

Now, something similar is happening with text. OpenAI and the Allen Institute, along with Google, lead an effort to build systems that can completely understand the natural way people write and talk. These systems are a long way from that goal, but they are rapidly improving.

“There is a real threat from unchecked text-generation systems, especially as the technology continues to mature,” said Delip Rao, vice president of research at the San Francisco start-up A.I. Foundation, who specializes in identifying false information online.

OpenAI argues the threat is imminent. When the lab’s researchers unveiled their tool this year, they theatrically said it was too dangerous to be released into the real world. The move was met with more than a little eye-rolling among other researchers. The Allen Institute sees things differently. Yejin Choi, one of the researchers on the project, said software like the tools the two labs created must be released so other researchers can learn to identify them. The Allen Institute plans to release its false news generator for this reason.

Among those making the same argument are engineers at Facebook who are trying to identify and suppress online disinformation, including Manohar Paluri, a director on the company’s applied A.I. team.

“If you have the generative model, you have the ability to fight it,” he said.

Message

From: Earley, Susan [REDACTED]
Sent: 12/13/2019 10:23:11 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Holbrook, Jeremy [REDACTED]
Subject: CCPA commentary

<https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf>

Commentary:

990.301(a) Please separate this section into three sections for clarity.

Suggested text:

(a) "Affirmative authorization" means an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information.

(1) For consumers under 13 years old, it means that the parent or guardian has provided consent to the sale of the child's personal information in accordance with the methods set forth in section 999.330.

(2) For consumers 13 years and older, it is demonstrated through a two-step process whereby the consumer shall first clearly request to opt-in, and then second, separately confirm their choice to opt-in.

990.301(u)

This does not cover the case where a parent may "request to delete" information for their children, or a guardian may "request to delete" information about the person they manage.

Suggested text:

"Verify" means to determine that the consumer making a "request to know" or "request to delete" is the consumer about whom the business has collected information, or is the parent or legal guardian of the consumer.

999.305(a)(1) This sentence is too complex and it looks like there is an extra clause. Remove the extra clause.

Suggested text:

The purpose of the notice at collection is to inform consumers at or before the time of collection of ~~a consumer's personal information~~ of the categories of personal information to be collected from them and the purposes for which the categories of personal information will be used.

999.305(a)(2)(e) Examples in laws are never a good idea.

Suggested text:

Be visible or accessible where consumers will see it before any personal information is collected.

- a. For online collection, at least one of*
 - (i) a conspicuous link to the notice on the business's website homepage*
 - (ii) a conspicuous link to the notice on the business's mobile application's homepage*
 - (iii) a conspicuous link to the notice on all webpages where personal information is collected.*
- b. For offline collection, at least one of*
 - (i) include the notice on printed forms that collect personal information*
 - (ii) provide the consumer with a paper version of the notice*
 - (iii) post prominent signage directing consumers to the web address where the notice can be found.*

999.305(a)(3) Reword for clarity.

Suggested text:

(3) A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection. Prior notification and explicit consent from a consumer is required to allow usage of that consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection.

999.305(b)(4) Offline notices should not be directed to a website!

Suggested text:

A link to the business's privacy policy, or in the case of offline notices, the email or postal address used to request a copy of the business's privacy policy.

999.306(b)(2) For clarity and ease of maintenance, refer to section 999.305(a)(2)(e)(b), or just to 999.305(a)(2)(e) if the prior suggestion was not accepted.

Suggested text:

A business that substantially interacts with consumers offline shall also provide notice to the consumer by an offline method that facilitates consumer awareness of their right to opt-out. Such methods are described in section 999.305(a)(2)(e)(b).

999.308(b)(2) Add explanation of effects of deletion, or reasons why a business can't delete their information. (open accounts with balances, sale of merchandise that may be subject to legal notification of recalls, etc.)

Suggested text:

- a. *Explain that the consumer has a right to request the deletion of their personal information collected or maintained by the business.*
 - i. *Deletion of personal information related to accounts held with the business will require closing of those accounts. If the account terms have not been satisfied, then the request cannot be honored at that time.*
 - ii. *Deletion of personal information related to the business' legal notification obligations to that consumer is prohibited without a properly executed waiver of those rights.*

Thanks!

Susan Earley

Director

*Certified Computing Professional, Principal Level
Certified Data Management Professional, Master Level
Certified Business Intelligence Professional, Master Level*

This message, including any attachments, is the property of Transform HoldCo LLC and/or one of its subsidiaries. It is confidential and may contain proprietary or legally privileged information. If you are not the intended recipient, please delete it without reading the contents. Thank you.



January 29, 2020

California Attorney General Xavier Becerra
ATTN: Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Postponing CCPA Enforcement for Six Months

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 substantially benefits consumers and the economy, and we strongly support meaningful and effective privacy protections in the marketplace.

Although the California Consumer Privacy Act ("CCPA") went into effect on January 1, 2020, the final regulations have not yet been promulgated, leaving our members and thousands of other California businesses uncertain concerning their ultimate compliance obligations. Given the extraordinary complexity of the law and the wide range of open issues to be clarified from the draft guidance, there will not be sufficient time for many businesses to effectively implement the final regulations prior to the anticipated enforcement date of July 1, 2020. We therefore ask you to delay enforcement of the CCPA until at least six months from the date of finalization of the rules implementing the law, in order to provide businesses a sufficient time period to implement the new regulations before being subject to enforcement.

I. It is Appropriate to Provide Businesses a Reasonable Period of Time to Implement the New Regulations

As soon as the California Legislature passed the CCPA, it was clear that the law's requirements would evolve through both the legislative and rulemaking process. It was not clear, however, that the key CCPA provisions would be substantially amended so close to its effective date, and that the rules implementing its terms would not be finalized until after the law became operative.

While we recognize that the amendments in the California Legislature delayed the development and formal release of draft regulations implementing the CCPA until October 11, 2019,¹ these draft rules presented significant new and unprecedented requirements, such as the requirement for a business upon receipt of a consumer opt-out request, to "notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business' receipt of the consumer's request that the consumer has exercised their right to opt-out and instruct them not to further sell the information."²

¹ See State of California Office of Administrative Law, *Notice Publication/Regulations Submission* (Oct. 11, 2019), located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-std400a.pdf> (last visited Jan. 28, 2020).

² Cal. Code Regs. tit. 11, § 999.315(f) (proposed Oct. 11, 2019).

Moreover, the draft rules imposed on businesses entirely new recordkeeping obligations, notice requirements, and verification rules, among many other novel requirements.³ Businesses are still contending with the proposed regulations' new mandates and are working earnestly to adjust their systems and build new processes to facilitate compliance.

Unfortunately, it is presently unclear when the rules will be finalized and whether they will be further amended. Just five months before enforcement is scheduled to begin, companies that are subject to the CCPA are faced with the likelihood that the draft rules could substantially change from their present form and impose entirely new requirements. Publications disseminated by your office indicate that the draft rules will be revised not only after input received during the initial comment period, but that you will also hold at least one subsequent 15-day comment period on the content of those updates.⁴ If any changes to the regulations are made that constitute "substantial and sufficiently related" changes, the Attorney General ("AG") must provide for at least a 15-day public comment period.⁵ If, on the other hand, any of the changes to the regulations are "substantial, but not sufficiently related" changes, the AG must issue a new notice in the California Regulatory Notice Register and provide for a new 45-day public comment period.⁶ The rules will not be effective until the rules are submitted and reviewed by the Office of Administrative Law, further reducing the time available to businesses to implement the regulations. This timeline increases the likelihood that the draft rules will not be finalized before, or only a short period prior, to the law's July 1, 2020 enforcement date.

We and our members strongly support the underlying goals of the CCPA. The limited and quickly shrinking time before the existing enforcement deadline, however, will place business in a nearly untenable position. Without final regulatory requirements, business will be unable to make operational changes to their systems, further delaying finalization of their compliance programs. Businesses should be afforded an appropriate time period to implement the new regulations once they become final and before being subject to enforcement.

II. Providing a Reasonable Period of Time for Implementing the New Regulations Benefits Consumers

While the law instructs the AG not to bring any enforcement action prior to July 1, 2020, there is no restriction on you providing a reasonable period of additional time for California businesses to review and implement the final regulations before initiating any enforcement actions. Thus, in order to avoid consumer and business confusion with respect to the new rules, we request that you further delay the enforcement of the law to begin six months from the date the CCPA regulations become final. This short deferral will give businesses the time they need to understand and effectively operationalize the rules helping ensure consumers have access to the rights afforded under the new law.

Business attempts to comply with an incomplete legal regime risks causing significant consumer frustration and the implementation of inadequate or duplicative compliance tools. While we understand

³ *Id.* at §§ 999.305 – 308, 317, 323-325.

⁴ See Office of the California Attorney General, *California Consumer Privacy Act (CCPA) Fact Sheet* at 3, located at https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf (last visited Jan. 28, 2020).

⁵ *Id.* See also Office of the Attorney General California Department of Justice, *California Consumer Privacy Act (CCPA) Department of Justice Office of the California Attorney General: Background on Rulemaking Process* at 3, located at <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-ppt.pdf> (last visited Jan. 28, 2020) and California Office of Administrative Law, *About the Regular Rulemaking Process*, located at https://oal.ca.gov/rulemaking_participation/ (last visited Jan. 28, 2020).

⁶ *Id.*

that your office is working expeditiously to provide clear rules for businesses to operationalize the CCPA, the clock is working against well-intentioned businesses in their compliance efforts.

We urge you to give California businesses the opportunity to understand what is required under the law before they are put at risk for being penalized for violating its terms.

* * *

While our members support California's intent to provide consumers enhanced privacy protections, the evolving nature of the CCPA and the draft nature of the proposed rules makes the current enforcement date of July 1, 2020 a difficult deadline for businesses and consumers alike. Consumer privacy is best served when businesses that leverage data do so in accordance with clear and concrete laws and regulations that present them with adequate time to adjust their practices to come into compliance with the new requirements.

We urge you to accept this proposed six-month enforcement moratorium, thereby giving businesses throughout the United States that operate in California adequate time to prepare to adhere to the law's final form. Delaying the CCPA's enforcement in this manner will help ensure that businesses can effectively provide consumers with the new protections and rights that the law and its implementing regulations require.

Thank you in advance for consideration of this request.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
[REDACTED]

Alison Pepper
Senior Vice President
American Association of Advertising Agencies, 4A's
[REDACTED]

Christopher Oswald
SVP, Government Relations
Association of National Advertisers
[REDACTED]

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
[REDACTED]

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
[REDACTED]

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
[REDACTED]

CC: Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP