

Message

From: Alan Titus [REDACTED]
Sent: 12/6/2019 11:37:22 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments on Privacy Regulations
Attachments: Comments on Privacy Regs.Alan Titus.pdf

Dear DOJ,

Attached please find a comment letter on the proposed privacy regulations.

Alan Titus
Robb & Ross
591 Redwood Hwy, Suite 2250
Mill Valley, CA 94941
[REDACTED]

ROBB & ROSS

PHILIP A. ROBB
ALAN J. TITUS
ANNE C. SLATER †
JOSEPH W. ROBB **

JOSEPH W. ROBB A PROFESSIONAL CORPORATION

591 REDWOOD HIGHWAY, SUITE 2250
MILL VALLEY, CALIFORNIA 94941
TELEPHONE: (415) 332-3831
FAX: (415) 383-2074

STERLING L. ROSS, JR. *†
*OF COUNSEL

†CERTIFIED SPECIALIST IN ESTATE
PLANNING, PROBATE AND TRUST
LAW, THE STATE BAR OF
CALIFORNIA BOARD OF LEGAL
SPECIALIZATION

** (1926 - 2019)

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: Comments on Proposed CCPA Regulations

Dear Sir or Madam:

I write on behalf of a licensed California cardroom with comments on the proposed privacy regulations to implement the California Consumer Privacy Act (the "CCPA").

Cardrooms are old-fashioned, brick and mortar businesses. Customers come in and play card and tile games against one another and place bets on the games. Betting is done by means of gaming chips, and players purchase and redeem chips from the house. My client has a website but does not interact with customers on the website in any fashion. Nor does my client engage in any advertising or marketing.

My client collects information regarding its players only to the extent required by federal and state law. The federal Bank Secrecy Act (the "BSA") and state regulation require that the cardroom file Cash Transaction Reports when a player has cash-in transactions or cash-out transactions in a single day over \$10,000. 31 CFR §1021.311. This requires collection of certain information, namely, the patron's social security number, his or her proof of identification, and the amount of the transaction. 31 CFR §1010.312. My client is required to aggregate multiple transactions by the player and is required under federal law to maintain a Multiple Transaction Log, tracking purchases, redemptions and exchanges. 31 CFR §1021.410(b)(11).

The BSA further requires my client to file Suspicious Activity Reports ("SARs") on players and activity that appear suspicious. 31 CFR §1021.320. This entails detection, investigations, and collection of information on suspicious persons and suspicious financial activity. It also requires the card room to have procedures to perform various levels of due diligence on its customers to know their source of funds. FIN-2007-G005 Q&A 14.

The purpose of the BSA is to provide law enforcement with information useful in investigations of money laundering, terrorist financing or other financial crimes. To that end, the BSA prohibits disclosure of a SAR and any information that would reveal the existence of a SAR. 31 CFR §1021.320(e). In addition, disclosure of information to a player that could assist them in structuring transactions to evade the law is made illegal. 31 USC §5324(a)(3). Thus, if a player were to request the know his or her total chips purchases so far that day, the cardroom is not allowed to provide the information. In general, law enforcement expects detection of suspicious activity and investigations to proceed without the subject's knowledge.

The only other reason my client collects information on players is to comply with federal and state tax reporting rules. When my client offers a promotion and pays a jackpot, the cardroom is required to file information reports with the IRS and with the FTB. Absent legal requirements under the BSA and the tax codes, my client would not collect information on its customers.

It is difficult to determine to what extent the CCPA applies under these circumstances. Section 1798.145(a) provides, "The obligations imposed on businesses by this title shall not restrict a business's ability to: (1) Comply with federal, state, or local laws." Further, Section 1798.196 provides, "This title...shall not apply if such application is preempted by, or in conflict with, federal law...." However, concepts of interference, preemption and conflict of laws are highly dependent on administrative and judicial interpretations. Whether the CCPA is preempted by or in conflict with federal law is not easily determined by a private party.

The draft regulations do not address this preemption issue, and we request that provisions be added to provide guidance on the application of sections 1798.145 and 1798.196. We believe that where information is collected to comply with federal or state law, CCPA is preempted. But further, where the law

requires collection of information for law enforcement purposes as with the BSA, the federal law occupies the field and preempts the BSA. The only information that might not be preempted is identification and tax information collected directly and openly from the customers.

In addition to issues of preemption, the proposed regulations set forth a number of requirements that are inconsistent with sections 1798.145 and 1798.196, and we detail those below.

Section 999.305. Notice at Collection of Personal Information

Subsection (a)(3)

This subsection provides, "A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection." This regulation would conflict with the BSA and with the IRC by prohibiting a business from complying with the BSA and IRC if the business failed to provide the notice required by the CCPA. This regulation is also inconsistent with CCPA provisions not to interfere with compliance with federal law.

Subsection (a)(4)

This subsection provides, "A business shall not collect categories of personal information other than those disclosed in the notice at collection." This regulation would conflict with the BSA and the IRC by prohibiting a business from complying with those laws if the business failed to provide the notice required by the CCPA. This regulation is also inconsistent with CCPA provisions not to interfere with compliance with federal law.

Subsection (a)(5)

This subsection provides, "If a business does not give the notice at collection to the consumer at or before collection of their personal information, the business shall not collect personal information from the consumer." Again, this fails to take into account legal obligations under the BSA and IRC as well as state law, and is inconsistent with the CCPA.

Subsection (b)(1)

This subsection requires that the notice at collection include “a list of the categories of personal information about consumers to be collected.” This raises the question as to what extent cardrooms are required to disclose categories to their customers given that such disclosure could impede federal and state law enforcement efforts. Disclosure of collection of a category such as ‘personal and tax identification’ is not a problem since that is collected openly and directly from the player. But disclosure of transactional information could violate the BSA and disclosure of any other categories would likely impede the purposes of the BSA.

Subsection (b)(2)

Subsection (b)(2) requires that a notice be served on customers informing them of the “business or commercial purposes” for which information is being collected. But what if the collection of personal information is required by law and not done for either business or commercial purposes? This subsection does not address that possibility and thus creates uncertainty.

Section 999.307. Notice of Financial Incentive

This subsection states that the “purpose of the notice of financial incentive is to explain to the consumer *each financial incentive ... a business may offer* in exchange for the retention or sale of a consumer’s personal information....” However, this is not consistent with Civil Code §1798.125.

The draft regulation would apply to all financial incentives, but the statute does not require notice of all financial incentives. Civil Code section 1798.125(b)(2) requires notice only of specific financial incentives, namely those offered pursuant to 1798.125(a). Subsection (a) applies to the following specific events, when a business denies goods or services to the consumer; charges different prices or rates for goods or services; provides a different level or quality of goods or services; or suggests that consumer will receive a different price or rate for goods or services or a different level or quality of goods or services. If none of those specific situations apply, offering of a financial incentive does not trigger the notice requirement. The proposed regulation, by applying to other financial incentives, is broader than and inconsistent with the statute.

My client is required to obtain a patron's personal and tax identification when the player has a transaction that exceeds the \$10,000 threshold. However, my client often attempts to obtain a player's identification before the player reaches that threshold in order to improve compliance and to discourage illegal structuring. My client offers promotional items as gifts to customers who are reluctant to provide identification and has found this to be an effective way to improve compliance with the BSA. Providing notice of financial incentive will only serve to discourage customers from providing their identification, a result clearly at odds with federal and state law.

Section 999.308. Privacy Policy

Subsection (b)(1)(a.)

This regulation would require that the privacy policy "explain that a consumer has a right to request that the business disclose what personal information it collects." This raises the question of what rights a consumer really has when the BSA applies. If the CCPA requires disclosure of personal information used to file a SAR, it clearly conflicts with the BSA. If the CCPA requires disclosure of personal information obtained in an investigation, we believe that the BSA preempts the field. As suggested above, we believe that the CCPA should be limited at most to disclosure of information collected directly from the customer, and not apply to other information gathered in compliance with the BSA.

Subsection (b)(1)(d.)(1.)

This subsection would require the privacy policy to list the categories of consumers' personal information the business has collected in the preceding 12 months. This raises the same questions as in the prior discussion. What rights does a consumer really have given the purposes of the BSA? Again, we suggest that where information is collected to comply with the BSA, the CCPA should be limited at most to disclosure of information collected directly from the customer, and not apply to other information gathered in compliance with the BSA.

Subsection (b)(1)(d.)(2.)

This regulation would require the privacy policy to provide the sources from which personal information was collected. Again, where information is being

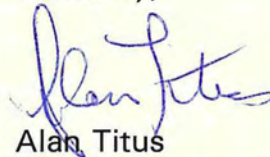
Privacy Regulations Coordinator
California Office of the Attorney General
December 6, 2019
Page 6

collected to comply with the BSA, we believe that this law would impede the purposes of the BSA and thus is preempted by the BSA.

* * *

We appreciate your consideration of these comments.

Sincerely,



Alan Titus

Message

From: Matt Akin [REDACTED]
Sent: 12/5/2019 10:56:11 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments on Proposed California Consumer Privacy Act Regulations (ACLHIC - ACLI)
Attachments: ACLHIC - ACLI CCPA Comment Letter.pdf

Dear Attorney General Becerra:

The Association of California Life and Health Insurance Companies ("ACLHIC") and The American Council of Life Insurers ("ACLI") respectfully submit the following comments on behalf of our members. We appreciate the thoughtful and deliberative process your office has undertaken for the development of the proposed regulations.

Please do not hesitate to contact ACLHIC staff with any questions you may have.

Sincerely,

Matt Akin
Legislative and Communications Associate
ACLHIC
1201 K Street, Suite 1820
Sacramento, CA 95814
[REDACTED]

Website: www.aclhic.com

December 5, 2019

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

Re: *Comments on Proposed California Consumer Privacy Act Regulations (October 11, 2019)*

Dear Attorney General Becerra:

The American Council of Life Insurers (“ACLI”) and the Association of California Life and Health Insurance Companies (“ACLHIC”) respectfully submit the following comments on behalf of our members. We appreciate the thoughtful and deliberative process your office has undertaken for the development of the proposed regulations.

Life insurers have long been the diligent stewards of our customers’ highly sensitive personal information. We support, and already abide by, strong consumer privacy laws. We have managed consumers’ confidential medical and financial information appropriately for decades, and in the instance of a number of member companies, a couple of centuries. We look forward to working with you and lending our industry’s historical expertise to this weighty issue.

Executive Summary

- *Insurers have a strong and historic consumer privacy track record*
- *The regulations exceed statutory authority in certain areas*
- *Sufficient time is needed for regulatory compliance*
- *The regulations should not compromise consumer or company security*
- *The regulations should be harmonized with existing privacy laws and regulations*
- *Notice requirements should maximize consumer clarity and minimize complexity*
- *Opt-out provisions should be simple to understand and apply narrowly to businesses that sell personal information*
- *Less proscriptive privacy requirements lead to clearer privacy notices for consumers*
- *Regulatory enforcement must be prospective*

The California Consumer Privacy Act of 2018 (“CCPA”) is a complex and comprehensive law. And while we appreciate the clarification and guidance provided by the proposed regulations, we are concerned with the complexity of certain substantive provisions and believe that, in some instances, the proposed regulatory requirements go beyond the underlying law.

Compliance Deadline

The proposed regulations are slated for completion and/or final adoption in the Spring of 2020. We strongly believe that the date for compliance with the rules should be at least 2 years after they have been finalized and that the rules should be enforced solely on a prospective basis and should not be retroactively applied. The underlying California privacy law has not yet stabilized as borne out by the comprehensive and material new changes proposed in the *California Privacy Rights Act of 2020* ballot initiative. It is possible a number of provisions of the underlying law will be materially changed if the ballot initiative passes next year, resulting in the regulations being rendered out of conformance. Moreover, the proposed regulations are comprehensive, contain new substantive provisions and, as we address later in this letter, in some instances are beyond the scope of the underlying law. Companies must have reasonable time to come into compliance with these comprehensive rules.

Data Security

While the focus of the proposed regulations and the underlying law is protection of consumers' personal information, we are concerned that the regulations may put the **security** of that personal information at risk. We will discuss the individual security concerns in more depth below, however, we offer as an example the requirements to describe the verification process to consumers and the process for the right to request deletion in §999.308 as potentially creating an added security risk by making it easier for bad actors to compromise the process.

Regulatory Impact

Of fundamental concern, some provisions of the proposed regulations go beyond the scope of the new privacy law to impose substantive new requirements upon companies operating both in California and, because of the comprehensive nature of the new statute and the ubiquitous nature of personal information, on companies' business far beyond the state's borders. As the Attorney General stated in the "Notice of Proposed Rulemaking Action", the adoption of these regulations "may have a significant, statewide adverse economic impact directly affecting business, including the ability of California businesses to compete with businesses in other states." As the Attorney General acknowledges, the proposed regulations impose a number of significant reporting, recordkeeping and other compliance requirements on companies doing business in California. The Standardized Regulatory Impact Analysis (SRIA) provided by the Attorney General estimates that the cost of the regulations over a ten-year period to be between \$467 million to \$16.4 billion. These are costs, as the Attorney General points out, that "go beyond the impacts of the CCPA." We believe the Attorney General should carefully consider and address compliance and potential conflicts with regulatory alternatives, such as the privacy protection requirements found in current laws. The current compliance hurdles and potential conflicts will jeopardize consumer benefits and protections and are likely to have the adverse effect on companies described above. A good example is consumer familiarity with current privacy notices. Several industry privacy notice requirements have been in place for a number of years and have been perfected over time. We believe that a simplified standardized approach to this issue would ultimately benefit both consumers and companies.

Article 2: Notice

Consumer notice should be designed to provide transparency and understanding to consumers about the collection and use of their personal information. Over the course of time, regulators and industry partners have

struggled for a balance in the advancement and perfection of consumer notices. In development of a regulatory framework for the General Data Protection Regulation (“GDPR”), the E.U. has faced these same issues. European Article 29 Working Party Guidelines on Transparency recognizes the need to inform consumers and provide a sufficient level of transparency, but given the diversity of businesses and practices, recognized the important need for flexibility in how to format and provide consumer transparency:

“There is an inherent tension in the GDPR between the requirements on the one hand to provide the comprehensive information to data subjects which is required under the GDPR, and on the other hand do so in a form that is concise, transparent, intelligible and easily accessible. As such, an bearing in mind the fundamental principles of accountability and fairness, controllers must undertake their own analysis of the nature, circumstances, scope and context of the processing of personal data which they carry out and decide....how to prioritize information which must be provided to data subjects and what are the appropriate level of detail and methods for conveying the information.”

Rather than the over-proscriptive requirements in the draft regulations, California should take a similarly flexible approach.

Timing of Notice

Section 999.305 (a)(3) requires notice to consumers at the time of collection and explicit consent for any new, previously undisclosed, use of information. The notices will become long and less consumer friendly if businesses are required to include every potential purpose prior to the collection of personal information. The stated goal of the CCPA is to provide meaningful information to consumers regarding the use of their personal information. However, some provisions of the proposed rule, including in this section, are counterproductive to that goal. Instead of explicit consent for any new use of information, a more meaningful solution would be to require that a business may use a consumer’s personal information only for purposes that are compatible with those disclosed in the notice at collection.

It appears that two separate and distinct types of notices are contemplated by the proposed regulations. A notice at the time of collection (§999.305) and a notice by means of the privacy policy (§ 999.308). As a practical matter, it would be much more consumer friendly to have a single privacy notice/ policy that contains all of the information consumers need. It makes little sense to require two separate documents which essentially serve the same purpose.

Notice of Right to Opt-Out of Sale

The statute is unambiguous in §1798.120(b) in establishing that the notice of opt-out requirement does not apply to businesses that do not currently sell consumer personal information. However, the proposed regulations, in Section 999.306, greatly expand upon the notice of right to opt-out of sale requirement, creating new obligations on businesses which are not contemplated by the CCPA.

Specifically, §999.306(a)(1) states that the purpose of the notice of right to opt-out of the sale of personal information is to inform consumers of their right to direct a business that sells or may in the future sell their personal information to stop selling and refrain from doing so in the future. Section 999.306(a)(2) requires a business to state in its privacy policy that it does not and will not sell personal information and, in addition, mandates that a consumer whose personal information is collected while a notice of right to opt-out of sale is not posted is deemed to have opted out. Lastly, §999.316 requires businesses to seek opt-in consent from a consumer who has previously opted out. The combination of these three provisions is problematic for both businesses and consumers.

The CCPA, in §1798.120, requires businesses to provide a notice of right to opt out of sale only if they currently sell consumer personal information. The underlying statute does not place this requirement on companies that may sell personal information in the future. Under the requirements of the proposed regulation, companies currently not selling personal information will be confronted with an intractable situation in which

the compliance structure they have already put in motion may put them at a disadvantage as compared to those who are currently selling information. Therefore, the perverse consequence of the currently drafted requirement could be that more businesses decide to act as if they sell, even if they do not. Companies might post opt-out of sale buttons to protect themselves against the need to get opt-in consent from an unknown population of consumers in the event they change business models or, more troubling, because of the perpetually changing and complex definition of sale may potentially be determined to include an existing or future business practice.

For the reasons stated above, the requirement in §999.306(d)(2) that a business proactively declare that it will not sell consumer personal information in the future should be deleted.

Privacy Policy

There are several beneficial provisions in the privacy policy requirement section such as the ability for the policy to be generic and posted online. However, the proposed requirements for the privacy policy are much more prescriptive than past California statutory requirements. While regulatory guidance is welcomed and needed, one-size does *not* fit all. Instead a less proscriptive, more flexible approach is warranted to make privacy policies easier for consumers to understand and for businesses to comply with the related requirements.

Consumers have been receiving privacy notices in established, limited and stabilized formats, such as under Gramm-Leach-Bliley, for years. Use of similar formats for compliance with CCPA will make new notices more understandable. Companies should be permitted to use and appropriately modify existing formats.

➤ *Verification*

- The requirement to describe the verification process in §999.308 (b)(1)(c) is beyond the scope of CCPA and is likely to create a significant security risk with little added value to the consumer by making it easier for criminals to compromise the process. For security purposes a company's internal verification process should be confidential. We respectfully submit that a description of the verification process is not necessary, and that the consumer should simply be provided with information on how to submit a request, and what documentation must be provided for a valid verification.
- Similarly, §999.308(b)(1)(d)(2) contains overly prescriptive and redundant requirements. The underlying statute does not require disclosure of sources, purposes and third parties by category of personal information. The requirements under this section should be less prescriptive and more focused on what would be useful to the consumer. As long as all relevant information is disclosed, companies should not be required to specify sources and third parties. Businesses should not be required to change their privacy notice or provide an additional notice unless a process has been materially altered, otherwise consumers could potentially become immune to the constant stream of notices.

➤ *Disclosure or Sale of Personal Information*

- The CCPA requires businesses that do not sell consumers' personal information to disclose that fact. §999.308(b)(1)(e)(1) appears to require that companies disclose that they disclose, which is a redundant exercise. If the business does not disclose to third parties, that should be stated in the privacy policy, but if they do disclose to third parties, listing the categories of third parties to whom the business discloses should be sufficient. A quick fix of this provision would be to delete the words "disclosed or" from this clause.
- A single statement which informs consumers that the business does not sell personal information should be sufficient. As written, § 999.308(b)(1)(e)(3) seems to imply a business redundantly state again that it does not sell the personal information.

➤ *Right to Request Deletion of Personal Information*

- Similar to the comments above, § 999.308 (b)(2) which requires the disclosure of the process for the right to request deletion, could create a security risk. For the reasons stated above, a business should not have to describe the process they will use to verify. Authentication techniques should be kept confidential.
- Designation of an authorized agent may vary dramatically based on the type of consumer as well as the type of request. Designation of an authorized agent can be addressed simply and clearly through the verification process itself. Any nuances should be addressed through state laws regarding agency. Moreover, detailed disclosure of authorized agent requirements could be exploited for fraudulent purposes. To ameliorate the above issues and to protect against abuse of the process the requirement in § 999.308 (b)(5) that companies explain the designation process in the privacy notice, should either be removed or be simplified to note that consumers have a right to designate an authorized agent.

Article 3. Business Practices for Handling Consumer Requests

As mentioned above, the financial services industry has a strong historical track record on consumer privacy. Not only are financial service companies leaning into compliance with CCPA, they continually strive to maintain the level of trust they have established with customers over generations. Because of the lack of consideration for existing privacy regimes, both the CCPA and certain requirements proposed in the regulation are creating “exception paths” which may cause divergent practices. These variations in implementation will almost certainly lead to consumer and company confusion. As we have stated before, a repeatable, homogenized and simplified approach to a regulatory framework for privacy is ultimately better for the consumer.

Some of the most substantive provisions of the proposed regulations are the requirements under Article 3. Anticipating the effective date of CCPA in January 2020, many companies have moved forward with compliance programs. While much of the content of Article 3 is helpful in guiding companies with compliance, the level of detailed requirements means companies will have to make changes to their already developed systems. It is fundamental that companies be given adequate time to come into compliance with these new requirements.

Responding to Requests to Know and Requests to Delete

The requirement in §999.313(a) to confirm the receipt of a request to know or delete personal information is inconsistent with the CCPA, unnecessary and overly burdensome to businesses. If a consumer submits a request by phone or website as instructed in the privacy notice, a consumer can assume that the request was received and that he or she will get a response within the 45-day time period set by the CCPA. A 10-day confirmation is impractical and bureaucratic. The relevant information the consumer needs to effectuate a request to know or delete personal information is already in the privacy notice. In many cases, if the consumer has submitted a request, then they have already been verified (e.g. they have logged in to their online account). This provision should be deleted.

Section 999.313(c)(2) permits a business to deny a consumer's request to disclose categories of information if it cannot verify the person making the request. If a company denies a request, the subsection requires that the business provide the person with the company's general business practices regarding collection, maintenance and sale of personal information. This is another example of why one, single, comprehensive notice makes sense. The consumer will see everything in one place, including the general business practices and how to submit a request. Repeating information or putting additional information in the communication

denying a request is unnecessary and bureaucratic. We would therefore suggest the deletion of the last sentence in §999.313(c)(2).

The language in §999.313(d)(1) regarding responding to requests to delete is unreasonably burdensome for companies that do not sell personal information. There should be an exception for businesses not selling personal information so that they are not forced to manage an unnecessary opt-out list. A more simplified approach for both consumers and companies is for a notice to be provided offering the opt-out prior to selling in the future, similar to the process described in the comments above.

As long as the information is secured and unused, companies should be permitted to retain personal information stored on an archived or backup system for as long needed for legal or regulatory purposes or because deletion is infeasible. In many cases it is impossible to selectively delete data from a backup system without compromising its integrity. We would suggest the following language found in NY DFS 500.13 as proposed remediation: *“As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information ... that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.”*

As we have previously stated, to achieve functional efficiencies, compliance with CCPA should be easy to automate and standardize. Unfortunately, a number of provisions in the draft regulations will make the development of productive compliance systems difficult with little to no benefit to either companies or consumers. A perfect example is §999.313(d)(6) which requires businesses to provide a detailed explanation when they deny a consumer's request to delete personal information. If a consumer believes a denial is inappropriate, there are administrative avenues for them to raise their concerns. And, if a business does not comply with the law, there are appropriate regulatory enforcement mechanisms. It is our position that §999.313(d)(6)(c) exceeds the scope of the CCPA and is a detrimental restraint of trade and should be deleted.

Service Providers

Section 999.314(d) imposes a new burden on service providers that is not contemplated by the CCPA. The requirements in this section will unreasonably require service providers to put processes in place for CCPA compliance even when they are not directly subject to the law. The privacy notices required under the CCPA provide enough information for consumers to determine out how to properly submit individual rights requests without creating a disproportionate burden on businesses to implement new operational process.

Disclosure of Consumer Request Metrics

Finally, the scope of §999.317(g) should be limited to businesses that buy or sell personal information. The phrase “receives for the business's commercial purposes” is vague and subject to overly broad construction. The additional recordkeeping requirements in §999.317(g) are onerous and do not seem to satisfy a cost/benefit analysis litmus test.

Conclusion

The life insurance industry generates approximately 225,600 jobs in California, including 81,500 direct employees and 144,100 non-insurance jobs. There are 417 life insurers licensed to do business in California and 11 are domiciled in the state. California residents have \$3.7 trillion in total life insurance coverage. State residents own 10 million individual life insurance policies, with coverage averaging \$244,000 per policyholder. And \$38 billion was paid to California residents in the form of death benefits, matured endowments, policy

dividends, surrender values, and other payments in 2016 with \$8 billion in annuity benefits paid in the state in the same year.

Not only is our industry a robust contributing member of the California economy, we are proud of the fact that the financial services industry has traditionally been a conscientious and responsible guardian of customers' highly vulnerable personal information. Our industry has appropriately managed consumers' confidential medical and financial information for decades. As we mentioned at the outset, we look forward to working with you and lending our industry's historical expertise to this crucial issue.

As stated previously, while we appreciate the clarification and guidance provided by the proposed regulations, we are concerned with the complexity and overreach of some substantive provisions. The regulations should be simplified to facilitate company compliance and, more importantly, enhance consumer clarity. And, importantly, as we indicated earlier, adequate time for compliance must be provided.

Thank you, in advance, for your consideration of our comments. We would be happy to answer any questions.

Sincerely,



John Mangan
Regional Vice President, State Relations
ACLI



John Shirikian
President and CEO
ACLHIC

Message

From: John Jennings [REDACTED]
Sent: 12/6/2019 9:14:40 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments on Proposed California Consumer Privacy Act Regulations (October 11, 2019)
Attachments: IRI CCPA Regulations Comment Letter.pdf

To whom it may concern,

Please see the attached letter with the Insured Retirement Institute's comments regarding the proposed California Consumer Privacy Act Regulations. If you have any questions, please do not hesitate to contact me.

Thank you for the opportunity to provide these comments.

Best,

John B Jennings



Insured Retirement Institute

John B. Jennings
Manager, Government Affairs
Insured Retirement Institute
1100 Vermont Avenue, NW 10th Floor
Washington, DC 20005
Office: [REDACTED]
Cell: [REDACTED]
Fax: (202) 469-3030
Email: [REDACTED]



Insured Retirement Institute
1100 Vermont Avenue, NW | 10th Floor
Washington, DC 20005

t | 202.469.3000
f | 202.469.3030

www.IRionline.org
www.mylRionline.org

December 5, 2019

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

Re: *Comments on Proposed California Consumer Privacy Act Regulations (October 11, 2019)*

Dear Attorney General Becerra:

On behalf of our members, the Insured Retirement Institute ("IRI")¹ appreciates the opportunity to provide the following comments in response to your office's proposed *California Consumer Privacy Act Regulations*. IRI has long advocated for public policies aimed at providing Americans with a secured retirement. It is our belief that a portion of a secure retirement is ensuring that the sensitive financial and personal information of all Americans is properly safeguarded. As such, IRI has called for the adoption of laws and regulations providing standards for data privacy that protect the public, are compatible across jurisdictions, and minimize costs for the overall economy in our [Retirement Security Blueprint](#).

We have reviewed the comment letter being submitted to Privacy Regulations Coordinator by the American Council of Life Insurers (ACLI) and the Association of California Life and Health Insurance Companies (ACLHIC). We support and agree with the constructive comments and recommendations made by the ACLI and ACLHIC. The comments outlined in their letter will simplify industry compliance and enable greater understanding of consumers' rights.

As your office considers whether and how to revise the proposal prior to final adoption, we respectfully request that you pay particular attention to the following comments. Consumer notices should be presented in a manner that provides consumers with a transparent understanding about how their

¹ The Insured Retirement Institute (IRI) is the leading association for the entire supply chain of insured retirement strategies, including life insurers, asset managers, and distributors such as broker-dealers, banks and marketing organizations. IRI members account for more than 95 percent of annuity assets in the U.S., include the top 10 distributors of annuities ranked by assets under management, and are represented by financial professionals serving millions of Americans. IRI champions retirement security for all through leadership in advocacy, awareness, research, and the advancement of digital solutions within a collaborative industry community. Learn more at www.irionline.org.

information is collected and used. Given the diversity of businesses and their practices, being over prescriptive in the development of notices runs counter to their intended goal. Rather, the requirements should allow for an adaptable approach prioritizing information in the appropriate level of detail to properly convey the intent of the notice. Additionally, several of the provisions contained within the regulations exceed the statutory language of the enacted law. We respectfully request that the provisions contained in the final regulations are amended to ensure that they are within the scope of the *California Consumer Privacy Act*.

Thank you again for the opportunity to provide these comments. If you have questions about our views on the proposed regulations, or if we can be of any further assistance in connection to this important regulatory office, please feel free to contact me at [REDACTED] or [REDACTED]

Sincerely,

A handwritten signature in black ink, appearing to read 'Jason Berkowitz', with a stylized, elongated horizontal stroke at the end.

Jason Berkowitz
Chief Legal and Regulatory Affairs Officer
Insured Retirement Institute

Message

From: Joseph Garibyan [REDACTED]
Sent: 12/7/2019 12:51:43 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Raza Ali [REDACTED]; Steve Balian [REDACTED]
Subject: Comments on Proposed CCPA Regulations
Importance: High

To: Privacy Regulations Coordinator (Office of the California Attorney General)

On behalf of Styskal, Wiese & Melchione ("SW&M"), a law firm that provides comprehensive legal services to small and medium-sized financial institutions in the transactional, regulatory, compliance and governance practice areas, we have the following comments, questions and requests for clarification on the California Consumer Privacy Act of 2018 ("CCPA"):

1) Does the Federal Gramm-Leach-Bliley Act ("GLBA") or the California Financial Information Privacy Act ("FIPA") exemption apply to financial institutions regulated under these sectoral privacy laws, or does it only apply to personal information collected, processed, sold or disclosed under GLBA or FIPA?

The CCPA provides an exemption for "personal information collected, processed, sold, or disclosed under the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code)." The GLBA and FIPA are sectoral privacy laws that govern financial institutions subject to these laws, which includes banks and credit unions, and much of their collection, processing or disclosure of "personal information" (as defined in the CCPA) is already covered under the GLBA and FIPA.

Two interpretations may be taken from the wording of the exemption. The first interpretation is that exemption only applies if the personal information is collected, processed, sold, or disclosed under the GLBA and FIPA. Under this interpretation, the full scope of the CCPA would apply to financial institutions only in the context of their collection, processing, sale, or disclosure of personal information outside of the GLBA or FIPA framework. For collection, processing, selling, or disclosure of personal information made under GLBA and FIPA, the CCPA would apply only for Section 1798.150 of the CCPA, and none of the other CCPA consumer rights would apply in this context.

The second interpretation is that this exemption is intended to apply to the financial institutions that are regulated under the GLBA and FIPA since financial institutions are already governed by both state and federal sectoral privacy laws and regulations. A CCPA-related bill (Assembly Bill No. 1202) regarding data brokers used much clearer verbiage to carve out an exception to the financial industry: "A financial institution to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations."

Many financial institutions that we represent would like clarification about the GLBA/FIPA exemption. Does it exempt the financial industry or just the type of data they collect, process, sell or disclose under GLBA or FIPA?

2) Does the CCPA apply to credit unions?

SW&M is counsel for state and federal credit unions of all sizes throughout the country. Credit unions are a special type of financial institution. As opposed to banks, which are for-profit institutions, credit unions are, in essence, non-profit or not-for-profit financial cooperatives that are owned by their "members." Members benefit from their credit union membership through lower interest rates on loans and dividends on their shares, among other benefits of credit union membership. Credit unions, like banks, accept deposits and make loans and provide a wide array of other financial services. However, unlike banks, credit unions seek to serve their members as a primary objective rather than seeking to earn profits.

Federally chartered credit unions are tax-exempt under Section 501(c)(1) of the Internal Revenue Code ("IRC"). California state-chartered credit unions are tax-exempt under Section 501(c)(14)(A). Also, California state-chartered credit unions are formed under the Corporations Code as non-profit mutual benefit corporations.

On page 21 of the Initial Statement of Reasons (ISOR), under the discussion on service providers, the following statement was made: “This unintended and undesired consequence will lead to significant disruption in the functioning of those non-profits and governmental entities and is not in furtherance of the purposes of the CCPA, which clearly excluded non-profits and other government entities from being subject to the CCPA.” We are requesting the Attorney General to clarify this statement in the context of the following definition of “Business” under the CCPA:

“Business” means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners....”

Non-profits are not expressly referenced or excluded in the definition of “business” in the CCPA. Furthermore, the Proposed Regulations do not mention any non-profit exception. We respectfully request the Attorney General to clarify its position regarding whether non-profit organizations are exempt from the CCPA in its Final Regulations and whether the Attorney General believes credit unions are exempt by their special status as a not-for-profit or non-profit mutual benefit corporation. This clarification is needed because the phrase “or financial benefit” in the above definition of a “business” may be interpreted broadly to capture all sorts of nonprofit mutual benefit corporations, where their members or owners directly or indirectly benefit financially through membership, not just credit unions.

Additionally, concerning federal credit unions chartered under the Federal Credit Union Act, are they exempt by being an instrumentality of the United States? See Section 501(c)(1) of the IRC; See also Section 1614 of the California Code of Regulations (“Examples of incorporated federal instrumentalities exempt from tax are federal reserve banks, federal credit unions, federal land banks, and federal home loan banks”).

3) If the definitions of “Business Purpose” and “Commercial Purpose” are intended to be mutually exclusive, please provide a method to differentiate between the two definitions, particularly in the advertising and marketing context in Final Regulations.

The definition of a “Business Purpose” and “Commercial Purpose” in the CCPA are challenging to differentiate in a variety of applications, particularly advertising and marketing. If the Attorney General considers these definitions mutually exclusive, then please provide a method to differentiate between the two definitions, such as a factor-based analysis. Both definitions seem to apply equally to advertising and marketing contexts.

“Business Purpose” is defined as the “use of personal information for the business’s or service provider’s operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are: ... (5) [p]erforming services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising and marketing services, providing analytical services, or providing similar services on behalf of the business or service provider.

“Commercial Purposes” is defined as “[advancing] a person’s commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction...”

It is essential to differentiate between the two definitions in the advertising and marketing context because the definition of “sale” under the CCPA expressly excludes “[using] and [sharing] with a service provider personal information of a consumer that is necessary to perform a business purpose...” “Commercial Purpose” is not included in this exclusion. Thus, if a service provider is engaged to provide a business an advertising and marketing service, and such service is considered a “business purpose,” then the transfer of personal information to the servicer in this context will not be a “sale.” However, if the service deemed for a “commercial purpose,” then the transfer may arguably be considered a “sale” of personal information.

4) Please provide a factor-based method to determine whether “valuable consideration” is provided to establish “sale” under the CCPA.

The CCPA defines “sell,” “selling,” “sale,” or “sold,” as “selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.” Presuming that the term “consideration” in this definition is the same standard used to determine the validity of contracts, consideration is generally considered to have some economic value, which is necessary for a contract to be enforceable. California Civil Code section 1605 defines consideration as “[a]ny benefit conferred, or agreed to be conferred, upon the promisor, by any other person, to which the promisor is not lawfully entitled, or any prejudice suffered, or agreed to be suffered, by such person, other than such as he is at the time of consent lawfully bound to suffer, as an inducement to the promisor, is good consideration for a promise.” Any benefit one confers on another is enough to establish consideration for form a contract; the value of such consideration does not matter. Thus, the term “valuable” is even more ambiguous and subjective in the context of the definition of “sale” if it is used to qualify the term “consideration.”

Please consider a factor-based analysis to provide some objective framework to analyze “valuable consideration.” Furthermore, please consider placing a determinative factor in this analysis whereby if a business is paying a service provider to provide a service which requires a transfer of personal information from the business to the service provider, which is presumptively “valuable” for the business otherwise the business would not be paying for it), then the business should not be deemed to be “selling” personal information to the service provider. The business is paying the service provider, not the other way around, and the mere fact that the service provider’s services to the business is maybe “valuable” for the business should not constitute a “sale” under the CCPA.

5) Please provide guidance on “audio” information.

The definition of “personal information” in the CCPA expressly includes “audio” if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household. Consumers may leave “audio” information in a variety of interactions with financial institutions, for instance, voicemail messages left with employees to live-recorded calls with their call centers. The Proposed Regulations did not provide any guidance on handling audio information. How are notices at or before collection supposed to be provided to such consumers with all of the minimum required information required by Section 999.305(a)(2) of the Proposed Regulation? If the Attorney General requires a notice at or before collecting audio information from consumers, we suggest providing an abbreviated notice that directs consumers to the business’s privacy policy on its website.

Furthermore, are business’s expected to operationalize voicemail messages left with employees for CCPA purposes? In other words, will voicemail messages left with employees constitute a collection of personal information under the CCPA by the business? For instance, you have an individual leave a voicemail with an employee, which includes the person’s name and other identifiers that satisfy the definition of “personal information” under the CCPA. Are such employees expected to save the voicemail and/or make a record of such messages for purposes of being able to disclose the business collected that information and to provide consumers the right to know categories and specific pieces of information collected and the right to delete such information? If so, this will put an extraordinary burden on businesses to screen and record all of their calls, including employee voicemail information, which could potentially trespass into the privacy rights of employees.

Arguably, a business should not be considered to be “collecting” or “processing” (let alone “sharing” or “selling”) audio information if a consumer calls and leaves a voicemail message if the business does not retain that information for an extended period of time. We suggest that the Attorney General’s Final Regulations address this issue and state that a business should not be considered to be collecting, processing, sharing or selling personal information if the voicemail message is left with an employee and if the business deletes the voicemail message within a certain number of days (e.g., 30 days).

6) Please clarify the reference to Civil Code section 1798.105(d) in Section 999.313(d)(5) of the Proposed Regulations.

Section 999.313(d)(5) of the proposed regulations states, “[i]n responding to a request to delete, a business shall disclose that it will maintain a record of the request pursuant to Civil Code section 1798.105(d).” Section 1798.105(d) only lists the exceptions for a business or service provider’s obligation to respond to a consumer’s deletion request. It is neither the operative section for making the request to delete, which is covered under Civil Code section 1798.105(a), or maintaining

a record of the data, which is addressed in Section 999.317 of the Proposed Regulations. Therefore, the reference to Civil Code section 1798.105(d) 999.313(d)(5) of the Proposed Regulation appears to be a mistake.

7) The Attorney General should stay the disclosure required under Section 999.317(g) until January 1, 2021.

Section 999.317(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 request to opt-out that the business received, complied with in whole or in part, and denied; (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 complied in subsection (g)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy....

For all intents and purposes, even if a business has met the 4,000,000 threshold for the calendar year 2019, its Privacy Policy posted on January 1, 2020, when the CCPA takes effect, will have zero as the response to all of the metrics because consumers could not have exercised their CCPA right to information, deletion and opt-out before the CCPA took effect. It makes sense to require businesses to collect the analytical information in 2020 and post it in their Privacy Policies as of January 1, 2021.

We respectfully request the Office of the Attorney General to clarify and respond to the above-referenced questions and suggestions in its Final Regulations. As provided in CCPA, the Attorney General may adopt additional regulations as necessary to further the purposes of the CCPA. As representatives of financial institutions, SW&M respectfully requests clarification on all of the issues above, particularly but issues about the scope and application of the CCPA on banks and credit unions.

Joseph Garibyan
Senior Associate | CIPP/US, CIPM, CIPT
STYSKAL, WIESE & MELCHIONE, LLP
T: [REDACTED] | F: 818.241.5733
www.swmlp.com | [REDACTED]



NOTICE: This communication may contain privileged or other confidential information. If you are not the intended recipient, or believe that you have received this communication in error, please do not print, copy, retransmit, disseminate, or otherwise use the information contained herein. Also, please indicate to the sender that you have received this e-mail in error, and delete the copy you have received. Thank you.

Our comments are based upon the very limited information provided to us and our analysis could change in the event of different or additional information. Except as we have specifically noted and discussed above, we have not undertaken an examination of the effects on any proposed action, transaction, or agreement on other issues, including but not limited to, memberization issues, tax, actuarial, or accounting consequences, possible bankruptcy or insolvency of any party, underwriting considerations, conflicts with any other agreement to which the Financial Institution may be a party, or conflicts with any Financial Institution planned or current policy or procedure. Our comments and analysis are limited solely to those statutes, regulations, cases, or interpretive comments cited above and our understanding of them as of the date of this response. Also, we have not engaged in any due diligence, or any other research or investigation into any issue, fact, or circumstance. Given the very limited scope of our research and this assignment, this response does not constitute a formal legal opinion on this matter. We do not provide any opinion as to whether any particular action,

transaction, agreement, or program is appropriate, financially sound, or otherwise “safe and sound” for the Financial Institution, and the Financial Institution should ensure that it is relying on its own sound judgment in making its business decisions. We trust that the Financial Institution understands that we do not insure the Financial Institution’s business decisions, and that any comments, analysis, and advice from our office in no way substitutes for independent examination of facts and decision-making.

Message

From: Alan Kyle [REDACTED]
Sent: 12/7/2019 12:15:41 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Mark Kahn [REDACTED]
Subject: Comments on proposed CCPA regulations
Attachments: Segment comments on CCPA rulemaking 2019.12.06.pdf

Dear Office of the Attorney General,

Please find the attached PDF with Segment's comments regarding the Attorney General's proposed CCPA regulations.

Thank you for your consideration,

Alan Kyle



Alan P. Kyle · Privacy/Policy Analyst
he/him/his

[Integrations](#) · [Blog](#) · [We're Hiring!](#)



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

Dear Office of the Attorney General,

I represent Segment, a leading Customer Data Infrastructure company that sits at the center of thousands of company's analytics operations.

We write to you to submit public comments on the proposed CCPA regulations. We recognize the enormous task you have been given and we thank you for your work to clarify and further the CCPA's purposes. To help promote this work, we would like to raise two points (below) in the proposed regulations that we believe need clarification. In addition to these comments, Segment has submitted separate comments in association with the law offices of Gunderson Dettmer and other entities and individuals involved in technology.

Segment provides a unified view of an organization's own customer data across every channel: website, apps, payments, help desk, etc., all while respecting their customers' privacy. We do this by helping companies collect all their first-party data, the information about all their own interactions with their customers, and route it to whatever business application needs it within their organization. Using Segment, companies can innovate the customer experience more efficiently, building trusted relationships with their customers while putting their privacy first.

We are a privacy forward company that embraces and welcomes the new rights that CCPA will give Californians.

DocuSigned by:
Kind regards,

4A3AC932849A468
Mark Kahn

General Counsel and VP of Policy



1. § 999.305. Notice at Collection of Personal Information

Civil Code section 1798.100(b) and § 999.305(a)(1) state that notice must be given “at or before” collection. But later § 999.305(a)(2)(e) states that notice shall be visible or accessible “before” any personal information is collected. Which is it? If IP addresses and other online identifiers automatically collected from website use constitutes the collection of personal information, it would be impossible to give a notice before collection.

Civil Code section 1798.100 as referenced in the Initial Statement of Reasons provides no mention of a notice that is strictly “before” collection. To the extent that comparisons with GDPR are helpful, it’s worth pointing out that that GDPR Art. 13(1) only requires notice “at the time when personal data are obtained.”

We recommend that the language in § 999.305(a)(2)(e) be modified to read: “Be visible or accessible where consumers will see it **before at the time** any personal information is collected.” This language further clarifies notice obligations for online businesses while remaining applicable to offline notices.

2. § 999.308. Privacy Policy

§ 999.308(a)(3) states: “If the business has a California-specific description of consumers’ privacy rights on its website, then the privacy policy shall be included in that description.” This may be read to mean that the whole privacy policy must be included in California-specific descriptions of consumer’s privacy rights.

If this were the intended understanding, then it would be out of the CCPA’s scope. The Initial Statement of Reasons say that § 999.308(a)(3) is meant to implement and clarify where and how privacy policies are to be posted as described in Civil Code section 1798.130(a)(5), which makes no mention of the privacy policy being included in California-specific descriptions.

If this were not the intended understanding, the language should be clarified. If the intent of this proposed regulation is for the privacy policy to be accessible from the California-specific descriptions, we recommend the language state that a link to the rest of the privacy policy be required.

§ 999.308(a)(3) may be modified to read: “If the business has a California-specific description of consumers’ privacy rights on its website, *a link to the privacy policy* shall be included in that description.”

Message

From: McCarthy, Colman D. (SHB) [REDACTED]
Sent: 12/6/2019 10:30:32 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments on proposed CCPA regulations
Attachments: 2019.06.12 Comment letter on CCPA regulations.pdf

Dear Sir/Madam,

I write to submit the attached comments on the CCPA regulations. Your time and attention is very much appreciated.

Regards,

Colman D. McCarthy
Associate
Shook, Hardy & Bacon L.L.P.



CONFIDENTIALITY NOTICE: This e-mail message including attachments, if any, is intended for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message. Thank you.



December 6, 2019

Colman D. McCarthy

The Honorable Xavier Becerra
Attorney General
ATTN: Privacy Regulations Coordinator
300 South Sprint Street, First Floor
Los Angeles, CA 90013

2555 Grand Blvd.
Kansas City, Missouri 64108

t [REDACTED]
f 816.421.5547
c [REDACTED]

Re: Comments on Proposed California Consumer Privacy Act Regulations

Dear Attorney General Becerra:

We write to provide several comments on the proposed regulations under the California Consumer Privacy Act (CCPA). We applaud the dedication and effort of your office in drafting and publishing the proposed regulations, especially given the timeline and legislative activity surrounding the CCPA, and hope that these comments will help strengthen and clarify the proposed regulations.

Comment: Those proposed regulations that focus on the primary interaction with consumers should be modified to focus on the primary manner in which personal information is collected.

Analysis: The proposed regulations use the concept of primary interaction in several locations, shown below, related to methods for submitting consumer requests and to disclosure of contact information in a business's privacy policy.

999.312. Methods For Submitting Requests to Know and Requests to Delete

- 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.
 - *Example 2:* If the business operates a website but **primarily interacts with customers in person at a retail location**, the business shall offer three methods to submit requests to know—a toll-free telephone number, an interactive webform

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

999.315. Requests to Opt Out

The Honorable Xavier Becerra

- 999.315(b)
 - A business shall consider the methods by which it interacts with consumers when determining which methods consumers may use to submit requests to opt-out, the manner in which the business sells personal information to third parties, available technology, and ease of use by the average consumer. At least one method offered shall reflect the **manner in which the business primarily interacts with the consumer.**

December 6, 2019
Page 2

999.308. Privacy Policy

- 999.308(b)(6)
 - Contact for More Information: Provide consumers with a contact for questions or concerns about the business's privacy policies and practices using a method reflecting the **manner in which the business primarily interacts with the consumer.**

In addition, § 999.317(a) would require that “[a]ll 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.”

These provisions could both hinder the exercise of consumer rights and impose unreasonable costs of compliance on businesses, particularly in the retail sector. The retail industry experiences high rates of turnover¹ among store employees, who interact with consumers on a daily basis. But a retail business’s primary manner of collection of personal information may be through online means (such as through an online account), with little to no personal information collected at physical retail locations. The proposed regulations would nevertheless appear to require that the business train all store employees (even seasonal or part-time employees working only a few

¹ According to the ADP Research Institute 2019 State of the Workforce Report (available at <https://www.adp.com/resources/articles-and-insights/articles/2/2019-state-of-the-workforce-report.aspx>), the Trade/Transportation/Utilities sector, which includes retail, has the highest monthly turnover rate at 5% (which amounts to a 60% annual turnover). Other estimates, from 2018, included 65% turnover for hourly retail employees, and up to 81% turnover for part-time hourly store workers. See <https://business.dailypay.com/blog/employee-turnover-rates-in-retail> (citing National Retail Federation research); <https://www.retaildive.com/news/retailers-are-seeing-high-employee-turnover/542396/> (citing research by consulting firm Korn Ferry).

hours a week) on all requirements in the CCPA and on how to assist a consumer when filling out a form at the employee's location. This situation carries the real possibility that, though unintentionally, consumers would be hindered in exercising their rights under the CCPA.

The Honorable Xavier Becerra

December 6, 2019
Page 3

The Initial Statement of Reasons justifies the primary-interaction requirement as a way to prevent “businesses from picking obscure methods for submitting requests as a way of discouraging consumers from exercising their rights.” ISOR at 15, 24. But that justification, resting on an assumption that businesses will seek to discourage consumers, could instead lead to a situation where a consumer improperly fills out a form because an inexperienced store employee innocently gives erroneous directions, or where a form is accidentally lost before it can be forwarded to personnel who would carry out the consumer requests.

Other personnel at a business who have more relevant knowledge bases and skill sets would be better situated—even though remote from the consumer—to assist consumers than a busy cashier in a convenience store.

By focusing instead on the primary manner in which a business collects information, a business will be better positioned to provide the information and methods for requests that are required by the CCPA and the proposed regulations, and to do so at the most relevant point of the interaction with the consumer. It would be more efficient and more likely to result in the successful exercise of a consumer's rights (for both the consumer and business).

That is not to say that retail locations would somehow be exempt from compliance with the CCPA or proposed regulations. It would rather allow businesses with physical locations to direct consumers to more appropriate methods for submitting consumer requests that will more likely lead to successfully received and implemented requests.

Comment: More guidance is needed on verification when a business cannot verify a consumer's identity to the necessary degree of certainty.

Analysis: For certain businesses, it may be too difficult or resource-intensive to respond to separate tiers for the right to know. Rather, these businesses would treat each request as seeking both specific pieces of personal information and categories of personal information, and would respond with all such information. When verifying non-accountholders, these businesses would need to verify to a reasonably high degree of certainty, since specific information is involved. § 999.325(c). But if the business cannot verify the consumer's identity to that degree of certainty, its next actions are unclear under the proposed regulations. While Section 999.313(c)(1) directs businesses to consider a request for specific pieces of information as a request

for categories of personal information, that would force the business into the same process of separating out the request that may have been too difficult in the first instance. Other possible options appear to be continuing to request additional information (§ 999.323(c)) or directing the consumer to the business's privacy policy (§ 999.313(c)(2)). Additional guidance on this process would be welcome.

The Honorable Xavier Becerra

December 6, 2019
Page 4

Comment: The proposed regulations should clarify that there is no violation where online assets or online means for receiving consumer requests are temporarily unavailable.

Analysis: Numerous proposed regulations require online disclosures or the use of webforms as a method by which consumers may submit requests. For example:

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

- 999.306(b)(1)
 - 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.
- 999.306(c)(2)
 - A business shall include the following in its notice of right to opt out: . . . (2) The **webform** by which the consumer can submit their request to opt out online[.]

999.308. Privacy Policy

- 999.308(a)(3)
 - The privacy policy shall be posted **online** through a conspicuous link using the word “privacy,” on the business's **website homepage** or on the download or landing page of a **mobile application**.

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

- 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**. 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.

999.315. Requests to Opt Out

- 999.315(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**.

The Honorable Xavier Becerra

December 6, 2019
Page 5

No online asset (such as websites or mobile applications) can possibly be available 100% of the time. Any number of reasons can result in downtime when an online asset is unavailable to a consumer attempting to access a business’s disclosures or to submit a consumer request, such as an interruption in power to the hosting server, routine maintenance, or some malfunction in a consumer’s device or browser. But the proposed regulations, as currently drafted, do not acknowledge this fact.

It would be unreasonable to expect 100% availability, and the proposed regulations should clarify that temporary interruptions in the availability of online assets or online means for receiving consumer requests are not violations of the CCPA or the proposed regulations.

Comment: The proposed regulations should clarify that “do not track” signals are not “user-enabled privacy controls.”

Analysis: Under the proposed regulations, businesses would be required to treat “user-enabled privacy controls” as valid opt-out requests:

999.315. Requests to Opt out

- 999.315(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.

That provision could be read to apply to “do not track” signals as a “privacy setting or other mechanism.” But, as has been widely documented, there is no standard implementation and the vast majority of websites do not respond to “do not track” signals. The website All About Do Not Track itself acknowledges there is no consensus on “do not track” signals, and lists only nine websites that have committed to implementing “do not track.”² And the

² <https://allaboutdnt.com/>.

W3C Working Group that worked for eight years to develop a standard for “do not track” finally abandoned the effort in January 2019.³

The Honorable Xavier Becerra

December 6, 2019
Page 6

While the Initial Statement of Reasons justifies this treatment of user-enabled controls as preventing businesses from rejecting or ignoring consumer tools, it also acknowledges the subdivision “is intended to support innovation for privacy services that facilitate the exercise of consumer rights in furtherance of the purposes of the CCPA.” ISOR at 24. Requiring compliance with a moribund standard that never enjoyed consensus would not support innovation in privacy services. Rather “do not track” is “an extra piece of information about [consumers] that can be tracked . . . and misleads people just by existing.”⁴ The proposed regulations should therefore make clear that “do not track” signals are not “user-enabled privacy controls.”

Comment: The proposed regulations should provide guidance on what proof businesses may require from authorized agents.

Analysis: When addressing requirements related to authorized agents, the proposed regulations allow a business to require that such agents have “written permission” from the consumer where a power of attorney is not present. § 999.326(a)(1). And a business may deny a request if the agent does not “submit proof” of authorization. § 999.326(c). But no further guidance is provided, either in the proposed regulations or the Initial Statement of Reasons. *See* ISOR at 33-34.

To protect both consumers and businesses against fraud by individuals or entities claiming authorization, the need for some way to confirm the validity of the written permission is apparent.⁵ Further guidance, or examples of the “proof” a business may permissibly require (notarization, for example), would be welcome.

Additional clarity would also be welcome in the case of a power of attorney. It is unclear to what extent a business may require an authorized agent to provide proof of the power of attorney, and what a business may do or require in order to confirm the validity of that power of attorney. *See* § 999.326(b)-(c).

³ <https://www.w3.org/TR/tracking-dnt/>; <https://www.w3.org/TR/2011/WD-tracking-dnt-20111114/> (first working draft from 2011).

⁴ Chris Hoffman, *RIP “Do Not Track,” the Privacy Standard Everyone Ignored*, HOW-TO-GEEK, February 7, 2019, available at <https://www.howtogeek.com/fyi/rip-do-not-track-the-privacy-standard-everyone-ignored/>.

⁵ Even though the proposed regulations also allow businesses to require a consumer to separately verify her identity, that does not eliminate the potential for fraud.

Comment: The regulations should add provisions under § 999.313(d) or § 999.314 to clarify the obligations of service providers when a business passes along a deletion request under § 1798.105(c) of the CCPA.

The Honorable Xavier Becerra

December 6, 2019
Page 7

Analysis: Under § 1798.105(c) of the CCPA a business that receives a verifiable request to delete from a consumer must “direct any service providers to delete the consumer’s personal information from their records.” And while the proposed regulations provide additional direction that a business must notify third parties to which it has sold personal information (§ 999.315(f)), there is no further guidance where requests to delete are involved. For instance, it is not clear whether a service provider’s obligation to delete personal information extends only to that personal information received from the business that received the consumer request.

The provisions should also address the extent to which a service provider may 1) separately verify the identity of the consumer and confirm her wish to delete her personal information, or 2) rely on the business that received to request for the necessary verification and confirmation. It would seem that allowing service providers to rely on the business receiving the request would be preferable, for two reasons. First, it would reduce the burden on the consumer to verify and confirm on multiple occasions with separate entities with which she may have no familiarity. And second, it would help protect consumers against individuals and entities fraudulently posing as service providers requesting verification.

But on the other hand there is a concern that the consumer may be unaware of the affiliation between the two entities, and therefore unaware of consequences for the deletion of her personal information, such as unintended loss of benefits under a loyalty program. This would counsel in favor of allowing service providers to at the least provide notice to consumers of the potential consequences of deleting personal information.

We appreciate your consideration of these comments, and look forward to seeing the regulations in final form.

Sincerely,



Colman D. McCarthy

Message

From: Mike Stinson [REDACTED]
Sent: 12/6/2019 6:15:37 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments on Proposed CCPA Regulations
Attachments: MPL Assn Comments on Proposed CCPA Regulation.pdf

Attached, please find formal comments from the Medical Professional Liability Association regarding the proposed regulations for the California Consumer Privacy Act.

Should you have any questions, or need additional information, please do not hesitate to contact me.

Michael C. Stinson, JM

Vice President of Government Relations & Public Policy



MEDICAL PROFESSIONAL
LIABILITY ASSOCIATION

2275 Research Blvd., Suite 250
Rockville, MD 20850

Direct: [REDACTED]

Cell: [REDACTED]

www.MPLassociation.org

Don't miss the MPL Association's spring meetings and workshops—professional development and networking opportunities across the medical liability insurance spectrum. [Learn more and register now!](#)



**MEDICAL PROFESSIONAL
LIABILITY ASSOCIATION**

December 6, 2019

The Honorable Xavier Becerra
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

ATTN: Privacy Regulations Coordinator

Subject: Comments on Proposed CA Consumer Privacy Act Regulation

Dear Attorney General Becerra:

On behalf of the Medical Professional Liability Association and our medical professional liability (MPL) insurers that conduct business in California, I would like to thank you for giving us the opportunity to share our perspective on the potential impact of the proposed California Consumer Privacy Act (CCPA) Regulations on the MPL insurance industry.

The Medical Professional Liability Association ("MPL Association") is the leading trade association representing insurance companies, risk retention groups, captives, trusts, and other entities owned and/or operated by their policyholders, as well as other insurance carriers with a substantial commitment to the MPL line. MPL Association members insure more than 2 million healthcare professionals worldwide—doctors, nurses and nurse practitioners, and other healthcare providers—including more than two thirds of America's private practice physicians. MPL Association members also insure more than 150,000 dentists and oral surgeons, 2,500 hospitals and 8,000 medical facilities around the world.

The MPL Association supports the adoption of consumer data privacy measures that enhance transparency and data protections related to consumers' personal information without restricting its member companies' ability to use consumer data that is necessary to conduct a full range of insurance services to its insureds. While the draft regulations clearly attempt to strike this balance, we would like to draw your attention to some aspects of the regulation which are still of concern to our industry.

To begin, Section 999.313, Subsection (d) of the draft regulation stipulates how businesses must respond to consumer requests for the deletion of personal information. Paragraph 2 provides a business with options for complying with a request to delete, including an option to "permanently and completely erase the personal information on its existing systems *with the exception of archived or back-up systems.*" Paragraph 3, however, appears to require a business to require an entity to delete personal information stored on archived or backup systems when the archived or backup system is next accessed or used. These paragraphs seem to contradict

one another with respect to a business' obligations related to archived personal information. Given the "long-tail" nature of MPL insurance, you can understand how important it is for our members to be able to access historical data on claims. As such, we recommend modifying paragraph 3 to clarify that it only applies when an entity *voluntarily* chooses to delete archived or backup system information following a consumer request. This would maintain the intent of paragraph 2 while still clarifying the timeframe in which companies that choose to delete historical data choose to do so.

Relatedly, while the CCPA provides exceptions from the requirement for a business to delete consumer information, our members are concerned that several of the exceptions rely on the consumer's interpretation of how the data may be used. Given that all individuals who interact with an MPL insurer may not be aware of all the relevant uses of the information they provide during the claims process, and the need to access that information even after a claim is resolved, we believe clarification would be beneficial. As such, we advise adding to the draft Regulation, pursuant to your authority under section 1798.185(b) of the CCPA, to clarify when an entity may not be required to delete consumer data. Specifically, we recommend that the regulation explain that Section 1798.105(d)(9) applies to the lawful, internal use of data by an entity so long as the entity has explained to the consumer how the data may be used at the time it is provided. Otherwise, as applied to an MPL insurer, Section 1798.105(d)(9) currently could be interpreted to apply only to the "context" of a claimant's specific case, thus denying insurers the ability to retain data necessary for long-term underwriting and risk management purposes. With the clarification requested above, consumer data would still be protected as intended, but insurers could be sure of their ability to maintain historical data necessary for their ongoing business functions.

In closing, the MPL Association appreciates this opportunity to provide input regarding the proposed California Consumer Privacy Act Regulations. Please do not hesitate to contact me at [REDACTED] should you need any further information.

Sincerely,

A handwritten signature in blue ink that reads "B. K. Atchinson". The signature is fluid and cursive, with the first name and last name clearly legible.

Brian K. Atchinson
President & CEO

Message

From: Mark Webb [REDACTED]
Sent: 12/7/2019 1:01:29 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments on Proposed CCPA Regulations
Attachments: CCPA DOJ Comments.pdf

See attached.

Thank you,

Mark Webb

"As the Workmen's Compensation, Insurance and Safety Act has proved to be beneficial, humane, and just, and has wholly justified its enactment in all features, it should receive full constitutional sanction." – Senator Edgar A. Luce (1918) Proposition 23 Ballot Statement.



Prop 23 Advisors
Analysis • Answers • Advocacy

Mark Webb, Owner
790 East Colorado Blvd., 9th Floor
PMB #691
Pasadena, CA 91101
[REDACTED]

<https://www.proposition23workerscomp.com>

DECEMBER 6, 2019

COMMENTS ON PROPOSED DEPARTMENT OF JUSTICE REGULATIONS

IMPLEMENTING THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018

PROPOSITION 23 ADVISORS

Mark Webb, Owner

790 East Colorado Blvd., 9th Floor

PMB #691

Pasadena, CA 91101

markwebb@proposition23workerscomp.com

Thank you for the opportunity to comment on proposed regulations implementing the California Consumer Privacy Act of 2018 (“CCPA”). By way of introduction, Prop 23 Advisors was formed in 2016 to provide compliance consultation services to small and medium sized businesses and to support research and advocacy efforts on workers’ compensation issues throughout the United States. Proposition 23 is the 1918 ballot measure which ratified the Workmen’s Compensation Insurance and Safety Act of 1917 upon which the current California workers’ compensation system is based.

The following comments are intended to address limited issues regarding California’s workers’ compensation system. These comments are not intended to conflict with or otherwise question comments from undoubtedly a wide range of groups on provisions not directly addressed herein.

The requested changes in the proposed regulations are modest in comparison with the length of this document. Regrettably, in over two years of the legislative process, the question of application of the CCPA to the highly regulated and highly complicated workers’ compensation system will given little if any attention. To the extent efforts were made to clarify the application of the CCPA to the insurance industry, particularly Assembly Bill 981 (Daly), such efforts become bogged down in the muck of disinterest and, to a degree, misinformation on the scope of privacy protections insurers are already providing.

Thank you in advance for your consideration of these comments.

I. Introduction.

As stated in Government Code § 11342.2, “Whenever by the express or implied terms of any statute a state agency has authority to adopt regulations to implement, interpret, make specific or otherwise carry out the provisions of the statute, no regulation adopted is valid or effective unless consistent and not in conflict with the statute and reasonably necessary to effectuate the purpose of the statute.”

The CCPA grants almost unprecedented regulatory powers to the Department of Justice. This extends beyond the initial implementation and contemplates an ongoing relationship with consumers and the business community commensurate with the challenges that are to come as technology becomes even more advanced. Because of this broad grant, it is difficult to argue that any of the provisions in the proposed regulations exceed the authority granted in Civil Code § 1798.185.

But authority is not the sole criterion by which regulations are evaluated by the Office of Administrative Law (OAL). In the particular case of the CCPA and the workers’ compensation claims administration community, the urgent issue is clarity. [See: Government Code § 11349(c), Civil Code § 1798.185(a)(6)]

II. Background on the Workers’ Compensation System.

The authority for California’s workers’ compensation system rests in Article XIV, § 4 of the California Constitution. This provision of the Constitution states, in part:

“The Legislature is hereby expressly vested with plenary power, unlimited by any provision of this Constitution, to create, and enforce a complete system of workers’ compensation, by appropriate legislation, and in that behalf to create and enforce a liability on the part of any or all persons to compensate any or all of their workers for injury or disability, and their dependents for death incurred or sustained by the said

workers in the course of their employment, irrespective of the fault of any party.”
(emphasis added)

In *Stevens v. Workers' Comp. Appeals Bd.* (2015), 241 Cal.App.4th 1074, 194 Cal.Rptr.3d 469, the Court of Appeal was confronted with a challenge to the constitutionality of recently enacted provisions regarding independent medical review (IMR) of denials by claim administrators of requests for authorization of medical treatment. The challenge was based both on separation of powers and due process. The Court rejected these arguments and, looking to the history of California's workers' compensation laws and concluded:

“This evolution compels the conclusion that Section 4 supersedes the state Constitution's due process clause with respect to legislation passed under the Legislature's plenary powers over the workers' compensation system... Thus, even if there were any conflicts between Section 4 and the state Constitution's separation of powers or due process clauses—a conclusion we do not and need not reach—the plenary powers conferred by Section 4 would still control.” 241 Cal.App.4th 1093

Central to the Court's analysis was that Proposition 23 was proposed by the Legislature for the 1918 ballot, “...to remove all doubts as to the constitutionality” of the workers' compensation laws. *Stevens* at 1093. It was adopted by the voters subsequent to the due process and separation of powers provisions already existing in the Constitution. In 1972, voters approved Proposition 11, a measure placed on the ballot by the Legislature to add the right of privacy to the Declaration of Rights in Article I, § 1 of the California Constitution. As noted in the legislative finds which are part of Assembly Bill 375 (Chau), the original CCPA legislation from 2018:

“Since California voters approved the right of privacy, the California Legislature has adopted specific mechanisms to safeguard Californians' privacy, including the Online Privacy Protection Act, the Privacy Rights for California Minors in the Digital World Act, and Shine the Light, a California law intended to give Californians the ‘who, what, where, and when’ of how businesses handle consumers' personal information.”

Proposition 11 was not self-executing. It contained no mandate to the Legislature to act, especially in regard to private business.

For a comprehensive treatment of this issue see: J. Clark Kelso, *California's Constitutional Right to Privacy*, 19 Pepp. L. Rev. 2 (1992), available at: <http://digitalcommons.pepperdine.edu/plr/vol19/iss2/1>

Thus, we are left with a Constitutional provision in the right to privacy that required years of legislative activity to define for purposes of private business – an ongoing process – and a far earlier provision in the Constitution relating to workers' compensation that confers upon the Legislature “plenary power” unlimited by any provisions in the Constitution. This should compel a deference to the workers' compensation laws adopted by the Legislature and the regulations promulgated under this plenary authority when considering the scope of the regulations implementing the CCPA.

This is not to suggest that there is a conflict *per se* with the proposed regulations and existing statutes, regulations, and court decisions regarding workers' compensation. It is to suggest, however, that to the extent these regulations could alter the fundamental flow of information, the notices required of employers to be provided to injured workers, or the disruption of the information necessary to

underwrite workers' compensation insurance, such regulations must be scrutinized in light of the Legislature's plenary power to create a workers' compensation system in all its aspects.

A.

**THERE ARE CONSIDERABLE PROVISIONS IN BOTH STATUTE AND REGULATIONS PRESERVING
PRIVACY RIGHTS FOR INJURED WORKERS**

As reported in Bloomberg on February 25, 2019, California Senate Judiciary Chair Hannah-Beth Jackson (D-Santa Barbara) said, "The tech industry, by its very nature, has been very much opposed to any form of regulation," she said in an interview about the CCPA. "It's an industry that's reincarnated the Wild West; no rules, no limits, no regulation. We've reached the tipping point."

That may well be the case for the industry that appears to be the focal point of the CCPA. But that is not the case when it comes to the protection of personal information in California's highly regulated workers' compensation system. As can be expected, when it relates to the claims for benefits by injured workers much of the personal information necessary to adjust a claim is submitted either to the Division of Workers' Compensation (DWC) or to the Workers' Compensation Appeals Board (WCAB). These are public entities and as such outside the scope of the CCPA. In terms of protecting personal information submitted to the DWC, Labor Code § 138.7 states:

"...a person or public or private entity not a party to a claim for workers' compensation benefits shall not obtain individually identifiable information obtained or maintained by the division on that claim. For purposes of this section, 'individually identifiable information' means any data concerning an injury or claim that is linked to a uniquely identifiable employee, employer, claims administrator, or any other person or entity."

There are necessary exceptions to that rule, but it is unlawful for any person who has received individually identifiable information from the DWC pursuant to this section to provide that information to any person who is not entitled to it under this section. (See also: 8 CCR § 9703)

Labor Code § 3762, subdivision (c), relating to the permissible disclosures by an insurer or claims administrator to an insured policyholder or to a self-insured employer states:

"An insurer, third-party administrator retained by a self-insured employer pursuant to Section 3702.1 to administer the employer's workers' compensation claims, and those employees and agents specified by a self-insured employer to administer the employer's workers' compensation claims, are prohibited from disclosing or causing to be disclosed to an employer, any medical information, as defined in Section 56.05 of the Civil Code, about an employee who has filed a workers' compensation claim, except as follows:

- (1) Medical information limited to the diagnosis of the mental or physical condition for which workers' compensation is claimed and the treatment provided for this condition.
- (2) Medical information regarding the injury for which workers' compensation is claimed that is necessary for the employer to have in order for the employer to modify the employee's work duties."

When implementing electronic billing procedures by medical providers, Labor Code § 4603.4 states that billing standards developed by the (DWC, "...shall be consistent with existing standards under the federal Health Insurance Portability and Accountability Act of 1996." [Labor Code § 4603.4(b)]

Labor Code § 4610.5, subdivision (m), states that when a claims administrator is transmitting medical records pursuant to a request for independent medical review, "The confidentiality of medical records shall be maintained pursuant to applicable state and federal laws." [See also: 8 CCR § 9792.10.5(d)]

Confidentiality of medical information was also a consideration in Labor Code § 4903.6, subdivision (d):

"With the exception of a lien for services provided by a physician as defined in Section 3209.3, a lien claimant shall not be entitled to any medical information, as defined in subdivision (g) of Section 56.05 of the Civil Code, about an injured worker without prior written approval of the appeals board. Any order authorizing disclosure of medical information to a lien claimant other than a physician shall specify the information to be provided to the lien claimant and include a finding that the information is relevant to the proof of the matter for which the information is sought."

The privacy protections within the Labor Code primarily address protection of medical information. This extends to regulations. See also: 8 CCR §§ 10608 and 10754 relating to sealing of documents containing confidential medical or other information by the Workers' Compensation Appeals Board (WCAB).

In addition, the form an injured worker is required to fill out per Labor Code § 5401, the DWC-1, contains the following language:

"After you make a claim for workers' compensation benefits, your medical records will not have the same level of privacy that you usually expect. If you don't agree to voluntarily release medical records, a workers' compensation judge may decide what records will be released. If you request privacy, the judge may "seal" (keep private) certain medical records."

The data reporting required to the Workers' Compensation Information System (WCIS) requires reporting of an injured workers' Social Security Number (SSN) if known. (See: 8 CCR § 9702) This information is kept confidential, in part, per Labor Code § 138.7. Regulations of the WCAB relating to the filing of an application for adjudication, 8 CCR § 10400(h), also state:

"Disclosure of the applicant's Social Security number is voluntary, not mandatory. A failure to provide a Social Security number will not have any adverse consequences. Nevertheless, although an applicant is not required by law to provide a Social Security number, he or she is encouraged to do so. Social Security numbers are used solely for identification and verification purposes in order to administer the workers' compensation system. A Social Security number will not be disclosed, made available, or otherwise used for purposes other than those specified, except with the consent of the applicant, or as permitted or required by statute, regulation, or judicial order."

During the routine administration of a workers' compensation claim, especially a claim involving indemnity (wage replacement and permanent disability) benefits, considerable personal information is collected and disclosed regarding injured workers and various providers of services. The personal

information collected from an injured worker, however, is generally not, *if ever*, subject to the CCPA per the provisions of Civil Code §§ 1798.145(e) relating to claimant information subject to the Gramm-Leach-Bliley Act (GLBA) and implementing regulations (See: 16 C.F.R. § 313(n), 16 C.F.R. § 313(o), and 10 CCR §§ 2689.1 *et seq.*), and the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code). For employers, Civil Code 1798.145(h)(1) relating to employee personal information clarifies that information necessary to collect and disclose regarding a workplace injury is also not subject to the CCPA except for the provisions of Civil Code §§ 1798.100(b) and 1798.150. The protection of personal information by licensees of the Department of Insurance is set forth in the “safeguards” rule under GLBA (16 C.F.R Part 314) and the Department of Insurance Privacy Regulations, 10 CCR §§ 2689.12 *et seq.*

Physicians, other healthcare providers, copy service businesses, interpreters, transportation service providers, lawyers, and other individuals or entities under contract with a business (which may be an employer, a claims administrator, or an insurer) may provide personal information in the ordinary course of business for purposes including contract administration, payment and remittance, or compliance with applicable sanctions laws, such as sanctions administered by the Office of Foreign Assets Control (OFAC). This personal information of these “consumers” would be subject to the “contract” exception in Civil Code § 1798.145(h)(1).

An employer is obligated to provide medical treatment to cure and relieve the effects of an injury arising out of and in the course of employment, make temporary disability payments while the injured worker is going through the healing process and, once the worker’s condition is permanent and stationary, provide permanent disability benefits to compensate for the effects of the worker’s impairment. While in most cases an injured worker will receive treatment from a physician under contract with the employer (or employer’s insurer or claims administrator), that is not always the case. In such situations, the claims administrator is nevertheless obligated to make payments to the provider generally as set forth in Labor Code § 4603.2. Payments to most providers is set forth either by contract or the Official Medical Fee Schedule (OMFS) authorized in Labor Code § 5307.1. If there is a dispute over a bill, payments subject to contract or fee schedules are resolved through independent bill review (IBR) in Labor Code § 4603.6.

Furthermore, there will be occasions where the worker disputes various decisions by the employer and will seek representation by counsel. The worker may also use the process established in the Labor Code and administered by the DWC to obtain an opinion from a qualified or agreed medical evaluator (QME or AME) on issues such as whether the injury arose out of employment, the nature and extent of permanent disability, or the need for future medical care. A worker may also seek the assistance of an interpreter or a transportation service, or the worker or the worker’s attorney may use a copy service for document preparation. The providers of these services are not under contract with the employer, but the employer is required by law to pay or reimburse the worker for such charges. Some of these services are paid for on what is called a lien basis, following the procedures in Labor Code §§ 4903 *et seq.* Liens are filed with the WCAB and subject to the Board’s policies and procedures.

As complex as this system is, it has served employers and workers well for over a century. For purposes of this rule making proceeding, it is hoped that the Department will look at the workers’ compensation system, recognize that its provisions are, “...an expression of the police power and are intended to make effective and apply to a complete system of workers’ compensation the provisions of Section 4 of Article

XIV of the California Constitution”, and consider regulations that are entirely consistent with the CCPA but will make more clear its application in this highly regulated environment.

Requested regulatory amendments:

(1) It is recommended that the Department adopt a definition of “excepted personal information”. In so doing, it will be clearer to consumers what their rights are under the CCPA and will not seek to limit the necessary disclosures of information a consumer – whether an injured worker or an individual providing services – required under the Labor Code for the system to function properly.

For example, in proposed 11 CCR § 999.313(c)(5), the Department states:

“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. If the request is denied only in part, the business shall disclose the other information sought by the consumer.”

It would seem preferable for a consumer to know in the notice at collection, where applicable, that certain personal information is not subject to the rights granted under the CCPA. Where a notice at collection is not required of a business, then the distinction between personal information subject to the CCPA and personal information excepted from it should be clearly stated in the privacy policy. In other words, a consumer should not find out that its personal information is not subject to the CCPA only once being told by a business that it cannot honor the consumer’s request to know or request to delete.

(2) The proposed regulations relating to “service providers” would seem to lack the clarity necessary under Government Code § 11349. Proposed 11 CCR § 999.314(a) is contrary to the environment created in the CCPA where a “business” as defined in Civil Code § 1798.140(c) discloses personal information to a service provider:

“...pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.”

The proposed regulation states, “To the extent that a person or entity provides services to a person or organization that is not a business, 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.” What constitutes “would otherwise meet the requirements” of a service provider? Does this mean that the entity disclosing the personal information who is not a “business” has a contract with the entity receiving that information who is not a “service provider” that would meet the requirements in Civil Code § 1798.140(v) and if it does the entity providing the service falls within the CCPA?

This would appear to conflate the concepts of a business and a service provider at least as it relates to obligations under the CCPA. This is particularly a concern when considering the application of Civil Code

§ 1798.155 to service providers where the entity providing the personal information is not similarly subject to the CCPA. It is recommended that subdivision (a) be deleted.

B.

THE PLENARY AUTHORITY OF THE LEGISLATURE EXTENDS TO INSURANCE COVERAGE FOR WORKERS' COMPENSATION OBLIGATIONS

Article XIV, § 4 of the California Constitution also grants plenary authority to the Legislature to make, "...full provision for adequate insurance coverage against liability to pay or furnish compensation; (and) full provision for regulating such insurance coverage in all its aspects, including the establishment and management of a state compensation insurance fund."

While it might border on axiomatic that an insurance company is a "business" as defined in Civil Code § 1798.140(c), that would be an incorrect assumption. One of the largest insurers in California, and indeed the nation, is the State Compensation Insurance Fund (SCIF). SCIF is a division of the Department of Industrial Relations (Labor Code § 56) and is organized as a public enterprise fund. (Insurance Code § 11773) It is intended to be no more or less than self-supporting. (Insurance Code § 11775) As such, it is not a for-profit enterprise falling within the definition of a "business" for purposes of the CCPA.

The fact that one of the largest writers of workers' compensation insurance in California is *not* a "business" under the CCPA is important for purposes of this rule making process because of the proposed regulations governing "service providers" in 11 CCR § 999.314.

The process for placement of workers' compensation insurance involving brokers, employers, and insurers, is a critical function in a competitive insurance marketplace. Given the broad definition of "consumer", personal information is collected when an insurer is asked to write a policy for a sole proprietor. In addition, to comply with the requirements of Senate Bill 189 (Bradford) regarding exemptions from the workers' compensation system, a "consumer" – natural persons who are residents of California – will need to disclose personal information to an insurer. Additional personal information may be collected regarding contact individuals of the insured.

Most, if not all, of the personal information obtained by an insurer from an insured or a prospective insured, will be excepted from the CCPA by operation of Civil Code §§ 1798.145(h) and 1798.145(n).

Requested Regulatory Amendments:

Insurers, as noted above, are regulated by the California Department of Insurance. Regulations under the Gramm-Leach-Bliley Act and the California Insurance Information and Privacy Protection Act (IIPPA), Insurance Code §§ 791 *et seq.*, require specific notices of information practices. (See: Insurance Code § 791.04; 10 CCR § 2689.5)

Civil Code § 1798.130(a)(5) states, "Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its internet website, and update that information at least once every 12 months:"

Without going into great detail, the required notice from the Department of Insurance and the required notice in the CCPA do not apply co-extensively. As noted in Civil Code § 1798.145(e), the personal

information subject to the Department of Insurance regulations is *excepted* from all provisions of the CCPA other than the penalty provisions of Civil Code § 1798.150. Trying to merge these notices into a single privacy policy would be at best confusing.

It is recommended that the regulations provide that a business subject to the privacy regulations of the California Department of Insurance in Title 10, Code of California Regulations, Subchapter 5.9 may post a separate privacy notice on its website in the form and manner as required by the Department's regulations advising consumers of their rights under the CCPA.

Appendix

Proposed Amendments¹

(1) Add 11 CCR § 999.301(i)

“Excepted personal information” means personal information not subject to the requirements of the CCPA except as otherwise set forth in the applicable provisions of Civil Code § 1798.145.

(2) Amend 11 CCR § 999.301(g), to read:

“Financial incentive” means a program, benefit, or other offering, including payments to consumers as compensation, for the disclosure, deletion, or sale of personal information. Financial incentive does not include a discount in the cost of insurance based upon the use of personal information necessary for the application of rating plans subject to filing and approval, or filing and use, for any insurance subject to regulation by the Insurance Commissioner under applicable provisions of the Insurance Code.

(3) Amend 11 CCR § 999.301(o), to read:

“Request to delete” means a consumer request that a business delete personal information, other than excepted personal information, about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105.

(4) Amend 11 CCR § 999.301(p), to read:

“Request to opt-out” means a consumer request that a business not sell the consumer’s personal information, other than excepted personal information, to third parties, pursuant to Civil Code section 1798.120(a).

(5) Amend 11 CCR § 999.301(q), to read:

“Request to opt-in” means the affirmative authorization that the business may sell personal information, other than excepted personal information, about the consumer required by Civil Code section 1798.120(c) by a parent or guardian of a consumer less than 13 years of age, or by a consumer who had previously opted out of the sale of their personal information.

(6) Add 11 CCR § 999.301(r), to read:

“Service provider” as defined in Civil Code § 1798.140(v) does not include a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes excepted personal information on behalf of a business.

¹ For sake of brevity, there are not conforming (renumbering) amendments included in definitions list



(7) Amend 11 CCR § 999.305, subdivision (b), to read:

A business shall include the following in its notice at collection:

- (1) A list of the categories of personal information about consumers subject to the CCPA 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. The notice shall inform the consumer about excepted personal information that is collected but is not subject to the CCPA.
- (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.

(8) Amend 11 CCR § 999.308, to read:

(a) Purpose and General Principles

- (1) The purpose of the privacy policy is to provide the consumer with a comprehensive description of a business’s online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information. The privacy policy shall inform consumers of the categories of personal information excepted from the CCPA and how it may affect their rights under the CCPA. The privacy policy shall not contain specific pieces of personal information about individual consumers and need not be personalized for each consumer.
- (2) The privacy policy shall be designed and presented in a way that is easy to read and understandable to an average consumer. The notice shall:
 - a. Use plain, straightforward language and avoid technical or legal jargon.
 - b. Use a format that makes the policy readable, including on smaller screens, if applicable.
 - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.
 - d. Be accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the policy in an alternative format.
 - e. Be available in an additional format that allows a consumer to print it out as a separate document.

(3) The privacy policy shall be posted online through a conspicuous link using the word “privacy,” on the business’s website homepage or on the download or landing page of a mobile application. If the business has a California-specific description of consumers’ privacy rights on its website, then the privacy policy shall be included in that description. A business that does not operate a website shall make the privacy policy conspicuously available to consumers.

(b) The privacy policy shall include the following information:

(1) Right to Know About Personal Information Collected, Disclosed, or Sold

a. Explain that a consumer has the right to request that the business disclose what personal information it collects, uses, discloses, and sells.

b. Provide instructions for submitting a verifiable consumer request to know and provide links to an online request form or portal for making the request, if offered by the business.

c. Describe the process the business will use to verify the consumer request, including any information the consumer must provide.

d. Collection of Personal Information

1. List the categories of consumers’ personal information the business has collected about consumers in the preceding 12 months. The notice shall be written in a manner that provides consumers a meaningful understanding of the information being collected.

2. 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 with whom the business shares personal information. The notice shall be written in a manner that provides consumers a meaningful understanding of the categories listed.

e. Disclosure or Sale of Personal Information

1. State whether or not the business has disclosed or sold any personal information to third parties for a business or commercial purpose in the preceding 12 months.

2. List the categories of personal information, if any, that it disclosed or sold to third parties for a business or commercial purpose in the preceding 12 months.

3. State whether or not the business sells the personal information of minors under 16 years of age without affirmative authorization.

(2) Right to Request Deletion of Personal Information

a. Explain that the consumer has a right to request the deletion of their personal information collected or maintained by the business.

- b. Provide instructions for submitting a verifiable consumer request to delete and provide links to an online request form or portal for making the request, if offered by the business.
- c. Describe the process the business will use to verify the consumer request, including any information the consumer must provide.

(3) Right to Opt-Out of the Sale of Personal Information

- a. Explain that the consumer has a right to opt-out of the sale of their personal information by a business.
- b. Include the contents of the notice of right to opt-out or a link to it in accordance with section 999.306.

(4) Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights

- a. Explain that the consumer has a right not to receive discriminatory treatment by the business for the exercise of the privacy rights conferred by the CCPA.

(5) Authorized Agent

- a. Explain how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf.

(6) Contact for More Information: Provide consumers with a contact for questions or concerns about the business's privacy policies and practices using a method reflecting the manner in which the business primarily interacts with the consumer.

(7) Date the privacy policy was last updated.

(8) If subject to the requirements set forth section 999.317(g), the information compiled in section 999.317(g)(1) or a link to it.

(9) A business subject to the privacy regulations of the California Department of Insurance in Title 10, Code of California Regulations, Subchapter 5.9 may post a separate privacy notice on its website in the form and manner as required by this Section advising consumers of their rights under the CCPA.

(9) Amend 11 CCR § 999.314, to read:

- ~~(a) To the extent that a person or entity provides services to a person or organization that is not a business, 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.~~
- ~~(b) To the extent that a business directs a person or entity to collect personal information directly from a consumer on the business's behalf, and would otherwise meet all other 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.

~~(e)~~ (b) 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.

~~(d)~~ (c) 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, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial. The service provider shall also inform the consumer that it should submit the request directly to the business on whose behalf the service provider processes the information and, when feasible, provide the consumer with contact information for that business.

~~(e)~~ (d) A service provider that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider.

Message

From: Lance Noggle [REDACTED]
Sent: 12/6/2019 6:58:57 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments on Proposed Regulations Concerning the California Consumer Privacy Act (CCPA)
Attachments: CCPA CUNA Final.pdf

Lance Noggle
Senior Director of Advocacy and Senior Counsel for Payments and Cybersecurity
Credit Union National Association, Inc.
99 M Street SE
Suite 300
Washington, D.C. 20003
Direct: [REDACTED]



WASHINGTON, D.C.
99 M Street SE
Suite 300
Washington, D.C. 20003-3799
Phone: [REDACTED]
Fax: [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: Comments on Proposed Regulations Concerning the California Consumer Privacy Act (CCPA)

Dear Sir or Madam:

The Credit Union National Association (CUNA) appreciates the opportunity to submit comments to the California Office of the Attorney General in response to the request for comment regarding proposed regulations for the California Consumer Privacy Act (CCPA). CUNA is a national trade association representing America's credit unions and their 115 million members.

Credit unions are cooperatively owned and democratically controlled financial institutions focused on serving members and their community. All federally-insured state-chartered and federally-chartered credit unions are subject to the the Gramm-Leach-Bliley Act (GLBA) of 1999's privacy and data security requirements. For credit unions, implementing regulations for GLBA have been issued by the Consumer Financial Protection Bureau for privacy and the National Credit Union Administration for data security. GLBA has provided Americans with robust privacy and data security protections for their information held at credit unions and banks.

CUNA supports robust privacy and data security protections for all Americans, and we support the protections that CCPA provides California residents. Nonetheless, we seek clarity in these rules so credit unions across the country can properly comply with the requirements, even when they do not operate in California and/or have very few members in California.

Definition of a “Business”

The definition of business needs further clarification. California Civil Code section 1798.140, subdivision (c)(1) defines business as 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.....”

Not-for-profit organizations operate under 501(c) of the Internal Revenue Code. Federal credit unions are tax exempt under section 501(c)(1) and state credit unions are tax exempt under section 501(c)(14) of the Internal Revenue Code. Because of credit unions’ not-for-profit status, there has been confusion whether they meet the definition of a business. Although not-for-profit, credit unions operate for the “financial benefit of [their] shareholders or other owners,” credit unions’ unique organization and tax status make additional clarity in the definition of a business necessary.

Credit unions also seek additional guidance on the “doing business in California” requirements. The vast majority of credit unions are located outside of California and likely do not seek to serve California residents. As a way to avoid doing business in California, a credit union could choose not to open an account for a California resident but cannot close the account of a member that subsequently moves to California. Some businesses with few customers in California may elect not to serve customers who live in the state, but credit unions cannot easily do this as they, by law, cannot close member share accounts without a vote of the membership of the credit union – a process that is involved and impractical for this purpose.

A company should be allowed to serve a de minimis number of California residents without meeting the “doing business in California” requirements to allow for isolated instances where a business, such as a credit union, must provide services to California residents by law, yet does not seek to market itself in California or open accounts for California residents.

GLBA Exemptions

There is significant confusion regarding the exemption for personal information collected, processed, sold, or disclosed pursuant to the federal GLBA or the California Financial Information Privacy Act (CFIPA). The confusion arises because the CCPA uses terms that are inconsistent with the GLBA and CFIPA. The GLBA and CFIPA both use the term “nonpublic personal information” and define that term to mean “personally identifiable financial information.” The CCPA uses the term “personal information,” which is defined in Calif. Civil Code 1798.145(o) and is broader than the GLBA’s definition of “nonpublic personal information.”

GLBA personally identifiable financial information is information collected in the course of a transaction or providing a financial product or service, while the CCPA pertains to personal information collected through every channel for nearly every reason. The result of these inconsistent definitions is that the financial services industry must segregate data and treat information differently. The Attorney General should clarify the GLBA exemption and the treatment of data in the regulations.

Model Notices

The Attorney General should adopt model notices that satisfy the notice requirements of the CCPA and proposed regulations. These notices include the “Notice at or Before Collection,” “Right to Opt-Out,” “Notice of Financial Incentives,” and updated Privacy Notices. Included in these model notices should be model responses to “Requests to Know” and “Requests to Delete.” Model notices are provided by federal regulators to meet GLBA’s notification requirements and they have worked well by ensuring consumers receive clear and consistent notices from financial institutions. Furthermore, financial institutions can rely on the proper use of model notices to ensure they are satisfying the requirements of the regulations.

The Attorney General should propose model notices for public comment and provide a safe harbor in the final regulations for the use of notices substantially similar to the model notices.

Notice at Collection

Proposed section 999.305(a)(3) requires the business to directly notify the consumer of a new use and obtain “explicit consent” from the consumer to use their personal information for this new purpose. The statute does not require an opt-in. We recommend replacing this requirement with a new notice to the consumer along with a 30-day opportunity to opt-out.

Privacy Policy

The proposed regulations require that additional information be provided in the privacy policy that is not required by the statute. The proposed regulations require the business to describe the process it will use to verify the consumer’s request, including any information the consumer must provide in the “Right to Know” and the “Right to Request Delete” disclosure. Describing the process the business will use to verify the consumer’s request adds an additional burden, adds little value to the consumer, and complicates the disclosure. The regulations should only require disclosure of the information consumers must provide for the business to verify their request.

Responses to “Request to Delete” and “Requests to Opt-In After Opting Out”

The two-step process for responding to proposed section 999.312(d) Request to Delete and proposed section 999.316(a) Requests to Opt-In After Opting Out is unnecessary and needlessly complex. The regulation’s requirement that a consumer must clearly submit the “Request to Delete” and then separately confirm that the consumer wants her personal information deleted are unnecessary. A one step process should be sufficient to ascertain intent and eliminate mistakes by both parties that could come from a two-step process.

Responding to “Requests to Know” and “Requests to Delete”

Upon receiving a section 999.313(a) “Request to Know” or a “Request to Delete,” the proposed regulations require a business to:

- Confirm receipt of the request within 10 days;
- Provide information about how the business will process the request;

- Describe the business's verification process; and
- Provide when the consumer should expect a response, except in instances where the business has already granted or denied the request.

This response is not required by statute and is not necessary. The response required by statute is sufficient.

Response Time

Proposed section 999.313(b) requires a business to respond to "Requests to Know" and "Requests to Delete" within 45 days. The proposed regulations permit an additional 45 days to respond, for a maximum of 90 days. The statute allows up to 90 additional days where necessary, taking into account the complexity and number of the requests, Calif. Civil Code 1798.145(g)(1). We recommend the regulations allow the 90-day extension.

Requests to Opt-Out

The proposed regulation 999.315(e) requires a business to act upon a request to opt-out as soon as feasibly possible, but no later than 15 days from the date the business receives the request. This adds a response timing obligation that is not specified in the original statute and is more prescriptive than the federal GLBA requirements. CUNA, for consistency purposes, requests that the regulations follow the GLBA regulations at 12 CFR 1016.7(g) which state, "You must comply with a consumer's opt out direction as soon as reasonably practicable after you receive it."

Effective Date

The effective date of the CCPA should be extended to a reasonable date after the Attorney General publishes the final regulations. The CCPA is effective January 1, 2020; however, the proposed implementing regulations were not issued until October 11, 2019, and comments are not due until December 6, 2020. We believe extending the effective date is reasonable to comply with a complex and entirely new privacy regulations that requires businesses to implement many new processes. CUNA recommends the Attorney General and Governor delay the effective date by two years, until Jan. 1, 2022.

Enforcement

The CCPA provides that the Attorney General can bring enforcement actions six months after publication of the final regulations or July 1, 2020, whichever is sooner. Enforcement by the Attorney General, along with the effective date, should be delayed a reasonable amount of time so that businesses have enough time to comply with the regulations.

Should you have any questions about CUNA's comments, please feel free to contact me at

[REDACTED]

Sincerely,

A handwritten signature in cursive script that reads "Lance Noggle".

Lance Noggle

Senior Director of Advocacy and Counsel Senior Counsel for Payments and Cybersecurity

Message

From: Scott Buchanan [REDACTED]
Sent: 12/6/2019 7:10:18 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments on proposed regulations for the CCPA
Attachments: SLSA CCPAFinalComment 12-6-2019 FINAL.pdf

Attached are the Student Loan Servicing Alliance's comments on Rulemaking adopting sections §§ 999.300 through 999.341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations, which create regulations implementing the CCPA.

Respectfully submitted,

C. Tapscott Buchanan
Executive Director
Student Loan Servicing Alliance
1100 Connecticut Avenue, NW
Suite 1200
Washington, DC 20036
(202)955-6055 (o)
[REDACTED] (c)
[REDACTED]



Student Loan Servicing Alliance
1100 Connecticut Avenue, NW
Suite 1200
Washington, DC 20036



December 6, 2019

VIA EMAIL: PrivacyRegulations@doj.ca.gov

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

Re: Comments on Rulemaking adopting sections §§ 999.300 through 999.341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations

The Student Loan Servicing Alliance ("SLSA") appreciates the opportunity to provide feedback on California's proposed rule making adopting sections §§ 999.300 through 999.341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations. SLSA is a non-profit trade association that represents federal and private student loan servicers, who collectively service over 90% of all student loans in the country.

We have previously provided comments on similar matters regarding the CCPA that we hope continue to be considered and are aware that many industry and trade associations will provide broader comments on areas of concern or potential improvement for provisions that will impact financial services companies and their providers or partners. Further, many of our members may be exempt from this statute and rulemaking, but some may not be today or in the future. Therefore, we will focus our comments on areas that specifically may impact student loan servicers and our ability to effectively and practically comply with the proposed regulations in a way that is beneficial to consumers if applicable. Below are several general comments worth considering for clarification or additional guidance, followed by comments and suggested changes related to specific provisions:

- Many of the disclosure requirements provided for in the regulations are ones that align with or may be similar to disclosures required by the federal Gramm-Leach-Bliley Act (GLBA). In an effort to reduce duplicative or confusing communication and disclosure to borrowers, we believe that GLBA disclosures may often be an appropriate disclosure vehicle to add any additional disclosures required by these regulations. It would be useful for the regulation or sub-regulatory guidance to make clear that separate and discrete disclosure notification is not necessary, as long as the GLBA required notice itself also includes all items applicable or required by the CCPA regulations. We believe

this is appropriate and consistent with the regulation as proposed, but making that ability to consolidate disclosures for a consumer clear would be useful.

- Unlike some other products - such as mortgages - student loans are products that “travel” with a consumer when they change residency and move in and out of a state. This means a lender and their servicer do not necessarily control the state regulations and timing of applicability of regulations governing data and interaction with that consumer. Further, California’s regulations may differ in specific and meaningful ways, both today and in the future, from other state regulations which we must comply with when the consumer is a resident of that state. Therefore, it is important to clarify that the regulations can only be applicable to consumers who are current residents of the state and in regard to information collected or maintained during that period of residency. Clarifying the population impacted and the time period in scope in guidance would be useful to ensure that we can also clearly communicate this to the consumer when asked, despite it being relatively clear that jurisdiction only exists during the period of residency and for data collected or maintained during residency.
- §999.314(c) – This provision contains the permissible, but not required, ability to “combine” personal information. For many businesses, including servicers, this creates challenges with contractual and legal data security requirements dictated by business clients (usually holders of the loans or lenders) that expressly prohibit such use of their data for other shared purposes. Therefore, while many businesses may not choose to do so or may be contractually unable, it may be useful to more fully clarify that what is being suggested is merely a separate data-matching or validation effort, rather than actual combination of data which suggests co-mingling of accounts and data in physically or logically separated systems of record across business clients.
- §999.325(d) – This section seeks to clarify the utilization of various standards of certainty of identity verification for purposes of requesting data deletion, which is useful to allow businesses to have more flexible options for lower “sensitivity” or “risk of harm” data for the consumer. We support the concept of allowing for flexible standards but believe that clarification that good faith efforts be defined as consistent and equitable treatment of such requests against a standard that has a reasonable basis as determined by the business. Consumers may dramatically differ in what they view as relatively more sensitive, and the safe harbor here should be consistent treatment based upon a reasonable assessment by the business.

Beyond those broad considerations, below are several specific comments and recommendations to improve the Final Rule:

Responding to Requests to Know and Requests to Delete - §999.313 (a) through (c) – This provision clearly is designed to provide a consumer with transparency about the status of their requests and provide them reasonable and timely updates and responses to those inquiries. We believe this is an important matter to address and support the requirement’s goal. In fact, we believe an ability to quickly respond to these requests with minimal extra communication is beneficial to the consumer as well as the business. Timely and consolidated response better ensure a consumer understands the outcome of the request while also reducing costs to a

business for compliance. Therefore, we suggest that the rule make clear that businesses are permitted to meet compliance with both subsections (a) and (b) of this provision if they can meet the requirements of (b) in the notice required by (a). While this may not always be the case due to the need for additional research, for many simple requests they may be able to be fully responded to within the time period of the origination confirmation receipt. Therefore, we are merely asking for clarification that these do not need to necessarily be separate responses if both can be accomplished and communicated in one response prior to the 10-day requirement of subsection (a)

SLSA recommends the following changes to the proposed Rule:

§ 999.313

(a) Upon receiving a request to know or a request to delete, a business shall confirm receipt of the request within 10 days and provide information about how the business will process the request. The information provided shall describe the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request. If the business is able to fully respond to the request or deny the request due to inability to verify prior to this confirmation, such notification may be included in this confirmation request and sufficiently meet both this notification requirement and that of subsection (b).

(b) Businesses shall respond to requests to know and requests to delete within 45 days. The 45day 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 days to respond to the consumer's request, for a maximum total of 90 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 days to respond to the request

Training; Record-Keeping - §999.317 (g) – SLSA has concerns with this provision, not only in terms of its arbitrary applicability but also the lack of any material value to consumers since the disclosures by different types of businesses with different products and services will inevitably lead to comparisons that may be substantively misleading. First of all, it is unclear how it was determined that a business that has more than 4,000,000 million consumers should be required to provide public information on aggregate statistics. Why 4MM is the appropriate trigger versus 10MM or 200,000 consumers is unclear and, on its face, appears to be an arbitrary threshold. But more importantly, we should turn to the question of consumer value. Regardless of who should disclose, these metrics do little to provide any insight into the comparative responsiveness of a business to other businesses. For example, simply requiring numerical counts of requests doesn't give any context to the size of the consumer base of the business or the level of complexity of its customer relationships. The latter of which is critical in timeliness of response. For example, student loan servicers are handling accounts that often have multiple loans for a single consumer, more than 10 years or repayment history and transaction history, and product complexity mandated by contract or law that exists in almost no other financial product. Therefore, comparing an unqualified metric of mean response time

about a simple consumer line of credit versus a student loan reveals little – or at least an unknowable amount – about the relative effort or consumer support of those businesses. If the goal is transparency to inform consumers about relative performance, then these metrics do not accomplish that. In fact, quite possibly the data will be inappropriately used to make incorrect comparisons since none of the product, consumer, or business complexity is revealed in these simple and unqualified metrics.

SLSA recommends the following changes to the proposed Rule:

§ 409.8 Servicing standards.

(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.

Requests to Access or Delete Household Information - § 999.318 –. While this provision is likely constructed to provide additional consolidation of information and requests on some data, services, and products that may be considered by some to be household accounts, rather than individual consumer-specific, it does pose significant risks and potentially may create additional privacy concerns. Consumer financial products, unless explicitly shared in joint and severable responsibility under the loan contract, are inherently individual products and consumers reasonably expect privacy about their individual contracts regardless of their household situation. Creating a new regime that attempts to treat multiple individual accounts as joint accounts outside of the contractual arrangements is very concerning. Further, existing and available legal methods exist to address the same goal. Consumers may provide legal power of attorney to others in their households or may otherwise designate explicitly to a business an individual who may also access this information. Those existing processes address

the potential goals of this provision and as such, this provision is unnecessary and potentially very risky to implement if privacy protection is the ultimate goal.

SLSA recommends the following changes to the proposed Rule:

§ 999.318. Requests to Access or Delete Household Information

(a) Where a consumer does not have a password-protected account with a business, a business may respond to a request to know or request to delete as it pertains to household personal information by providing aggregate household information, subject to verification requirements set forth in Article 4.

(b) If all consumers of the household jointly request access to specific pieces of information for the household or the deletion of household personal information, and the business can individually verify all the members of the household subject to verification requirements set forth in Article 4, then the business shall comply with the request.

Verification for Password-Protected Accounts - § 999.324 (a) – SLSA agrees with the goal of ensuring that access to accounts online is integral to privacy and protections for borrowers. Our members have deployed multiple and various methods and practices to ensure access, including IP monitoring, two-factor authentication, or other sophisticated means to protect access and password integrity. Those are essential steps all financial services companies and service providers must take today. However, requiring re-authentication before disclosing the consumer’s data would inherently interfere with a student loan servicer’s business and degrade consumer experience in those web interfaces. Requiring someone to reauthenticate in a consumer financial services product experience de facto means that each login and authentication would immediately require a reauthentication, since the entire point of account access through a website is to do only one thing: disclose to the consumer information about their personal data and loan status. Further, the requirement would do little if anything to reduce unauthorized access. If an account is being improperly accessed then that means the unauthorized accessor has the authentication information in hand, and reauthentication is therefore no new barrier to their continued access and deletion of consumer information. Further, most financial services companies and businesses control the ability to handle such functions through the website for the very reason that we always wish to control inadvertent deletion. At best this provision offers little benefit to a consumer’s privacy or data integrity, and at worst it creates an experience that is both cumbersome and a barrier to a consumer easily accessing their account information.

SLSA recommends the following changes to the proposed Rule:

§ 999.324. Verification for Password-Protected Accounts

(a) If a business maintains a password-protected account with the consumer, the business may verify the consumer’s identity through the business’s existing authentication practices for the consumer’s account, provided that the business follows the requirements in section 999.323. The business shall also require a consumer to re-authenticate themselves before disclosing or deleting the consumer’s data.

We thank you for the opportunity to provide our industry expertise, and if you would like to discuss the comments provided, please contact me at [REDACTED] or [REDACTED].

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'C. Tapscott Buchanan'. The signature is stylized with a large 'C' and a long horizontal stroke at the end.

C. Tapscott Buchanan
Executive Director

Message

From: Ryan Marlow [REDACTED]
Sent: 12/6/2019 4:59:09 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments on Proposed Regulations re: CCPA
Attachments: Comments_On_Proposed_Regulations.pdf

Please find the attached letter. Thank you for your attention and consideration in these matters.

—
Ryan Marlow

Director of Technology

Envoy Media Group, Inc.
[REDACTED] [REDACTED]



The Honorable Xavier Becerra
Attorney General
ATTN: Privacy Regulations Coordinator
300 South Spring Street, First Floor
Los Angeles, CA 90013

6 December 2019

Comments on Proposed Regulations

Dear Mr. Becerra,

I write to you on behalf of Envoy Media Group, Inc., a Los Angeles area company with over a decade of online business experience. I have some concerns regarding the California Consumer Privacy Act and the proposed regulations regarding the collection of Internet Protocol addresses (IP addresses) and their categorization as "personal information". I believe this is unnecessary and creates unintended detrimental effects for businesses. Consider the following from AB-375:

- 1798.135. (a) A business that is required to [...] (1) Provide a clear and conspicuous link on the business' Internet homepage, titled "Do Not Sell My Personal Information"
- 1798.140. (l) "Homepage" means [...] any Internet Web page where personal information is collected
- 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.
- 1798.140. (o) Personal information includes [...] Identifiers such as [...] Internet Protocol address
- 1798.140. (x) "Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to [...] an Internet Protocol address

These points seem to indicate that IP addresses qualify as personal information and therefore that any webpage where IP addresses are collected must include a "Do Not Sell My Personal Information" link. Also, if treated as personal information, any records of IP addresses must be included within the consumer's Right To Access and Right To Opt-Out. Given the above, my concerns are twofold.

First, IP addresses are not a viable means of identifying a consumer or household. IP addresses by design are not a permanent fixed identifier of a particular device or person. From "IP 101: The Basics of IP Addresses":

"[Your IP address is] not really yours. Even at home it can change if you do something as simple as turn your modem or router on and off. Plus, if you go on vacation and take along your laptop, your home IP address doesn't go with you. It can't, because on vacation you'll be using another network to connect to the Internet. So, when you're at a coffee shop in another city or state (or just down the road) and you're using their WiFi to get your email, you're using a different (and temporary) IP address, one assigned to your laptop on the fly by the ISP for that coffee shop's Internet provider. Same thing happens when you travel. As you move from the airport to your hotel to the local coffee house, your IP address will change each and every time." [1]

This inconsistency is borne out statistically when analyzing real data. For example, using our own customer database with a sample size of over 140,000 consumers, I can compare the self-reported names and ZIP codes of consumers against the names and ZIP codes identified using the free, publicly available WHOIS database of IP address ownership. Using this method, 95% of these IP addresses are listed as owned by a major telecom company or are of unknown ownership, and the ZIP code matches the consumer's self-reported zip code in less than 1% of the cases. I could instead choose to use a paid data matching service such as MaxMind, a major IP address geolocation database. Using this database with the same sample, the ZIP code found based on the IP address still matches the self-reported ZIP code only 22% of the time. These results fall far short of being able to identify a particular consumer or household.

Second, the treatment of IP addresses as "personal information" places undue burdens on businesses with regard to both their customer-facing websites and their digital services infrastructure. IP addresses are sent automatically in every packet of information exchanged over the Internet. This information passes through every layer of hardware and software between the origin of a web page request and its destination, including telecom backbones, local network hardware, content distribution networks, firewalls, proxies, and every piece of the server and software infrastructure that a business uses to respond to such a request. These components are owned and maintained by a large number of different organizations throughout the lifecycle of a request. Many of these components, both those fully controlled by a particular business and those outside its control, routinely store this information as part of normal operations. The purposes for this storage are acknowledged, and protected from a consumer's request to delete their data, in 1798.105. (d):

- (1) Complete the transaction for which the "personal information" was collected
- (2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity
- (3) Debug to identify and repair errors


Though protected against deletion, the classification of IP addresses as "personal information" would seem to require a business to gather and provide needlessly exhaustive detail of every aspect of the electronic communication process covering a dizzying variety of businesses, purposes, and methods when responding to a consumer's request to access their information. Also, since IP addresses are always automatically sent with a request and are passively received and stored by service infrastructure, this would seem to indicate that every webpage - even a blank screen or a 404 Not Found error page - would qualify as a "homepage" and would therefore require a "Do Not Sell My Personal Information" link and a data collection disclosure. This cannot be the intent of the law, however this interpretation does appear to follow from the law as currently written.

In sum, IP addresses fail to identify particular consumers or households, and they create undue burdens for businesses both in the gathering of consumer data to respond to access requests and in the overbroad

requirements for opt-outs and disclosures on every webpage. For these reasons, I believe that IP addresses should not be treated as "personal information" under the CCPA, and that the proposed regulations should be amended to clarify that the passive storage of IP addresses does not constitute collection of personal data.

Thank you for your consideration in this matter. If any further information or discussion would be helpful, I am at your service.

Sincerely,

A handwritten signature in black ink that reads "Ryan Marlow". The script is cursive and fluid, with the first name "Ryan" and last name "Marlow" clearly legible.

Ryan Marlow
Director of Technology, Envoy Media Group, Inc.

[1] IP 101: The Basics of IP Addresses (<https://whatismyipaddress.com/ip-basics>)

Message

From: Joe Scalone [REDACTED]
Sent: 12/7/2019 12:10:09 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments on the CCPA
Attachments: CCPA Privacy Tabula Rasa.docx

Privacy Regulations Coordinator

Please accept the following (also attached) comments on the proposed CCPA regulations.

Many thanks

Joe Scalone

Privacy Proficient

info@PrivacyProficient.com

JD, CIPP/US, CIPP/E, CIPT, CIPM



Privacy Proficient Study Network: <http://www.privacyproficient.com/privacy-proficient-study-network/>

Privacy Proficient Blog: [Privacy topics on the Privacy Proficient blog](#)

Privacy Proficient Instagram: <https://www.instagram.com/privacyproficient/>

Privacy Proficient Twitter: <https://twitter.com/Privacycient>

Privacy Proficient Facebook: <https://www.facebook.com/PrivacyProficient>

Privacy Proficient YouTube: <https://www.youtube.com/channel/UC3zI-YsJtWCm1nHZZa4L4wQ>

CCPA Privacy Tabula Rasa

The CCPA will automatically opt-out many consumers, creating a privacy tabula rasa, or clean slate for consumers to start over with businesses not otherwise in compliance.

Businesses that sell personal information, but don't have an updated web site and privacy policy with the appropriate opt-out notices will have to broadly stop using all Personal Information of all Consumers from whom they collect any additional personal information after December 31st, 2019. It will happen suddenly starting on January 1st, 2020 as soon as consumers visit web sites, receive advertising or get emails and will create a "privacy tabula rasa" – cleaning the privacy slate, giving personal information control to consumers and allowing them to start over with businesses who are not in compliance.

The regulation says:

"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." CCPA Proposed Regs § 999.306 (d)

This deemed opt-out appears to be a global opt-out of for all personal information (and not just some personal information) for all consumers for which any additional personal information is collected before the notice is posted, which will be true for many, if not most businesses. Collecting even one piece of personal information from a consumer after 2019 will trigger the deemed opt-out.

A global opt-out must be the most prominently presented opt-out option, so it follows that a deemed out without specificity would be global.

"§ 999.315. Requests to Opt-Out ... (d) 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 as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices." CCPA Proposed Regs § 999.315 (d)

This interpretation seems reasonable given that the regulation must be construed liberally in favor of its purposes (e.g., protecting consumer privacy).

"1798.194. This title shall be liberally construed to effectuate its purposes." CCPA § 1798.194

Starting on the morning of January 1st, 2020, there will be a massive amount of violations because "collecting" personal information is defined very broadly ("by any means" "either actively or passively") and business will continue to do so, many unknowingly.

"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.' CCPA § 1798.140 (e)

Because the definition of personal information is extremely broad, many businesses will probably collect personal information on consumers without even realizing it.

'Cal. Civ. Code § 1798.140 (o) (1) "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. ...'
Cal. Civ. Code § 1798.140 (o)

Personal information includes cookies, IP addresses, and advertising and marketing meta-data. Consumers that are exposed to a business' web site or any of the business' advertising, through use of the internet, email, apps or otherwise will have had personal information collected by such businesses, instantly triggering the deemed opt-out.

Personal information includes any inferences drawn from any other personal information to create a profile (such as for marketing or used in real-time bidding advertising), including any assumptions or conclusions derived from the personal information.

"1798.140 ... (o) (1) (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes...." CCPA § 1798.140 (o) (1) (K)

'1798.140 ... (m) "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data' CCPA § 1798.140 (m)

Personal information also includes behavioral characteristics (because it includes biometrics), such as how a person clicks-through or otherwise interacts with a web site. The combined scope

of personal information and inferences from behavior would, among other things, include use of personal information for advertising or marketing, even analytics and the use of artificial intelligence such as deep learning on the data.

"CCPA § 1798.140 (o) (1) (e) ... 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: ... (E) Biometric information." CCPA § 1798.140 (o) (1) (e)

'CCPA § 1798.140 ... (b) "Biometric information" means an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information....'" CCPA § 1798.140 (b)

The opt-out must be respected for 12 months and businesses are prohibited from requesting that consumers opt back in.

"1798.135. (a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:

(5) For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information." CCPA § 1798.135 (a) (5)

In the mean-time, those businesses cannot use any of the personal information for any purpose other than opt-out. Any other use will have to cease. The statute says the personal information can be used "solely for the purposes of complying with the opt-out request". Among other things, the businesses will have to stop direct marketing to those consumers. Arguably, businesses would also have to stop otherwise delivering products or services to the affected consumers except as part of a transaction.

"1798.135. (a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:

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

If the personal information has been already deidentified or aggregated, then the deidentified or aggregated form of it can be used ("collect, use, retain, sell, or disclose"). However, after the moment of deemed opt-out, personal information cannot be used to create deidentified or aggregate information.

"§ 1798.145 (a) (5) ... The obligations imposed on businesses by this title shall not restrict a business' ability to: ... Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information." [Note it does not say "create" deidentified information] Cal. Civ. Code § 1798.145 (a) (5)

The affected businesses will have only a few days to “act” – to stop using all personal information for those consumers.

“§ 999.315. Requests to Opt-Out ... (e) Upon receiving a request to opt-out, a business shall act upon the request as soon as feasibly possible, but no later than 15 days from the date the business receives the request.” CCPA Proposed Regs § 999.315 (e)

The affected businesses will have to notify all third parties not to sell any of the personal information of any of the consumers, and then notify the consumers themselves. Perhaps the only practical way to identify and notify these consumers would be to reverse engineer the advertising mechanisms and present notices (“You have opted out”) instead of ads after an initial ad is displayed (collecting their personal information and triggering the opt-out).

“§ 999.315. Requests to Opt-Out ... (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.” CCPA Proposed Regs § 999.315 (f)

Businesses will have the limited ability to inform consumers of the possibility of opting back in where there is a transaction that requires the sale of personal information as a condition of completing the transaction.

“§ 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. (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.” CCPA Proposed Regs § 999.316 (a), (b)

Otherwise, the affected businesses will have to start over with those consumers, not using their personal information until they each decide to opt back in on their own or wait 12 months to recontact them.

The privacy tabula rasa will probably apply to many businesses outside of California that don’t even suspect that the CCPA applies to them. The applicability of the CCPA pivots on the definition of “business”.

“1798.140. For purposes of this title: ... (c) “Business” means: (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers’ personal information, or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

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

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

(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information. ..." CCPA § 1798.140 (c)

Note that the definition includes businesses that "... [a]lone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices." (emphasis added). Because it says "alone or in combination", the numbers of consumers must be added to the numbers of households and the numbers of devices.

A household means a person or group of people occupying a single dwelling. Assuming that most Californians live in dwellings, then each consumer counts for two, not one – the consumer and the household. This means that it would only take the personal information of 25,000 to trigger the CCPA.

1798.301 (h) "Household" means a person or group of people occupying a single dwelling'

Devices also must be added in. Many people use multiple devices – cell phones, laptops, tablets, desk tops, digital assistant speakers, televisions, cars, thermostats, door bells, etc. If the average Consumer used 3 devices, that would bring the triggering number down to about 8,000. Don't forget about work computers. While there is an employee exemption to the CCPA, it applies "... solely within the context..." of an employee's "...role". CCPA § 1798.145 (h). Arguably a work machine used by an employee to visit a social network or other personal web site would be outside the employee's role, and thus counted in the number of devices. Consequently, the real number of items from which person information is collected to trigger the CCPA is far fewer than 50,000 Consumers.

To avoid the privacy tabula rasa, businesses would be wise to update their web site and privacy policy to adjust for opt-out notices per CCPA § 1798.120, § 1798.135 and CCPA Proposed Regs § 999.306 and § 999.315.

CCPA Privacy Tabula Rasa

The CCPA will automatically opt-out many consumers, creating a privacy tabula rasa, or clean slate for consumers to start over with businesses not otherwise in compliance.

Businesses that sell personal information, but don't have an updated web site and privacy policy with the appropriate opt-out notices will have to broadly stop using all Personal Information of all Consumers from whom they collect any additional personal information after December 31st, 2019. It will happen suddenly starting on January 1st, 2020 as soon as consumers visit web sites, receive advertising or get emails and will create a "privacy tabula rasa" – cleaning the privacy slate, giving personal information control to consumers and allowing them to start over with businesses who are not in compliance.

The regulation says:

"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." CCPA Proposed Regs § 999.306 (d)

This deemed opt-out appears to be a global opt-out of for all personal information (and not just some personal information) for all consumers for which any additional personal information is collected before the notice is posted, which will be true for many, if not most businesses. Collecting even one piece of personal information from a consumer after 2019 will trigger the deemed opt-out.

A global opt-out must be the most prominently presented opt-out option, so it follows that a deemed out without specificity would be global.

"§ 999.315. Requests to Opt-Out ... (d) 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 as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices." CCPA Proposed Regs § 999.315 (d)

This interpretation seems reasonable given that the regulation must be construed liberally in favor of its purposes (e.g., protecting consumer privacy).

"1798.194. This title shall be liberally construed to effectuate its purposes."
CCPA § 1798.194

Starting on the morning of January 1st, 2020, there will be a massive amount of violations because "collecting" personal information is defined very broadly ("by any means" "either actively or passively") and business will continue to do so, many unknowingly.

“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.’ CCPA § 1798.140 (e)

Because the definition of personal information is extremely broad, many businesses will probably collect personal information on consumers without even realizing it.

‘Cal. Civ. Code § 1798.140 (o) (1) “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. ...’ Cal. Civ. Code § 1798.140 (o)

Personal information includes cookies, IP addresses, and advertising and marketing meta-data. Consumers that are exposed to a business’ web site or any of the business’ advertising, through use of the internet, email, apps or otherwise will have had personal information collected by such businesses, instantly triggering the deemed opt-out.

Personal information includes any inferences drawn from any other personal information to create a profile (such as for marketing or used in real-time bidding advertising), including any assumptions or conclusions derived from the personal information.

“1798.140 ... (o) (1) (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes....” CCPA § 1798.140 (o) (1) (K)

‘1798.140 ... (m) “Infer” or “inference” means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data’ CCPA § 1798.140 (m)

Personal information also includes behavioral characteristics (because it includes biometrics), such as how a person clicks-through or otherwise interacts with a web site. The combined scope of personal information and inferences from behavior would, among other things, include use of personal information for advertising or marketing, even analytics and the use of artificial intelligence such as deep learning on the data.

“CCPA § 1798.140 (o) (1) (e) ... 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: ... (E) Biometric information.” CCPA § 1798.140 (o) (1) (e)

'CCPA § 1798.140 ... (b) "Biometric information" means an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information....'" CCPA § 1798.140 (b)

The opt-out must be respected for 12 months and businesses are prohibited from requesting that consumers opt back in.

"1798.135. (a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:
(5) For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information." CCPA § 1798.135 (a) (5)

In the mean-time, those businesses cannot use any of the personal information for any purpose other than opt-out. Any other use will have to cease. The statute says the personal information can be used "solely for the purposes of complying with the opt-out request". Among other things, the businesses will have to stop direct marketing to those consumers. Arguably, businesses would also have to stop otherwise delivering products or services to the affected consumers except as part of a transaction.

"1798.135. (a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:
(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request."

If the personal information has been already deidentified or aggregated, then the deidentified or aggregated form of it can be used ("collect, use, retain, sell, or disclose"). However, after the moment of deemed opt-out, personal information cannot be used to create deidentified or aggregate information.

"§ 1798.145 (a) (5) ... The obligations imposed on businesses by this title shall not restrict a business' ability to: ... Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information." [Note it does not say "create" deidentified information] Cal. Civ. Code § 1798.145 (a) (5)

The affected businesses will have only a few days to "act" – to stop using all personal information for those consumers.

"§ 999.315. Requests to Opt-Out ... (e) Upon receiving a request to opt-out, a business shall act upon the request as soon as feasibly possible, but no later than 15 days from the date the business receives the request." CCPA Proposed Regs § 999.315 (e)

The affected businesses will have to notify all third parties not to sell any of the personal information of any of the consumers, and then notify the consumers themselves. Perhaps the only practical way to identify and notify these consumers would be to reverse engineer the advertising mechanisms and present notices ("You have opted out") instead of ads after an initial ad is displayed (collecting their personal information and triggering the opt-out).

"§ 999.315. Requests to Opt-Out ... (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." CCPA Proposed Regs § 999.315 (f)

Businesses will have the limited ability to inform consumers of the possibility of opting back in where there is a transaction that requires the sale of personal information as a condition of completing the transaction.

"§ 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. (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." CCPA Proposed Regs § 999.316 (a), (b)

Otherwise, the affected businesses will have to start over with those consumers, not using their personal information until they each decide to opt back in on their own or wait 12 months to recontact them.

The privacy tabula rasa will probably apply to many businesses outside of California that don't even suspect that the CCPA applies to them. The applicability of the CCPA pivots on the definition of "business".

"1798.140. For purposes of this title: ... (c) "Business" means: (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does

business in the State of California, and that satisfies one or more of the following thresholds:

- (A) Has annual gross revenues in excess of twenty-five million dollars (\$25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.
- (B) Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.
- (C) Derives 50 percent or more of its annual revenues from selling consumers' personal information. ..." CCPA § 1798.140 (c)

Note that the definition includes businesses that "... [a]lone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices." (emphasis added). Because it says "alone or in combination", the numbers of consumers must be added to the numbers of households and the numbers of devices.

A household means a person or group of people occupying a single dwelling. Assuming that most Californian's live in dwellings, then each consumer counts for two, not one – the consumer and the household. This means that it would only take the personal information of 25,000 to trigger the CCPA.

1798.301 (h) "'Household" means a person or group of people occupying a single dwelling'

Devices also must be added in. Many people use multiple devices – cell phones, laptops, tablets, desk tops, digital assistant speakers, televisions, cars, thermostats, door bells, etc. If the average Consumer used 3 devices, that would bring the triggering number down to about 8,000. Don't forget about work computers. While there is an employee exemption to the CCPA, it applies "... solely within the context..." of an employee's "...role". CCPA § 1798.145 (h). Arguably a work machine used by an employee to visit a social network or other personal web site would be outside the employee's role, and thus counted in the number of devices. Consequently, the real number of items from which person information is collected to trigger the CCPA is far fewer than 50,000 Consumers.

To avoid the privacy tabula rasa, businesses would be wise to update their web site and privacy policy to adjust for opt-out notices per CCPA § 1798.120, § 1798.135 and CCPA Proposed Regs § 999.306 and § 999.315.

Message

From: Lea Kissner [REDACTED]
Sent: 12/6/2019 10:06:23 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Lea Kissner [REDACTED]
Subject: Comments on the proposed CCPA regulations
Attachments: CCPA proposed regulations comments.pdf

Thank you for the opportunity to submit comments on the proposed CCPA regulations. My name is Lea Kissner and I'm a privacy engineer. Until recently, I was the Global Lead of Privacy Technology for Google, the technical lead for privacy across the company, and worked there for over a decade on building security and privacy into products and infrastructure, working in close collaboration with the legal and policy teams. I am currently the Chief Privacy Officer of a startup, Humu. My PhD is in cryptography from Carnegie Mellon University and BS in EECS from UC Berkeley. I am a founder of USENIX PEPR: Privacy Engineering, Practice, and Respect, the first conference for privacy engineering in practice and a member of the Advisory Board for the International Association of Privacy Professionals (IAPP) Privacy Engineering Section.

I suspect that few of these comments will come from privacy engineers who have run privacy programs and built privacy technology. I have experience developing and implementing policy and technical protections, in building privacy programs and systems in tech companies large and small. As such, I've learned a fair bit about how to make privacy work better and more smoothly. Good regulations are important to keeping users safe and their privacy intact, but the key to carrying through those ideas into practice is clarity and implementability. These comments are aimed at clarifying and modifying the regulations in order to maximize the strength of privacy and security protections for consumers in practice by making both privacy programs and system implementations robust.

Please feel free to contact me any time with questions or for clarification; I've devoted my professional life to helping people build respect into their products and systems and am thus happy to help here. Thank you for your consideration.

My comments are attached here.

Thank you,
Dr. Lea Kissner

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

Thank you for the opportunity to submit comments on the proposed CCPA regulations. My name is Lea Kissner and I'm a privacy engineer. Until recently, I was the Global Lead of Privacy Technology for Google, the technical lead for privacy across the company, and worked there for over a decade on building security and privacy into products and infrastructure, working in close collaboration with the legal and policy teams. I am currently the Chief Privacy Officer of a startup, Humu. My PhD is in cryptography from Carnegie Mellon University and BS in EECS from UC Berkeley. I am a founder of *USENIX PEPR: Privacy Engineering, Practice, and Respect*, the first conference for privacy engineering in practice and a member of the Advisory Board for the International Association of Privacy Professionals (IAPP) Privacy Engineering Section.

I suspect that few of these comments will come from privacy engineers who have run privacy programs and built privacy technology. I have experience developing and implementing policy and technical protections, in building privacy programs and systems in tech companies large and small. As such, I've learned a fair bit about how to make privacy work better and more smoothly. Good regulations are important to keeping users safe and their privacy intact, but the key to carrying through those ideas into practice is clarity and implementability. These comments are aimed at clarifying and modifying the regulations in order to maximize the strength of privacy and security protections for consumers in *practice* by making both privacy programs and system implementations robust.

Please feel free to contact me any time with questions or for clarification; I've devoted my professional life to helping people build respect into their products and systems and am thus happy to help here. Thank you for your consideration.

Thank you,

A handwritten signature in black ink that reads 'Lea Kissner'.

Dr. Lea Kissner

In 999.315(c), opt-out requests are allowed to come from “*user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism*”. Anyone can create a mechanism, including a browser plugin, but without a well-designed standard they cannot function. Servers can only understand and honor requests made using an agreed-upon, standard protocol. No provision for a standard is made in the regulation.

- Suggested change: modify to “that communicate or signal the consumer’s choice **using a standard protocol or mechanism**” and list these standard mechanisms in further versions of this regulation or in an associated document. There should be a small number of these standards, ideally one; more complex code sadly means more bugs and more difficulty in testing. Privacy settings must be robust and should thus avoid these issues.
- I would suggest that NIST or another organization experienced in standards could best handle the standards-making process. I would ask that you list standards to which companies should adhere.

999.312(a) requires that all businesses operate a toll-free telephone number for requests to know and requests to delete. The CCPA in 1798.130(1a) as amended in AB-1564 specifically provides an exemption from this phone number requirement for online-only businesses which is not reflected in this regulation. Such an exemption is particularly important for online businesses which may operate in many languages. Having a web site available in a large number of languages is important to increase access to and understanding of that site’s information and services. Translation for websites happens asynchronously: the text for the website is sent to translators who send back translations. In contrast, safely handling high-sensitivity real-time phone calls in many different languages is far more difficult and expensive, and is particularly prohibitive for small businesses.

- Suggested change: modify to include the text of the exemption “*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. 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. 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.*”

999.336(a) states that “*A financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations*” where service difference includes “*any difference in the level or quality of any*

goods or services offered to any consumer" This expansive phrasing can force websites to violate this provision in certain circumstances. For example, consider a website which uses a consumer's ratings of books to suggest new books to read, either to that consumer or to other consumers. When a consumer exercises their right of deletion over those ratings, the quality of recommendations will necessarily decrease as the ratings from the consumer who had requested deletion can no longer be included in the recommendation method; there is literally no way to avoid this decrease in quality caused by exercise of a consumer's right. This particular example does not encompass all reasonable services which will experience such contradictions, but does show a common pitfall.

- Suggested change:
 - Add a third example in 999.336(c) to clarify that level or quality of goods or services can be defined with regards to the data which the user has not requested to be deleted: *"Example 3: A website uses a consumer's ratings of books to suggest new books to read. If the consumer deletes some or all of their ratings, the quality of these recommendations may fall. If this fall in quality is reasonably related to the reduced quality and quantity of data on which to base recommendations, the differing quality is not discriminatory, because there is no way to simultaneously allow the consumer to exercise their rights and continue to provide the service at the same quality and level."*

999.305(a1b) requires that opt-out notice *"Use a format that draws the consumer's attention to the notice and makes the notice readable"*. Some lawyers are reading this as requiring a European-style cookie banner. From a privacy user experience point of view, this would be inappropriate, as this is a notice, not a consent, which is going to be on (nearly) every website. Research shows that people get so used to notices like these that they will become effectively blind to them¹, at which point: (1) a site operator can add extra consent terms without them being appropriately considered by most consumers and (2) it robs effectiveness from one of the techniques we have to notify users of new, important information (e.g. a change in service or that their computer may be infested with malware). I would note that there is nothing in the text of the CCPA itself which requires drawing the user's attention in this fashion.

- Suggested change: modify text to *"Use a format that makes the notice clearly visible and readable"*.

999.325(c) requires that *"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."* This degree of certainty is similar to that imposed by the GDPR. We have seen the level of security

¹ Studies of blindness to warnings and dialogs include "Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiments" (https://neurosecurity.byu.edu/media/Vance_et_al_2017_MISQ.pdf), "Harder to Ignore: Revisiting Pop-Up Fatigue and How to Prevent It" (<https://www.usenix.org/system/files/soups14-paper-bravo-lillo.pdf>)

there is far too low; studies have shown it is simple to exploit, especially for a spouse or partner². Given that such abuse is far too common³, we should avoid providing another avenue for technology-facilitated stalking⁴. The balancing control of requiring a signed declaration under penalty of perjury will not stop the vast majority of such stalkers; they are already using an assumed identity, which renders any requirement to attest to identity nearly meaningless.

- There is no simple change here. We frankly do not know how to authenticate otherwise unauthenticated people. The CCPA and GDPR have shown that there is keen interest in making information more available (as it should be); give academics and privacy engineers time (and potentially funding) to work on finding better solutions while protecting the security and privacy of consumer by requiring a “*high degree of certainty*”.

999.317(e) requires that “*Information maintained for record-keeping purposes shall not be used for any other purpose.*” However, there are critical operational uses of this data that use what are effectively the same records; these operational tasks are required to run one of these programs at scale: number and type of requests (for determining required levels of staffing), turnaround time (to monitor compliance with required timeframes), outcomes (as a warning indicator of issues with the identity validation process⁵), etc. Disallowing use of record-keeping records from operational use means that people will keep two copies of the same records. This might seem trivial, but keeping multiple sets of records will lead to errors either in creating the records, keeping them consistent, and in minimizing appropriate retention.

- Suggested change: modify text to “*Information maintained for record-keeping purposes may be used for purposes of running, improvement, and measurement of the privacy program, but shall not be used for any other purpose.*”

999.312(f) requires that “*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 ...*” largely, treat it like a request submitted through the normal channels. However, sometimes consumers will sometimes submit requests in a way that may reasonably not be received (e.g. sent to the wrong company, to an invalid email address, or even potentially put on a billboard) or recognized (e.g. written in a language in which the company does not customarily do business, or simply incomprehensibly). In addition,

² Studies of subject access request security failures include “Personal Information Leakage by Abusing the GDPR’s ‘Right of Access’” (<https://www.usenix.org/conference/soups2019/presentation/dimartino>), “GDPArrrr: Using Privacy Laws to Steal Identities”

(<https://www.blackhat.com/us-19/briefings/schedule/index.html#gdparrrr-using-privacy-laws-to-steal-identities-14526>)

³ Approx. 6% of women in a particular 12-month period alone, as measured by the CA Department of Public Health.

(<https://www.cdph.ca.gov/Programs/CCDPHP/DCDIC/SACB/Pages/DomesticViolenceIntimatePartnerViolence.aspx>)

⁴ https://nnedv.org/latest_update/technology-facilitated-stalking/

⁵ If the rate of successfully-validated identities suddenly drops to near-zero, there may be an issue in the identity validation process or technology which is causing validation to fail erroneously, or there may be an onslaught of attackers attempting to fool the identity validation. Outcome data is key to monitoring for anomalies like this.

consumers may send requests in a way which compromises their security. When I worked at Google, people would insist on sending me personally requests having to do with their account, without understanding — quite naturally — that the protections afforded to their email sent to me were very different from those of our official request submission mechanism. As a privacy and security engineer, I was not comfortable with having identity checks go through my email account, where they would be retained in line with our corporate email retention rules, rather than through the identity verification forms, where data could be thoroughly deleted as soon as practicable.

- Suggested change: modify text to “*If a consumer submits a **comprehensible, directly received** 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 ...*” and add option (3): “*If the submission method is insecure or directed to personnel who are not trained to handle requests under the CCPA, provide the consumer with specific directions on how to submit a secure request.*”

999.308(a2e) requires “*Be available in an additional format that allows a consumer to print it out as a separate document.*” If the privacy policy prints out well already, why require an additional format? Having more than one copy of anything makes it far easier to end up with accidental inconsistencies, where one is edited but not the other.

- Suggested change: modify text to “*Be available in a format that allows a consumer to print it out as a document.*”

999.305(a2d) requires accessibility for a privacy notice or “*At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.*” If that information about how to reach the alternative format is not itself accessible, then how will the consumer with a disability find it?

- Suggested change: modify text to “*At a minimum, provide **accessible** information on how a consumer with a disability may access the notice in an alternative format*”

In conclusion, these regulations have several places in which they can be changed to better support a clear, implementable technical program which better protects the privacy and security of consumers.

Thank you for this opportunity to submit comments and for your consideration. Please contact me for any additional questions or clarification. Privacy engineering allows us to build more robust and complete privacy protection; I believe that stronger regulations can be built in tandem with these technical protections and am dedicated to supporting this.

Message

From: Hoisington, Michael J. [REDACTED]
Sent: 12/6/2019 9:17:10 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments related to the California Consumer Privacy Act (CCPA) Draft Regulations

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

1. Timing of Implementation. More time is needed before the CCPA enters effect.
 - The Regulations are still in draft form less than a month before the Act is scheduled to go into effect.
 - The Regulations are complicated and confusing and additional time must be spent to address these concerns.
 - Additional materials need to be developed to assist businesses in complying with the Act, such as exemplar notices, signage and procedures.
 - Businesses need plenty of lead time to understand the CCPA and Regulations, generate the documents and procedures to comply, set up training for employees and management.
 - At least a 12 – 24 month delay until January of 2021 or 2022.
2. Definitions. There are numerous terms used in the CCPA and the Regulations that should be defined – in the context of the CCPA/Regulations - for clarity.
Examples: In the context of Regulations Section 999.313 (c)(3), what is meant by “substantial”? “unreasonable”?
3. It is difficult to interpret Regulations Section 999.313(c)(4) “a business shall not at any time disclose 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.” Does that mean even to the original consumer? That should be clarified.
4. Guidance is required on how businesses can deal with loyalty programs within the parameters of the CCPA Regulations Section 999.336 discriminatory prohibitions. Valuation (reasonable value) should be simplified in Regulations Section 999.337. If a consumer chooses to opt out of a loyalty program, or to delete his/her data, how does the business still offer incentives considering the consumer has exercised a right provided in the CCPA? The example provided in the draft Regulations does not make sense. The exchange of the consumer’s email for a discount is a logical exchange – and, if there is a request to know, of course it makes sense that that would not affect the discount. However, if the consumer opts out or deletes his/her data, it is nonsensical to expect that the consumer could continue to receive the discount – that is not fair to the business or the other consumers who have provided something of value in exchange for the discount. This section needs further thought and editing.
5. Notice requirements need to be simplified to one type of notice, displayed in one place. Probably a website is the best solution. It is difficult to figure out how best to comply with notice requirements in the Regulations.

6. The AG should be looking for ways to work with businesses that are required to comply with the Act to make it easy to do so and so that they are not punished if they make mistakes in attempting good faith compliance with the Act and Regulations.
7. When denying a request know or delete, how specific does the reason provided to the requester have to be? This could vary from “we are unable to verify your identity” to “we are unable to verify your identity based on a mismatching name, account number and/or address.” What will be specific enough to comply with the Regulations?
8. The CCPA should make exemptions related to other laws protecting personal information crystal clear in the Regulations and consider all such other laws in creating such exemptions.
9. The CCPA and/or the Regulations should define what “reasonable security procedures” means so there is a clear standard that can be understood and adhered to by all. See CCPA Section 1798.150 (a)(1).

Submitted by Michael Hoisington, Esq.
Higgs Fletcher & Mack LLP
401 West A Street, Suite 2600
San Diego, CA 92101



Michael J. Hoisington
Attorney at Law

Phone [REDACTED]
Fax (619) 696.1410
Email [REDACTED]

401 West A Street, Suite 2600, San Diego, CA 92101

www.higgslaw.com

Please read the [legal disclaimers](#) that govern this e-mail and any attachments.

TAX ADVICE: Any federal tax advice contained in this communication (including attachments) is not intended or written to be used, and cannot be used, for the purpose of avoiding penalties under the Internal Revenue Code or promoting, marketing, or recommending any transaction or matter discussed herein.

Message

From: Anna C. Westfelt [REDACTED]
Sent: 12/6/2019 8:48:37 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Derek Schwede [REDACTED]; Todd Smithline [REDACTED]
Subject: Comments to CCPA Implementing Regulations
Attachments: Comments to CCPA AG Implementing Regulations.pdf

On behalf of a working group of in-house and law firm attorneys listed in the attached letter, we respectfully submit these comments regarding the Attorney General's CCPA Implementing Regulations.

Very truly yours,

Anna Westfelt, Gunderson Dettmer Stough Villeneuve Franklin & Hachigian, LLP
Derek Schwede, Smithline PC
Todd Smithline, Smithline PC

Anna C. Westfelt



Gunderson Dettmer Stough Villeneuve Franklin & Hachigian, LLP
550 Allerton Street
Redwood City, CA 94063
Phone: [REDACTED] | Fax: 650-618-3267
[REDACTED] | www.gunder.com

This email and any attachments may contain private, confidential and privileged material for the sole use of the intended recipient. If you are not the intended recipient, please immediately delete this email and any attachments.

December 6, 2019

By email to privacyregulations@doj.ca.gov

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

Re: Comments to the Attorney General's CCPA Implementing Regulations

Dear Sir/Madam:

On behalf of a working group of California and national in-house and law firm attorneys, organized by Smithline PC, we thank you for the opportunity to submit comments regarding the Attorney General's CCPA Implementing Regulations (California Consumer Privacy Act Regulations (Stats. 2018, Ch.55 [AB 375], as amended by Stats. 2018, Ch. 735 [SB1121])) (the "Implementing Regulations").

We support the Attorney General's stated goal of providing clarity and specificity to assist in the implementation of the CCPA. For the reasons set forth below, we believe that in their current form, the draft Implementing Regulations will not achieve the stated goal, and in many cases risk introducing additional uncertainty for businesses and service providers seeking to comply with the CCPA.

Further, we believe that, while this uncertainty will hamper companies of all sizes, it will disproportionately impede (and create barriers to entry for) innovative smaller companies vis-à-vis their larger incumbent competitors who already have the money, legal resources, and legacy databases necessary to move forward despite the uncertainty.

With this in mind, we have outlined below our proposed revisions to the Implementing Regulations. These clarifications address ambiguities in the CCPA and the draft Implementing Regulations, and aim to provide more concrete guidance to companies on how to comply with the CCPA.

I. TABLE OF CONTENTS

	Issue	Para. Ref.
A.	Opt-In Consent for New Purpose	11 CCR § 999.305(a)(3)
B.	Service Providers	11 CCR § 999.314
C.	Compliance with Browser Opt-Out Signals	11 CCR § 999.315(c)
D.	Responding to Consumer and Agent Requests	11 CCR §§ 999.313 and Article 4
E.	Compliance Concerns Not Addressed in Current Draft of Implementing Regulations	N/A

II. PROPOSED AMENDMENTS AND REQUESTS FOR CLARIFICATION

A. Opt-In Consent for New Purpose - 11 CCR § 999.305(a)(3)

§ 999.305(a)(3): [Comment: AG should not introduce new requirements exceeding the scope of the CCPA]

1. Background: § 999.305(a)(3) provides that explicit consent is required for a business to use a consumer's personal information for any purpose other than those disclosed in the notice at collection.
2. Comment: This provision creates a new consent requirement for certain processing of personal information that a business initially performed legally on a notice basis (*with no consent required*). § 1798.100 of the CCPA expressly states that "A business shall not ... use personal information collected for additional purposes without providing the consumer with notice consistent with this section." As such, this provision in the Implementing Regulations is in direct conflict with, and significantly exceeds the scope of, the CCPA, even though it was not introduced through the appropriate legislative process.

Additionally, this provision does not increase privacy protections for California consumers. Instead, it incentivizes businesses to create over-broad, lengthy privacy notices covering every potential "purpose" and use of personal information they may consider in the future, leaving California consumers without meaningful and readable disclosures about how businesses use their personal information. This directly conflicts with the requirement in § 999.305(a)(2) to have a notice at collection that is "easy to read and understandable to an average consumer."

3. Request: We request the Attorney General reverse this material expansion of the scope of the CCPA and remove subsection (a)(3), or, alternatively, clarify that the express consent to a different purpose only applies when the initial processing was consent-based. To the extent the Attorney General believes there needs to be a requirement for consent-based processing of personal information in certain circumstances, that change should be made directly through the legislative process.

B. Service Providers - 11 CCR § 999.314

Subsection (a): [Comment: Vast Expansion of Scope of Service Providers]

1. Background: § 999.314(a) provides that a “person or entity” is still a “service provider” if it (1) provides services to a “person or organization” that is not a business and (2) otherwise meets the “service provider” definition. The Initial Statement of Reasons for these changes focuses on non-profit and government entities as potential non-business service recipients. For context, under the statute a “business” or “service provider” must be an *entity* (“sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity ...”) and an entity is a service provider only if it provides services to a “business” as defined by the statute. (§§ 1798.140(c)(1) and (v))

Comment: The Attorney General’s proposed regulations raise two important issues. First, this provision expands the definitions of “service provider” and “business” to include individuals in addition to legal entities. Second, in addition to non-profits and government entities, this would capture for-profit companies that do not meet the CCPA’s criteria for a business. The proposal exceeds the scope of the statute and imposes contractual obligations and potential liability on service providers for whom there is no corresponding “business”. The effects would fall especially on service providers to small businesses (who are likely small businesses themselves).

2. Request: We request the Attorney General reverse this material expansion of the scope of entities that qualify as service providers. To the extent the Attorney General believes other for-profit entities should be covered as businesses, that change should be made directly through the legislative process.

Subsection (c): [Comment: AG Should Not Overrule Statute’s “Reasonably Necessary and Proportionate” Standard]

1. Background: § 999.314(c) prohibits a service provider from using one customer’s personal information “for the purpose of providing services to another person or entity.” The sole exceptions relate to security, fraud and illegal activity. In explaining this new rule, the Attorney General states that other uses across businesses would be “outside the bounds of a ‘necessary and proportionate’ use of personal information” under the statute’s standards for a permitted business purpose. (See § 1798.140(d))

2. Comment:

- a. General. We support the Attorney General's goal of providing clear guidance for a complex statute. We are concerned, however, that the proposed regulation exceeds the scope of the statute and could have serious unintended consequences for California technology companies and consumers.
- b. Standard Industry Practice. Enterprise businesses frequently authorize service providers to use personal information to build, support and improve the services they provide. These activities are essential to technology development and benefit businesses, service providers and consumers. For instance, a service provider might use personal information provided by a business internally for feature optimization, troubleshooting bugs, or training algorithms that benefit all customers. (In modern product architecture, using only de-identified information for these purposes may be insufficient.)
- c. Part of the Service. These activities are expected as *part of the service provider providing its service as requested by customers*. Under the CCPA, they may certainly constitute "reasonably necessary and proportionate" business purposes within the service context. (§ 1798.140(d)) By way of analogy, the GDPR uses a balancing test of "legitimate interest" rather than predetermining all permitted uses of personal information.
- d. Respect for Private Contract. Businesses are sophisticated parties and the data rights they grant service providers depend on the services involved. Their private contracts should be respected, provided the contracts otherwise comply with the CCPA and businesses meet the CCPA's requirements in collecting personal information. The proposed regulation could void existing contracts and cause many enterprise SaaS services to become arguably "non-compliant" overnight under a rule that, by definition, refuses to even allow consideration of the nature of the parties, data or services involved. Note further in this context that most SaaS providers operate on a "single build" model, so any product changes implemented in response to this proposed regulation would likely de facto be extended to all users in all jurisdictions.
- e. Unneeded Change. Subsection (c) is unnecessary and appears to conflict with the statute. The statute already prohibits the service provider's use of personal information for "commercial purposes" outside of the service context, while also expressly allowing use for the service provider's "business purposes." This fact-based standard accommodates a variety of service types and relationships. (§ 1798.140(d) and (v))
- f. Exceeds Statutory Authority. The proposed regulation upsets that statutory balance, introducing a vague rule that certain uses of data could *never* be

“reasonably necessary and proportionate”, regardless of circumstances. No authority is cited for this sweeping change and none is evident.

- g. Unintended Consequences. The scope of subsection (c) is unclear. However, a blanket prohibition on using personal information for service improvement (if that is the regulation's intent or effect) would have no precedent at law, would disrupt technological and economic development, and runs contrary to industry practice and freedom of contract. While sector-specific statutes may impose restrictions on specific regulated information (e.g., financial, health or student data), the CCPA applies broadly to all personal information. It must remain flexible enough to apply across all industries and over time.
3. Request: We request that the Attorney General modify subsection (c) as follows:
 - a. Clarify that, when authorized by the business, a service provider may internally use personal information provided by a business to build, support or improve the service provider's services and for other permitted business purposes.
 - b. Alternatively, remove subsection (c).

These clarifications would protect consumers' privacy interests and provide much-needed clarity in the marketplace, while enabling the continued technology development on which California companies and millions of consumers rely.

§ 1798.140 of Statute: Definition of “Service Provider” vs. “Third Party” [Comment: Need to Separate Service Provider and Third Party]

1. Background: The CCPA creates two types of parties that process personal information under contract with a business: “service providers” and persons who are *not* “third parties” (to whom we refer as exempt third parties). While similar, each has different rights and obligations, creating confusion in the marketplace as to what contractual terms are required. (§ 1798.140(v) and (w))
2. Request: We request clarification of the relationship between service providers and exempt third parties, and specifically, confirmation that those who are “service providers” need not also be characterized as exempt third parties.

§ 1798.155(a) of Statute: Seeking Opinion of Attorney General [Comment: Service Providers May Also Seek Opinion]

1. Background: The CCPA provides that “Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title.” (§ 1798.155(a)) Service providers are not expressly mentioned, but also have legitimate reasons to seek the Attorney General’s opinion regarding compliance.

2. Request: Add service providers to the parties that may seek the Attorney General's opinion under § 1798.155(a). The ability of a service provider to clarify its compliance obligations will benefit it, the businesses it deals with and consumers.

C. Compliance with Browser Opt-Out Signals – 11 CCR § 999.315(c)

§ 999.315(c): [Comment: AG should not introduce new requirements exceeding the scope of the CCPA]

1. Background: § 999.315(c) states that a 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 for that browser or device, or, if known, for the consumer.
2. Comment: Pursuant to the California Online Privacy Protection Act ("CalOPPA"), website operators are required to state how they respond to "Do Not Track" browser signals, but are not required to implement technology changes to recognize and honor such signals. The requirement in the Implementing Regulations for businesses to be technically able to recognize and comply with "Do Not Sell" browser plugins or other browser privacy settings is a new, onerous requirement that exceeds the scope of the CCPA and existing California law. There is currently no standardized protocol for "Do Not Sell" browser requests or controls that businesses can reasonably identify and comply with, and any new requirement for businesses to recognize and honor browser signals and plugins needs to be addressed through the California legislative process.
3. Request: Amend § 999.315(c) to state that businesses are required to state in their privacy policy if and how they respond to "Do Not Sell" browser signals or settings, and if a business is unable to comply with such signals, it shall specify other available methods of submitting a "Do Not Sell" request as set forth in § 999.315(a).

D. Responding to Consumer and Agent Requests – 11 CCR §§ 999.313 and Article 4

§§ 999.313 and Article 4: [Comment: Need certainty on a business' liability when responding to consumer requests, including when dealing with an "authorized agent"]:

1. Background: The Implementing Regulations provide general guidance regarding a business' response to consumer requests in a variety of circumstances, depending on the type of request, the sensitivity of information involved, the degree of certainty required for verification and whether the request is made by a consumer, household member or authorized agent.
2. Comment: These guidelines inherently require a business to undertake a fact-based inquiry and exercise good-faith discretion. This leaves open the question of whether a business acting in good faith could be exposed to liability if it discloses or deletes

information in response to a request that is later determined to be fraudulent. The concern is heightened for requests from putative authorized agents. Even if the Secretary of State maintains a registry of authorized agents, it may be difficult for businesses to validate that *a particular agent* is truly authorized by *a particular consumer*, considering that consumer permissions or agent communications each may be forged. Since the GDPR took effect, EU businesses have been overwhelmed by automated, large-scale data subject requests through third party agents, often including fraudulent requests seeking to obtain data subjects' identity information or introduce phishing malware via suspicious links. Given technical limits and the sophistication of online crime, there is no fail-safe guarantee against fraud.

Businesses may reasonably be concerned about potential exposure under the CCPA or other laws based on their mistaken response to a consumer request. Without further clarity, businesses are left with a Hobson's choice: they will either tend *not* to disclose or delete the requested information without complete certainty of the request's validity (frustrating the consumer interests the CCPA is designed to protect) *or* they will risk potential liability for good faith disclosures in response to requests later determined to be fraudulent.

3. Request: We request that the Attorney General create a liability safe harbor for businesses: a business shall not be liable if, in response to a consumer or authorized agent request, it discloses or deletes information in good faith in accordance with a documented verification method reasonably designed to comply with the Implementing Regulations. We also request that the Attorney General provide further guidance regarding the proof a business is required to seek in order to verify that a particular agent is authorized by a particular consumer.

E. Compliance Concerns Not Addressed in Current Draft of Implementing Regulations

Website Cookies Shared with Third Parties:

1. Background: A common practice for businesses engaged in behavioral or interest-based advertising is the use of cookies placed on website visitors' devices and subsequently sent to third parties in exchange for information about such website visitor. Neither the CCPA nor the Implementing Regulations provide guidance on how to ensure compliance with respect to this common practice.
2. Request: We ask that the Attorney General provide clarity on whether the use of website cookies shared with third parties constitutes a "sale" of personal information pursuant to the CCPA.

Personal Information in User-Generated Content:

1. Background: Many websites and mobile applications allow for the uploading of significant amounts of user-generated content, which content is provided at the

discretion of the user. Sometimes the uploaded content includes personal information of consumers other than such user; however, the business (a) may have no way of knowing that such personal information has been included in uploaded content and (b) in any case, has no contact information or relationship with a consumer whose personal information may be so included in the content of uploading user.

2. Request: We ask that the Attorney General provides clarity on how to comply with the CCPA with respect to personal information that may be included in user-generated content. The business typically will not have contact information for the consumer whose personal information may be included in the content of a user (and may not be aware that such personal information is included in uploaded content), and, accordingly, the business cannot provide a privacy notice or notice at collection directly to such consumer.

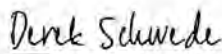
In particular, we would welcome clarification from the Attorney General that having the required notice and privacy policy prominently posted or referenced on the business' website or mobile application, as applicable, is sufficient for this common use case.

Thank you for your consideration of these comments. We appreciate the opportunity to provide ideas and information to assist in the process of clarifying the CCPA compliance obligations.

Note: The opinions and views expressed in these comments are those of the individual attorney authors and do not necessarily reflect the opinions or views of any such attorney's employer or client. Affiliations are provided for identification purposes only.

Very truly yours,


Anna Westfelt
Of Counsel
Gunderson Dettmer Stough
Villeneuve Franklin &
Hachigian, LLP


Derek Schwede
Principal
Smithline PC


Todd Smithline
Managing Principal
Smithline PC

Amanda Weare

Amanda Weare

Associate General Counsel – IP, Product
and Privacy
Collibra Inc.

Gabriel Ramsey

Gabriel M. Ramsey

Partner
Crowell & Moring LLP

David Mitchell

David Mitchell

VP, Legal
Demandbase, Inc.

Vikki Nguyen

Vikki Nguyen

Associate
Gunderson Dettmer Stough Villeneuve
Franklin & Hachigian, LLP

Diane Nahm

Diane Nahm

Head of Legal
RealtimeBoard, Inc. dba Miro

Brandon Wiebe

Brandon Wiebe

Senior Corporate Counsel
Segment.io, Inc.

Lisa Babel

Lisa Babel

General Counsel
StreamSets, Inc.

Eric Lambert

Eric Lambert

Division Counsel
Trimble Inc.

Jeffrey Poston

Jeffrey L. Poston

Partner
Crowell & Moring LLP

Lee Matheson

Lee Matheson

Associate
Crowell & Moring LLP

Elaine Tan

Elaine Tan

Sr. Manager, Compliance
Demandbase, Inc.

Xavier Le Hericy

Xavier Le Hericy

Chief Privacy Officer
New Relic, Inc.

Mark Kahn

Mark Kahn

General Counsel and VP of Policy
Segment.io, Inc.

Audrey Kittock

Audrey Kittock

Corporate Counsel
Segment.io, Inc.

Diana Olin

Diana Olin

Assistant General Counsel
Sumo Logic, Inc.

Annie Sun

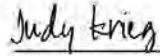
Annie Sun

In-house Attorney



Mark Webber

U.S. Managing Partner, Technology and
Privacy
Fieldfisher (Silicon Valley) LLP



Judy Krieg

Partner, Privacy, Security and Information
Fieldfisher LLP

Message

From: Paul Jurcys ([REDACTED])
Sent: 12/7/2019 12:16:39 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Markus Lampinen ([REDACTED])
Subject: Comments to CCPA Regulations | Prifina
Attachments: CCPA Comments-PRIFINA.pdf

Dear Privacy Regulations Coordinator,

Please find the Comments to the proposed Draft Privacy Regulations.

Sincerely,

Paul Jurcys

--
Paul Jurcys, LL.M. (Harvard), Ph.D.
Co-Founder | [Prifina](#)
1 Market St., San Francisco

PRIFINA

Dr. Paul Jurcys and
Markus Lampinen,
on behalf of Prifina, Inc.

1 Market Street,
Spear Tower, Suite 3600
San Francisco, CA 94105

Email:
policy@prifina.com

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

**Comments to the Proposed Chapter 20, of the California Code of
Regulations (CCR) concerning the California Consumer Privacy Act (CCPA)**

Dear Attorney General X. Becerra,

Prifina Inc. is pleased to have the opportunity to respond to the request for comments on the California Consumer Privacy Act and the proposed Regulations. We would also like to thank the Office of the Attorney General for making it possible for various interested parties to express their views.

Prifina appreciates the work that the Office of the Attorney General has done in providing more clarity as well as practical guidelines as to the implementation of the CCPA. The CCPA entitles consumers to access, delete and opt-out from the sale of their personal information. More generally, the CCPA and these Regulations provide a significant step forward in protecting consumer privacy and paving the way towards more user-controlled data privacy framework. We admire that the Office of the Attorney General has taken a firm stance to protect consumers' rights related to data privacy while also maintaining fair, orderly and efficient functioning of the digital market. As an active participant in developing more transparent and balanced data models, we share the goals enshrined in the CCPA and the Regulations. We encourage the AG to implement the CCPA in a manner that emphasizes transparency and certainty for various stakeholders while also leaving room for the growth, evolution, and vibrancy in the data privacy field.

Should you have any questions, please do not hesitate to contact us.

Sincerely yours,

Paul Jurcys and Markus Lampinen

About Prifina

Prifina is a San Francisco-based company building user-centric tools that help individuals gain control of their personal data and get tangible value from it.

Prifina is witnessing how various technological, political and commercial factors drive the change in the data market. In Europe, although imperfect, the General Data Protection Regulation (GDPR) was drafted and implemented in order to give individuals access to and control of their data. The adoption of the CCPA and increasing demands from consumers, buttressed by technological innovation, signal a clear shift in the United States towards user-controlled data models. This transition towards user-controlled data models is already affecting companies that are looking for ways to better comply with the requirements of data privacy regulations such as the CCPA and GDPR, not to mention companies that see the user-controlled data model as an opportunity. A wide variety of companies recognize the opportunity in user-controlled data solutions which are starting to shape how companies approach the business need to make their services more personalized and relevant to their customers.

Prifina's interest in the CCPA is simple: we want individuals to have access to their data in a manner and in a form that is useful to them, while also allowing businesses access to the information that is relevant to their businesses and their customers. We believe there also exist opportunities for novel regulatory technologies and solutions, that can leverage advances in user-centric data models giving regulatory agencies better data and channels at their disposal. We would welcome common-sense regulation in California that serves as a template for the rest of the country.

Below, we discuss some key characteristics that we believe are necessary for effective regulation of data privacy and consumer rights for California as a leader in this field.

Comments on the Draft Regulations

1. Notice of a Financial Incentive

Prifina suggests that the following modification the proposed wording of § 999.307(a)(1) is made as follows:

"1) The purpose of the notice of financial incentive is to explain to the consumer each financial incentive or price or service difference a business may offer in exchange for the access, retention or sale of a consumer's personal information so that the consumer may make an informed decision on whether to participate."

This suggestion to include “access” to personal information would benefit both businesses and individuals as the data collection models are becoming more user-centric. Businesses are starting to look into possible ways to minimize the amount of raw data they own, and one of the possible alternatives is to access the data which is held by consumers themselves. Accordingly, it is suggested that the wording of § 999.307(a)(1) be modified so that businesses would indicate financial incentives in cases where the business is seeking to access personal data from the consumers directly.

2. Responses to Consumers’ Requests to Know

§ 999.313(c)(9) of the Regulations mandates the businesses to provide *personalized* responses to consumers’ requests to know. Besides, § 999.313(c)(11) requires that businesses’ response to the consumers’ requests to know are offered “in a manner that provides consumers a meaningful understanding” of the information requested. This section of the Regulations aims to specify Section 1798.100(d) of the CCPA which provides that “[t]he information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance.”

Prifina would like to point out that requests to know should be fulfilled by providing data in a manner which is not only easy to understand to the consumers but also in a form and standard which is universally accepted in the market. Prifina notes, that at the time when these Comments are submitted, there is no single market-wide standard with regard to the format in which customers’ data is provided to the customers. In fact, businesses’ responses to customers’ requests to know are offered in multiple different formats (excel sheets, .zip archives, JSON, etc).

In order to facilitate data portability, the Attorney General could use this opportunity to clarify the notion of “meaningfully understandable manner” of the responses to requests to know and make data sharing more efficient.

Therefore, Prifina proposes that the Regulations specify a requirement that such responses to consumers’ requests to know should provide data in a (i) structured, (ii) commonly used, (iii) machine-readable, and (iv) interoperable format. Prifina is of the opinion that these four requirements should be treated as minimum requirements: they should be sufficient for achieving the goals of data portability and empowerment of the individuals with their data. Furthermore, these found minimum requirements should give enough flexibility for businesses to come up with interoperable data format solutions without superimposing them with a costly task of setting uniform data compatibility standards.

3. Consumers' Requests to Provide Data to Third Parties

An ecosystem, based on the principle of the free flow of data, would benefit if the Regulations enable the individual to instruct the business to whom the request is made to send the consumer's data to a third party. For instance, the consumer should be able to instruct its financial institution to release some information to a potential landlord. Such a possibility is not set forth in the CCPA, but it will be an important feature of a user-consent based data portability framework in the future.

4. Timely Responses to Consumers' Requests

§§ 999.313(a), 999.313(b), 999.315(e) and 999.315(f) of the Regulations provide certain periods during which the businesses have to respond to the consumers' requests to know, delete and opt-out. These periods range from 10 days to 90 days from the time when the request is received.

Prifina team can hardly conceive a situation where more than 30 days are needed to comply with the consumer's request to provide the data. From a consumer perspective, waiting for personal data for three months is completely unreasonable and defeats the purpose of data portability. It should be emphasized that at the time when these Comments are submitted, the biggest data silos usually respond to consumers' requests to provide personal data within one or two days. Therefore, if a business needs extensive time to fulfill customers' requests, that suggests there is no adequate process for handling consumer data requests in place. We believe that most requests to know should be able to be processed automatically; the responses should be made *nearly immediately*, or within a period of several days at the latest.

Therefore, Prifina team recommends the Attorney General prioritize data portability and demand that businesses implement technology measures to process the requests to know. The default standard period of time for processing data requests should be "nearly immediate".

5. Estimating the Value of Customer Data

Section 1798.125(a)(2) of the CCPA provides that business can charge a consumer a different price or rate, or provide a different level or quality of goods or services to the consumer, "if that difference is reasonably related to the value provided to the business by the consumer's data." § 999.337 of the Regulations lists seven methods which business *must* use in determining the value of customer data. All of those proposed methods for calculation of customer data are based on the variables that focus on the value that the business generates from that data.

Prifina suggests that the proposed Regulations should include the requirement to consider how much value customers attach to their personal data. Some helpful methods for estimating how customers value their private data could be found in the most recent academic literature.¹ One of the pertinent areas of research focuses on the so-called “endowment effect” in different settings.² In order to assess the personal value of their data to consumers, those findings suggest looking into two factors: (a) how much consumers would be willing to pay for keeping their data private (“Willingness-to-Pay”); and (b) how much consumers would be willing to accept for giving away their private data (“Willingness-to-Accept”). Economists who conducted empirical studies using these benchmarks of willingness to pay and willingness to accept in data privacy settings have found that individuals value their data much more than businesses (from 200% to 1800% more).³ Therefore, Prifina suggests that the proposed § 999.337 of the Regulations should require business to adopt scientifically proven methods that help estimate how much certain data is worth to consumers themselves.

6. Notice of Right to Opt-Out

§ 999.306 of the Regulations provides a framework for implementing notices of the right to opt-out of sale of personal information. Furthermore, § 999.306 (e) suggests that the Attorney General will propose a standard opt-out button or logo which may be used in addition to posting the notice of right to opt-out.

Prifina would like to suggest that the Attorney General aim to ascertain that the opt-out mechanism is consumer-friendly and does not require more time or effort than the opt-in procedures. From a technological point of view, the opt-out process should be as smooth and frictionless as opt-in and from a usability point of view it should be seamless and understandable for the individual.

¹ Angela G. Winegar, Cass R. Sunstein, ‘How Much Is Data Privacy Worth? A Preliminary Investigation’, forthcoming, *Journal of Consumer Policy*, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3413277.

² Daniel Kahneman, Jack L. Knetsch, Richard H. Thaler, ‘Experimental Tests of the Endowment Effect and the Coase Theorem’, *The Journal of Political Economy*, Vol. 98, No. 6 (Dec., 1990), pp. 1325–1348

³ See Note 1 above.

Message

From: Victoria Sheckler [REDACTED]
Sent: 12/6/2019 10:39:07 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: [REDACTED] [REDACTED] [REDACTED] Ken Doroshow [REDACTED]
Subject: comments to proposed regulations concerning CCPA
Attachments: Comments to CCPA proposed rules 12-6-19.pdf

Attached please find comments to the proposed regulations concerning the California Consumer Privacy Act submitted on behalf the International AntiCounterfeiting Coalition (IACC), the National Music Publishers Association (NMPA) and the Recording Industry Association of America (RIAA).

Regards,



Vicky Sheckler | SVP, Legal Affairs and Deputy General Counsel
Recording Industry Association of America
e. [REDACTED] | w. riaa.com
t. [REDACTED] | s. 1025 F Street, NW
10th Floor | Washington, DC 20004



December 6, 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

Dear Sir/Madam:

The International AntiCounterfeiting Coalition (IACC), the National Music Publishers' Association (NMPA) and the Recording Industry Association of America (RIAA) welcome the opportunity to provide comments on California's Department of Justice (Attorney General) proposal to adopt 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).

Who We Are

The IACC is the world's oldest and largest organization dedicated exclusively to combating trademark counterfeiting and copyright piracy. Founded in 1979, and based in Washington, D.C., the IACC represents approximately 250 corporations, trade associations and professional firms, spanning a broad cross-section of industries. IACC members include many of the world's best-known brands in the apparel, automotive, electronics, entertainment, luxury goods, pharmaceutical, software and other consumer product sectors. Central to the IACC's mission is the education of both the general public and policy makers regarding the severity and scope of the harms caused by intellectual property crimes – not only to legitimate manufacturers and retailers, but also to consumers and governments worldwide. The IACC seeks to address these threats by promoting the adoption of legislative and regulatory regimes to effectively protect intellectual property rights, and to encourage the application of resources sufficient to implement and enforce those regimes.

NMPA is the principal trade association representing the U.S. music publishing and songwriting industry. NMPA represents publishers and songwriters of all catalog and revenue sizes, from large international corporations to small businesses and individuals. Taken together, compositions owned or controlled by NMPA members account for the vast majority of the market for musical composition licensing in the United States. NMPA protects and advances the interests of music publishers and songwriters in matters relating to both the domestic and global protection of music copyrights before the legislative, judicial and executive branches of the U.S. government.

The RIAA is the trade association that supports and promotes the financial vitality of the major record companies. Its members comprise the most vibrant record industry in the world, investing in great artists to help them reach their potential and connect to their fans. Nearly 85% of all legitimate recorded music produced and sold in the United States is created, manufactured or distributed by RIAA members. In support of its mission, the RIAA works to protect the intellectual property and First Amendment rights of artists and music labels; conducts consumer, industry and technical research; and monitors and reviews state and federal laws, regulations and policies.

Introduction

Music is a vital part of our nation's and California's culture and economy,¹ and drives consumers to various online platforms to access, engage with and consume the music they love.² In addition, the other products and services offered by IACC members, which range from automotive to pharmaceuticals, and from apparel to software, significantly contribute to the health, wellbeing and economy of the U.S. and California.³

Unfortunately, rogue operators attempt to capitalize on our country's love for music and for the other products and services offered by IACC members by infringing the rights of intellectual property rights holders online. In terms of hard goods, a 2019 study by the Organization for Economic Cooperation and Development estimated the global market for counterfeit and pirated goods to exceed \$500 billion, annually.⁴ In recent years, counterfeiters have increasingly turned to the Internet to facilitate the distribution of their illicit wares, in part because of the relative anonymity available online. Just this week, the National Intellectual Property Rights Coordination Center announced the results of a joint operation with Europol, Interpol and police agencies from approximately 20 different countries which led to the seizure of over 30,000 web domains engaged in the illegal sale of counterfeit and pirated goods.⁵

In the case of music and other entertainment infringement, rogue operators not only steal the content, but also often use that content to as the lure to get consumers to their sites, apps or social media pages so the rogue operator can engage the consumer in activity associated with malware, identity theft and other malfeasance. Consider, for example, that in 2016 Digital Citizens Alliance found that one in three content theft sites exposed users to malware.⁶ A 2017 article reported that hundreds of music player apps on the Google Play Store had some form of malware.⁷ A 2018 report stated that "[i]llegal pirating sites are the most common source of malware infection on the internet," and that nearly one in 10 children have been affected by malware.⁸ And a recent survey found that 27% of the people surveyed had used unlicensed music services in the last month.⁹ Such widespread usage of rogue services exposes

¹ The music industry contributes \$38.49 billion to the state's GDP and supports over 447,000 jobs and 40,000 businesses in California. And there are over 190,000 songwriters and over 29,000 sound recording royalty participants in California. Source: RIAA. See <http://50statesofmusic.com/state/california/>.

² In the first half of 2019, 89% of the U.S. sound recording revenues came from digital sources, with 80% from streaming. Source: RIAA. See <http://www.riaa.com/wp-content/uploads/2019/09/Mid-Year-2019-RIAA-Music-Revenues-Report.pdf>. Today, seven of the top 10 most followed Twitter accounts and four of the top 10 most followed Instagram accounts are for sound recording artists, seven of the top 10 most liked Facebook accounts are for sound recording artists, and eight of the top 10 most watched videos on YouTube are for official music videos. Source: RIAA. See <http://www.musicfuels.com/>.

³ For a list of IACC members, see <https://www.iacc.org/membership/members>.

⁴ OECD/EUIPO (2019), *Trends in Trade in Counterfeit and Pirated Goods*, Illicit Trade, OECD Publishing, Paris, available at <https://doi.org/10.1787/g2g9f533-en>.

⁵ See U.S. immigration and Customs Enforcement (Dec. 2, 2019), ICE HSI-led IPR Center and Europol collaboration leads to massive illegal website seizures ahead of Cyber Monday., available at <https://www.ice.gov/news/releases/ice-hsi-led-ipr-center-and-europol-collaboration-leads-massive-illegal-website>.

⁶ See Digital Citizens Alliance news release at <https://www.digitalcitizensalliance.org/news/press-releases-2016/dangerous-partners-digital-citizens-investigation-finds-that-malware-operators-and-content-theft-websites-assisted-by-u.s.-based-tech-firms-are-targeting-millions-of-consumers/>.

⁷ HackReed, *Android Malware Found in Hundreds of Music Player Apps on Play Store*, Nov. 20, 2017, available at <https://www.hackread.com/android-malware-found-in-hundreds-of-music-player-apps-on-play-store/>.

⁸ Internetmatters.org, *Internet Safety and the Dangers of Digital Piracy: Understanding the Risks for Children*, July 2018, available at <https://www.internetmatters.org/wp-content/uploads/2019/04/Internet-Matters-Report-Dangers-of-digital-piracy.pdf>.

⁹ Source: IFPI. See <https://www.ifpi.org/news/IFPI-releases-music-listening-2019>.

consumers to unwanted activity that could harm them, harm our nation's industries and ultimately harm the ability to provide new creative and innovative offerings to consumers.

The significant relevance, importance and value of music and the other products and services offered by IACC members to both consumers and the online platforms that use music, entertainment or hard goods to engage consumers on their platforms (whether those platforms are licensed or infringing, or offering authentic or counterfeit products) gives us a unique and important perspective in considering rules of the road for consumer privacy.

Suggested Changes to Proposed Regulations

One of the main tenets of a privacy and consumer protection framework is that there should be transparency around who is engaging the consumer online – i.e., who is on the other side of the screen. Providing for such transparency, and with it attendant accountability, along with disclosures about the collection and use of personal information, helps build trust and provides incentives for players in the online ecosystem to create a safe and vibrant Internet.

Sometimes, however, privacy regimes are misconstrued to prohibit disclosure of personal information at all costs, even where such disclosure is appropriate to know who is on the other side of the screen, such as when that actor is engaged in illegal behavior. For example, it was recently reported that a European Data Protection Authority (DPA) asked a registrar for information about a domain name registrant in connection with a website that was improperly using personal information.¹⁰ Unfortunately, that registrar refused to provide the information requested to the DPA absent a court order because the DPA was not law enforcement, even though the DPA was in fact trying to investigate and enforce its privacy laws. We and others have also been denied access to registrant or online operator data in the name of privacy law constraints when attempting to legitimately investigate and enforce against infringing, fraudulent or other illegal behavior online. This shows that taking protection of personal information to extremes can sometimes exacerbate, rather than protect against, consumer harms.

We urge the California Attorney General to consider such unintended consequences in connection with its proposed regulations, and to modify its proposed regulations to avoid such results. Specifically, we ask that the proposed regulations obligate service providers to include a disclosure in their privacy policies that they may disclose personal information to third parties if the third party has reason to believe the person at issue has violated the rights of that third party or has engaged in other illegal or unlawful behavior, whether in terms of cybersecurity issues, identity theft, fraud, infringement or other harm. We would add such a disclosure obligation to Section 999.305(b) and Section 999.308(b)(1)(c).

Such a privacy policy disclosure does not foreclose the possibility of third parties getting reasonable access to personal information in cases of legitimate need to deter such harms, while at the same time does not mandate disclosure upon any bald request. This provides breathing room for a more mature, nuanced approach that helps reconcile and balance the various interests at stake in relation to privacy, accountability and transparency. It ensures that rights holders and others are not unnecessarily stymied in their efforts to protect their rights or investigate consumer harms, while ensuring that a person's legitimate interests in his or her personal information are preserved.

* * *

¹⁰ Source: Internet Coalition of Assigned Names and Numbers (ICANN) public meeting 66, GNSO – EPDP Phase 2 meeting, Nov. 2, 2019, audio recording available at http://audio.icann.org/meetings/yul66/yul66-OPEN-2019-11-02-T1150-511c-en-GNSO--EPDP-Phase-2-Meeting-1-of-_m3u.

Thank you for the opportunity to submit our comments on this important topic.

Sincerely,

The International AntiCounterfeiting Coalition

The National Music Publishers' Association

The Recording Industry Association of America

Message

From: Fisher, Katherine [REDACTED]
Sent: 12/6/2019 6:14:36 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Fisher, Katherine [REDACTED]
Subject: Commercial Finance Coalition CCPA Proposed Regulations Comments (Dec. 6, 2019)
Attachments: Commercial Finance Coalition CCPA Proposed Regulations Comments (Dec. 6, 2019).pdf

Hello. I am submitting the attached written comments regarding the proposed CCPA regulations on behalf of the Commercial Finance Coalition. Please let me know if you have issues opening the attachment or have any questions.

Thank you,

Kate Fisher

Katherine C. Fisher
Partner | Admitted in Maryland and Oregon
Hudson Cook, LLP
Direct: [REDACTED] | Cell: [REDACTED]
7037 Ridge Road | Suite 300 | Hanover, Maryland 21076

HUDSON
COOK

The information contained in this transmission may be privileged and may constitute attorney work product. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact Katherine C. Fisher at kfisher@hudco.com or 410.782.2356 and destroy all copies of the original message and any attachments.



Comments to the California Office of the Attorney General On Proposed Regulations for the California Consumer Privacy Act

The Commercial Finance Coalition ("CFC") is comprised of responsible finance companies that provide needed capital to small businesses through innovative methods. CFC members offer accounts receivable purchase financing to small businesses (also known as merchant cash advance or "MCA"), and some also engage in lending, specifically in the state of California through a California Finance Lender's license. Our members also include select vendors that provide technology services to the small business finance industry.

This letter responds to the invitation of the California Office of the Attorney General ("OAG") for written comments on proposed regulations implementing the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code §§ 1798.100 *et seq.*

The CFC appreciates the work of the OAG to further the privacy rights of Californians. We offer the comments in this letter in the hope that these regulations may be clear and effective in implementing the CCPA.

The CFC is specifically concerned about the amount of work needed for a business to properly implement compliance processes for these regulations. Therefore, we strongly urge the OAG to adopt an effective date for the regulations at least 6 months after publication of the final rule. This will provide businesses with adequate time to prepare to comply with the regulations. To compare with the European Union's General Data Protection Regulation, businesses subject to that law had two years to prepare before the compliance deadline.

Additionally, CFC members are concerned about how to comply on day 1 with provisions of the regulations that require notices to have been provided before the law is effective. For example, proposed section 999.305(d) requires businesses that obtain personal information from a source other than the consumer to confirm that the source provided a Notice at Collection to the consumer. In this case, such a source would not have provided a Notice at Collection before the CCPA was effective. Therefore, we strongly urge the OAG to provide expressly that no provision of these regulations will be construed to have retroactive effect or to expect compliance with the law before the law's effective date.

CFC provides the following specific comments about the proposed regulations:

- 1. Define the term "disability."**

Proposed sections 999.305(a)(2)(d), 999.306(a)(2)(d), 999.307(a)(2)(d), and 999.307(a)(2)(d) require that businesses make—or be able to make—various notices available to consumers with a “disability.” However, the term “disability” is not defined.

The CFC reads the term “disability” as relating to the medium of communication of notices, which is in writing or electronically. Therefore, a relevant “disability” for these notices would be a visual disability.

Recommendation: Define the term “disability” to refer to visual disabilities.

2. Define the term “conspicuous.”

Proposed sections 999.305(a)(2)(e), 999.308(a)(3), and 999.315(a) require businesses to post links “conspicuously.” However, the term “conspicuous” is not defined, so it is not clear how the OAG expects a “conspicuous” link to be presented.

Recommendation: Define the term “conspicuously,” or alternatively, give examples of what the OAG would deem to be a “conspicuous” link.

3. Remove the requirement that businesses obtain “explicit consent” to use personal information for additional purposes.

Proposed section 999.305(a)(3) requires businesses to obtain “explicit consent” before using personal information for a purpose that was not previously disclosed to the consumer in the Notice at Collection.

The CCPA does not require businesses to obtain affirmative consent before using personal information for a new purpose. CCPA section 1798.100(b) simply provides that a business may not use personal information previously collected for additional purposes “without providing the consumer with notice consistent with” section 1798.100. At most, the law requires a business to provide notice to use previously-collected information for additional purposes; *consent* is never contemplated. For information collected from the consumer, consumers can request deletion of personal information at any time.

Recommendation: Remove the requirement that a business obtain “explicit consent” to use personal information for purposes not disclosed in the Notice at Collection.

4. Eliminate or revise the sale restriction from non-consumer sourced personal information.

Proposed section 999.305(d) provides that in order to sell personal information collected from a source other than the consumer, a business must either (1) provide notice to the consumer or (2) obtain the notice at collection the source gave the consumer along with signed attestations describing how the source gave the notice.

This sale restriction is not provided for in the CCPA, and so it goes beyond what the OAG is authorized to require. The CCPA requires a notice at collection only when collecting personal information directly from consumers, and no other provision of the CCPA imposes any requirement other than honoring opt-out requests for a business to sell personal information.

Even if the CCPA contemplated this sale restriction, this provision assumes that either the business or the source will have a direct relationship with the consumer. However, this is not always the case, and this restriction, if finalized, would have a chilling effect on data transfers across the country.

Finally, given that this sale restriction does not appear in the CCPA, it is not clear whether this restriction is meant to apply to personal information that is exempt from some, but not all, of the CCPA. For example, it is not clear whether this sale restriction is meant to apply to employee data, for which a notice at collection is required. See Cal. Civ. Code § 1798.145(h).

Recommendation: Eliminate this sale restriction. Alternatively, require businesses to obtain certifications of compliance with the CCPA from their sources.

5. Clarify that businesses are only required to provide notice of those consumer rights available to consumers with the business.

Proposed section 999.308 requires a business to disclose, in a business' online privacy policy, that consumers have various rights under the CCPA.

Businesses are not required to comply with the CCPA for a number of types of personal information, as set out in section 1798.145 of the law. The proposed regulations do not make it clear that businesses are not expected to provide privacy policy disclosures for consumer rights that are not ever available with a particular business, considering the exemptions available to the business.

It would risk consumer confusion for a business to explain that a consumer has certain rights with the business under the CCPA when the business is not, in fact, required to honor consumer rights because of one or more exemptions.

Recommendation: Clarify that businesses are only required to provide notice of consumer rights that are available to consumers with the business.

6. Clarify that a business may describe its verification process in general terms.

Proposed sections 999.308(b)(1)(c), 999.308(b)(2)(c), and 999.313(a) require businesses to describe the business' verification process for right to know and delete requests, either in the business' online privacy policy or in the letter describing receipt of a consumer request.

Among other things, a verification process is needed to prevent the release of personal information to fraudsters. Therefore, it will be important to the efficacy of the verification process—and the protection

of personal information against identity theft—to keep the details of a particular business’ verification process confidential.

Therefore, it would be helpful for the regulations to specify that a business may describe its verification process *in general terms*.

Recommendation: Amend all requirements to describe a business’ verification process to clarify that such a description may be made “in general terms.”

7. Eliminate two-step process to delete.

Proposed section 999.312(d) requires a business to use a two-step process for online requests to delete where the consumer must first clearly submit the request to delete and then separately confirm that they want their personal information deleted.

A two-step process does not provide any particular benefit to consumers, so long as a business confirms that the requestor is who they say they are and the request is unambiguous. With a two-step process, consumers may fail to confirm their request after making it, which would prevent businesses from honoring a clear consumer request.

Recommendation: The OAG could require that deletion requests be made in writing or that businesses must take steps to confirm the requestor is the consumer about whom the request is being made.

8. Remove the requirement for a business to respond to a consumer request submitted by a non-designated method.

Proposed section 999.312(f) requires that a business in receipt of a Right to Know or deletion request submitted by a method other than one of its designated methods of submission must either treat the request as if it had been submitted in accordance with a designated method or provide the consumer with specific directions on how to submit the request or remedy any deficiencies with the request, if applicable.

The CCPA does not require businesses to accept or redirect a request made to a business by any method. Section 1798.130(a)(1) of the CCPA requires businesses to establish one or two designated methods, depending on the way in which the business interacts with consumers. Therefore, the OAG exceeds its authority in requiring businesses to respond to a request submitted by any method.

Compliance with this requirement will prove difficult for businesses. Businesses may not be able to monitor and respond to all possible channels by which a request may be provided. For example, businesses may have email addresses by which they email consumers, but those businesses do not monitor those email addresses for incoming traffic. A consumer may attempt to place a request to such an email address, but since the business does not monitor the email address, the business would not receive the request.

Consumers will be provided one or two methods by which they can submit requests. Businesses will have to explain these methods in the business' online privacy policy.

Recommendation: Remove the section 999.312(f) requirement that a business respond to consumer requests submitted by non-designated methods.

9. Modify the requirement that business provide categories of personal information to only where consumer requests the categories.

Proposed section 999.313(c)(1) requires that if a business cannot verify a consumer for a request to know specific pieces of personal information about a consumer, it must consider whether it can verify the consumer as if the consumer requested the categories of personal information about the consumer.

The CCPA permits a consumer to request to know the categories of personal information a business collected, sold, or disclosed for a business purpose about the consumer, and it permits a consumer to request the specific pieces of personal information the business collected, sold, or disclosed for a business purpose. The CCPA requires businesses to comply with these consumer requests. *See* Cal. Civ. Code §§ 1798.110 and 1798.115. The CCPA does not, however, require a business to comply with a Right to Know request by providing information to a consumer that a consumer does not request.

As a result, the OAG exceeds its authority under the CCPA in requiring businesses to provide a consumer with categories of personal information when the consumer only requests the specific pieces of personal information.

Recommendation: Amend this requirement to apply only where a consumer specifically requests categories of personal information in addition to the specific pieces of information.

10. Remove the requirement that a business respond to a consumer request relating to exempt personal information.

Proposed sections 999.313(c)(5) and 999.313(d)(6)(a) provide that a business declining to honor a consumer's request to know or delete on the basis of an exemption under the CCPA must inform the consumer that it will not honor the request and explain the basis for the denial.

However, section 1798.145 of the CCPA provides that businesses are not required to comply with CCPA consumer rights for certain kinds of exempt data. Therefore, the OAG is not authorized to require businesses that are exempt from the CCPA to comply with CCPA obligations, including responding to consumer requests in a particular way.

Recommendation: Eliminate the requirement that a business respond to a consumer request relating only to exempt personal information.

11. Eliminate the deletion request waterfall requirement.

Proposed section 999.313(d)(1) requires a business that cannot verify a consumer for a deletion request to treat the request as an opt-out request.

The CCPA requires businesses to honor a consumer's deletion request and a consumer's opt-out request, but it does not provide a sale opt out where the consumer requested deletion. Consumers have the ability to request one or both of these rights, and different processes govern receipt and consideration of each of these rights. Consumers may, for example, want to request deletion, but not sale opt-out.

Recommendation: Eliminate the waterfall requirement that a non-verifiable deletion request be treated as an opt-out request.

12. Permit businesses to delete archived personal information on set purge schedules.

Proposed section 999.313(d)(3) permits a business to delay deletion of personal information maintained on archived or backup systems until the archived or backup data is next accessed or used.

Businesses may access archived databases regularly, as new information is archived or the database is managed. However, businesses regularly set purge schedules for archived data. Businesses should be permitted to utilize regular purge schedules for information that the business no longer accesses or uses in its ordinary course.

Recommendation: Permit deletion to be made consistent with a business' preestablished purge schedule.

13. Clarify that businesses are required only to note generally the method by which personal information is deleted.

Proposed section 999.313(d)(4) requires businesses to specify to the consumer the manner in which it deleted personal information upon the consumer's request. The same section permits businesses to delete information by erasing it, deidentifying it, or aggregating it.

It would be helpful for the OAG to clarify that the expectation under proposed section 999.313(d)(4) is that businesses are required to note whether deletion is made by erasure, or deidentification, or aggregation, but a business is not expected to explain the process by which it deidentified the information, for example. Safeguarding the particular deidentification or aggregation processes is necessary for a business to protect its information security.

Recommendation: Clarify that section 999.313(d)(4) requires that businesses state whether deletion was made by erasure, deidentification, or aggregation.

14. Clarify that a business may use personal information for any exempt purpose after declining to honor a deletion request.

Proposed section 999.313(d)(6)(c) prohibits a business that denies a consumer request to delete on the basis of a particular exemption under the CCPA from using that personal information for any purpose other than provided for by that exception.

The CCPA provides various exceptions from the law, without imposing any kind of a restriction on a business only using personal information under one exception. Prohibiting a business from using personal information for an exempt purpose after it used it for—and denied a deletion request on the basis of—a separate exempt purpose defeats the purposes of having multiple exceptions, frustrates compliance with federal law, and is contrary to the purposes of the CCPA.

Recommendation: Clarify that a business may use personal information that the business declined to delete under any exemption.

15. Clarify website placement of “Do Not Sell” button.

Proposed section 999.315(a) requires that businesses place the “Do Not Sell My Personal Information” or “Do Not Sell My Info” link “on the business’s website or mobile application.”

CCPA section 1798.135(b) permits businesses to include this link on a California-specific homepage, so long as California residents are directed to this homepage. It would be helpful for the regulations to specifically permit use of a California-specific homepage as well.

Recommendation: Amend proposed section 999.315(d) to clarify that businesses can comply with the requirement by placing the “Do Not Sell” button on a California-specific website homepage.

16. Remove the requirement to treat user-enabled privacy controls as valid opt-out requests.

Proposed section 999.315(c) requires that businesses treat user-enabled privacy controls that communicate or signal a consumer’s choice to opt out of the sale of their personal information to third parties as a valid request to opt out for that browser or device or, if known, for the consumer. The CCPA protects “personal information,” which means information that reasonably may be linkable to a particular individual or household, not merely a device. See Cal. Civ. Code § 1798.140(o)(1).

The CCPA protects information that is reasonably able to be linked with a person or household, not merely a device. To the extent that this section regulates information that is not reasonably linkable with a person or household, the OAG exceeds its authority in proposing this requirement.

Furthermore, to the extent that this opt-out requirement applies to information reasonably linkable to a particular consumer or household, the CCPA does not require businesses to accept the signal of a user-enabled privacy device as an opt out request. Businesses selling personal information must provide that right in other ways under the statute.

Consumers may install a privacy device for many reasons, not just to prevent personal information from being sold to third parties. This technology is also evolving, and there will likely be compatibility issues between systems.

Recommendation: Remove the requirement that businesses treat user-enabled privacy controls as a valid opt-out request.

17. Eliminate the requirement that business notify third parties upon sale opt out.

Proposed section 999.315(f) requires that, after accepting an opt out request, a business must notify all third parties to whom it sold the personal information within the last 90 days and instruct them not to sell the information.

The CCPA does not impose any retroactive third party opt-out notification requirement, nor does it prohibit third parties from selling personal information after the instruction of another entity. Rather, the right to opt-out runs to future sales. Therefore, the OAG does not have the authority to impose this requirement.

Even if a business did instruct a third party not to sell personal information, many businesses may not have a current contractual relationship with that third party that would permit it to control the third party's sale of that information.

Further, this provision would require businesses to exchange personal information to instruct third parties, so if finalized, it could increase the risk of data breaches and identity theft.

Recommendation: Eliminate this third party opt-out notification and instruction requirement.

18. Eliminate the two-step process to opt-in to sale.

Proposed section 999.316(a) requires that businesses utilize a two-step process to opt-in consumers to the sale of personal information after their opt-out.

A two-step process does not provide any particular benefit to consumers, so long as a business confirms that the requestor is who they say they are and the request is unambiguous. With a two-step process, consumers may fail to confirm their request after making it, which would prevent businesses from honoring a clear consumer request.

Recommendation: The OAG could require that opt-in requests be made in writing or that businesses must take steps to confirm the requestor is the consumer about whom the request is being made.

19. Eliminate standalone data security requirement.

Proposed section 999.323(d) provides that businesses must implement “reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer’s personal information.”

The CCPA does not include any requirement to implement data security protections. The only related provision in the CCPA provides certain defenses to private suits in the event that a data breach results from a business’ “violation of the duty to implement and maintain reasonable security procedures and practices.” As a result, the OAG exceeds its authority in this proposed requirement.

Furthermore, federal and state law already impose data security requirements. Federal law, including the Safeguards Rule promulgated under the Gramm-Leach-Bliley Act and prohibitions against unfair, deceptive, and abusive acts and practices, already imposes data security requirements. Preexisting California law requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Cal. Civ. Code § 1798.81.5(b). Overlapping data security expectation are, at best, redundant, and at worst, may result in conflicts in implementation.

Recommendation: Eliminate the data security requirement in proposed section 999.323(d).

20. Do not require signed declaration for request to know specific pieces of personal information.

Proposed section 999.325(c) provides that a business may comply with a consumer’s request to know specific pieces of information by matching three pieces of personal information and obtain a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request.

The CCPA gives business broad discretion in verifying that a requestor is the consumer that it claims. It is not clear whether this signed declaration is expected of all businesses verifying requests to know specific pieces of information on a consumer who does not have a password-protected account with the business, since the combination of three identifiers and the signed declaration is presented as one way that a business “may” match to a reasonably high degree of certainty.

To the extent that a signed declaration is expected when a business matches on three identifiers, requiring a signed declaration would be unduly burdensome to businesses. Businesses will likely process requests electronically, so requiring consumers to provide a signed declaration would be problematic to both businesses and consumers. Such a declaration is also not likely to protect consumers, as fraudsters

would not likely be warded off by the requirement of a signed declaration and consumers would have to work harder to exercise their rights under the CCPA.

Recommendation: Explain that a “reasonably high degree of certainty” means matching on three pieces of personal information and remove the mention of a signed declaration.

* * * * *

Thank you for the opportunity to provide comments on the OAG’s proposed CCPA regulations.

Message

From: Pedro Gonzalez [REDACTED]
Sent: 12/4/2019 10:20:22 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Consumer privacy law
Flag: Follow up

Dear Att. Gen. Xavier Becerra,

I tried to be present this morning at the meeting in San Francisco, but heavy traffic held me back. The reason for my visit was to oppose the CCPA from becoming a law. I used to tell my insurance not to release any of my or my wife's personal information to other business. Of course I have to sign a letter prohibiting them from releasing any of our personal information. I fear that our identity might be stolen. The general public does not read all documents that these business send them, we only see the figure that we have to pay. Many people do not read English. People need to be educated on this CCPA AB375. I appreciate it if you can hold this decision on this Assembly Bill 375.

Sincerely,

Pedro Gonzalez,
Former City Council/Mayor of
City of South San Francisco

Message

From: Rachel Nemeth [REDACTED]
Sent: 12/6/2019 6:39:38 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CTA comments on proposed privacy regulations
Attachments: CTA CA AG CCPA Proposed Regulations Comments FINAL.pdf

See attached for comments from the Consumer Technology Association.

Thank you,
Rachel

Rachel Sanford Nemeth

Director, Regulatory Affairs

Consumer Technology Association, producer of CES®

d: [REDACTED]

m: [REDACTED]

[CTA.tech](#) | [CES.tech](#)

Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an innovator in Software as a Service (SaaS) for business. Providing a **safer** and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more [Click Here](#).

Before the
CALIFORNIA OFFICE OF THE ATTORNEY GENERAL
Los Angeles, CA 90013

In the Matter of)
)
Proposed Adoption of California Consumer)
Privacy Act Regulations)
)

**COMMENTS OF
CONSUMER TECHNOLOGY ASSOCIATION**

Michael Petricone
Sr. VP, Government and Regulatory Affairs

Rachel Nemeth
Director, Regulatory Affairs

1919 S. Eads Street
Arlington, VA 22202
[REDACTED]

December 6, 2019

TABLE OF CONTENTS

I. Introduction.....	1
II. The AG Should Exercise Caution in Expanding the CCPA’s Disclosure Requirements.....	2
A. Notice at Collection and Disclosures in Businesses’ Privacy Policies – Sections 999.305 and 999.308.....	2
B. Notice of Financial Incentive – Section 999.307(b)(5)	5
III. The Proposed Regulations On Consumer Requests Are Overly Burdensome	6
A. Timeline to Respond to Requests to Know or Delete – Section 999.313	6
B. Requests to Delete Personal Information – Section 999.313(d).....	7
C. The Proposed Service Provider Regulations Contradicts the Statute – Section 999.314.....	9
D. Requests to Opt Out of the Sale of Personal Information – Section 999.315.....	11
IV. The Proposed Regulations Should Afford Flexibility in Establishing Verification Procedures – Sections 999.323-999.325	12
V. Parental Consent Methods Should Track Federal Law and Regulation – Section 999.330(a).....	13
VI. There Is No Need to Adopt Overly Burdensome Recordkeeping Requirements – Section 999.317.....	14
VII. Conclusion	16

General Data Protection Regulation (“GDPR”) as well as U.S.-focused businesses that were not subject to the GDPR and therefore had not yet deployed new data governance processes and systems, building CCPA-compliant programs already has been a significant, challenging, and expensive initiative.

To that end, CTA welcomes the AG’s efforts to clarify certain ambiguous or conflicting aspects of the CCPA through the proposed regulations. CTA is concerned, however, that a number of the proposed regulations would add to the significant compliance burdens and operational challenges already imposed by the CCPA – and would do so without a commensurate benefit to privacy. CTA addresses such proposals below.

II. THE AG SHOULD EXERCISE CAUTION IN EXPANDING THE CCPA’S DISCLOSURE REQUIREMENTS

As described below, requiring businesses to provide overly detailed and specific information in their privacy notices and disclosures can make such notices and disclosures more complicated, less comprehensible, and, ultimately, less useful for consumers.

A. Notice at Collection and Disclosures in Businesses’ Privacy Policies – Sections 999.305 and 999.308

The CCPA already includes extensive notice requirements to inform consumers about the collection, use, and disclosure of their personal information.³ Though some of the clarifications regarding notice in the proposed regulations provide welcome guidance to industry – *e.g.*, that notice at collection can be included as part of a privacy policy⁴ – the proposed regulations in the aggregate, as currently drafted, will ultimately lead to longer, more complex notices and privacy

³ See, *e.g.*, Cal Civ. Code § 1798.130(a)(5) (requiring specific disclosures in a business’s online privacy policy or policies).

⁴ Proposed 20 CCR § 999.305(a)(2)(e); ISOR at 9.

policies. Regulations governing privacy policies and other notices should ensure that disclosures provide meaningful and clear information to consumers, consistent with the statutory requirements set forth in the CCPA, but they should not require a level of detail and complexity that can create additional operational challenges and overwhelm consumers.

Sections 999.305(b)(2) and 999.308(b)(1)(d)(2). Section 999.305(b)(2) would require that a notice at collection state “[f]or each category of personal information, the business or commercial purpose(s) for which it will be used.”⁵ Similarly, section 999.308(b)(1)(d)(2) would require that a privacy policy state “[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.”⁶ No matter the outcome of the AG’s proposed regulations, notices and privacy policies inevitably will become more complex as businesses draft their policies to comply with myriad existing and emerging legal regimes. There is no need to make these notices and policies even more complicated. The requirement to not only list the categories of personal information collected and shared as the CCPA requires, but also list for each the “business or commercial purpose(s)” for which the information was collected and/or shared, will add detail and complexity not meaningful to consumers, in turn making notices and privacy policies less consumer-friendly.⁷

⁵ Proposed 20 CCR § 999.305(b)(2).

⁶ *Id.* § 999.308(b)(1)(2)(d).

⁷ In addition, use of the word “shares” here as it relates to third parties should actually be “sells” for consistency with section 1798.130(a)(5)(C)(i) of the CCPA. *See* Cal. Civ. Code 1798.130(a)(5)(C)(i).

The proposed regulations also would be an operational challenge, even for well-intentioned companies. Companies may need to continuously update their privacy policies to ensure that the appropriate “business or commercial purpose(s)” for each category of personal information they collect or disclose remains up to date, even when they already have disclosed more generally the information they collect and the purposes for which they collect and share it – *i.e.*, they already provide consumers the information needed to understand the businesses’ information practices. Worse, companies that wish to avoid a constant review of their privacy policy may instead indicate that each category of data collected or shared is done so broadly for multiple business or commercial purposes – even if not currently – actually providing *less* precise information to consumers, contravening the purpose of the requirement.

Section 999.308(a)(3). Subsection (a)(3) similarly risks forcing companies to draft broader, less specific disclosures. The subsection would require a business to obtain “explicit consent” before using collected personal information for a new purpose,⁸ regardless of whether that purpose is consistent with consumer expectations as well as the purpose for which the information was collected. As a result, companies would need to ensure that the disclosures they make when they first collect personal information are broad enough to capture potential future uses so that they lower the chance they need to obtain subsequent “explicit consent.”

Section 999.308(b)(1)(c). Subsection (b)(1)(c) would require businesses to have privacy policies that “describe the process the business will use to verify the consumer request, including any information the consumer must provide.”⁹ Such a requirement would prove confusing for

⁸ Proposed 20 CCR § 999.308(a)(3).

⁹ *Id.* § 999.308(b)(1)(c).

consumers, as companies may employ different verification methods for different types of information. It also is unnecessary, as the verification process can be sufficiently explained as part of any given consumer request in the request interface and response flow.

Section 999.308(a)(2)(d). Subsection (a)(2)(d) would require that a business’s privacy policy “[b]e accessible to consumers with disabilities” by, at a minimum, “provid[ing] information on how a consumer with a disability may access the policy in an alternative format.”¹⁰ CTA is a strong supporter of ensuring that people with disabilities have access to innovative technology, and actively works with the accessibility community to achieve that goal. CTA is concerned, however, that the proposed requirement as drafted goes beyond what may be reasonable in every circumstance, particularly for small and medium businesses with fewer resources. To that end, CTA encourages the AG to clarify the accessibility requirement and make clear that business’ efforts to make their privacy policy and other notices accessible need be reasonable, but not infallible.

B. Notice of Financial Incentive – Section 999.307(b)(5)

Section 999.307(b)(5) is infeasible, overly complicated, and unnecessary. This section would require a business to provide: “[a]n explanation of why the financial incentive or price or service difference is permitted under the CCPA,” including: (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

¹⁰ *Id.* § 999.308(a)(2)(d). Equivalent requirements would apply to the notice at collection, *see id.* § 999.305(a)(2)(d); notice of right to opt-out of sale, *see id.* § 999.306(a)(2)(d); and notice of financial incentive, *see id.* § 999.307(a)(2)(d).

consumer's data.¹¹ Companies have no practical way to estimate the value of an individual consumer's data, regardless of whether they provide a financial incentive that relates to the use of such data. Additionally, given that there is no uniform, widely-accept method to calculate the value of consumer data, the estimates offered by businesses in turn likely will be wide-ranging and inconsistent. These various "good faith" estimates will only confuse consumers and will not provide them with any additional helpful information to make decisions about accepting a customer rewards or other financial incentive-based service or feature.¹²

III. THE PROPOSED REGULATIONS ON CONSUMER REQUESTS ARE OVERLY BURDENSOME

The requirement to receive, verify, and respond to consumer requests under the CCPA already poses significant operational challenges and burdens; the AG's proposed regulations, as currently drafted, would add more.

A. Timeline to Respond to Requests to Know or Delete – Section 999.313

Section 999.313(a). This section would require that, "[u]pon receiving a request to know or a request to delete, a business shall confirm receipt of the request within 10 days and provide information about how the business will process the request. The information provided shall describe the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request."¹³ A 10-day turnaround time for receipt confirmation, however, would pose significant operational challenge

¹¹ *Id.* § 999.308(b)(5).

¹² Should the AG ultimately decide to adopt this requirement, it should ensure that the requirement does not force companies to publicly reveal trade secrets or proprietary information.

¹³ Proposed 20 CCR § 999.313(a).

to businesses. In addition, this requirement will be particularly challenging for small businesses that, though subject to the CCPA, may not have the resources to customize and deploy automated systems in order to avoid manual processing. At a minimum, the 10 days should be modified to 10 business days.

Section 999.313(b). Separately, under the proposed regulations, the 45-day trigger for responding to a request begins upon receipt of the request regardless of the time required to verify the request.¹⁴ The CCPA, however, consistently refers to any such request as a “*verifiable* consumer request”¹⁵ – *i.e.*, the statute itself suggests that a request only needs to be acted on when it qualifies as “verifiable.” Therefore tying the timeline for a response to when the request is made, regardless of when it is verified, is inconsistent with the statute. It also may be unreasonable in situations where verification of a particular consumer takes more time. Instead, any timing requirements to respond should be based on when the request was verified, which is when the “verifiable request” is actually first made.

B. Requests to Delete Personal Information – Section 999.313(d)

Section 999.313(d)(6). Subsection (d)(6) presents unnecessary operational challenges. The proposed regulation would require a business denying a consumer’s request to delete information to (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; (b) delete the consumer’s personal information that is not subject to the exception; and (c) not use the consumer’s personal information retained for any other purpose than provided for by that

¹⁴ *Id.* § 999.313(b).

¹⁵ *E.g.*, Cal. Civ. Code 1798.100(c) (emphasis added).

exception.¹⁶ The first part of the requirement, disclosing the reason for a denial, would not be feasible in many instances, such as where the denial is related to a law enforcement investigation or to exercise or defend a legal claim.¹⁷ The last part of the proposed requirement, which in effect institutes processing limitations for some of the personal information that must be maintained, raises substantial operational challenges in the short-term. The AG instead should afford more flexibility for businesses, including by allowing them to refer to general disclosures in their privacy policy regarding why they may deny a request.

Section 999.313(d)(1). Subsection (d)(1) would require businesses that are unable to verify a deletion request to treat such request as an “opt-out of sale.”¹⁸ Businesses that cannot verify a deletion request, however, may not have sufficient data to identify the consumer and therefore execute a sale opt-out. Moreover, treating an unverified deletion request as an opt-out request conflicts with the purpose of verifying the consumer in the first instance – to ensure that the consumer actually is the person making the request. This proposed requirement goes well beyond the statutory requirements set forth in the CCPA, and is, at best, a substantial stretch of the AG’s rulemaking authority.

¹⁶ Proposed 20 CCR § 999.313(d)(6).

¹⁷ See Cal. Civ. Code §§ 1798.105(d)(8) (deletion exception to comply with a legal obligation), 1798.145(a)(2)-(4) (CCPA obligations should not restrict a business’s ability to comply an investigation, cooperate with law enforcement, or exercise or defend legal claims).

¹⁸ Proposed 20 CCR § 999.313(d)(1).

C. The Proposed Service Provider Regulations Contradicts the Statute – Section 999.314

Section 999.314(c). Subsection (c) would impose limitations on service providers' permissible uses of data in a way that contradicts and goes beyond the statutory definition of "business purpose" and "service provider." Specifically, subsection (c) would restrict service providers from using personal information it receives from a person or entity it services "for the purpose of providing services to another person or entity."¹⁹

This restriction conflicts with the statute. The CCPA explicitly exempts from the definition of "sale" disclosures to "service providers" for a broad list of enumerated "business purposes."²⁰ In turn, the law defines "business purpose" to include both "the business's or a service provider's operational purposes or other notified purposes."²¹ Further, the statutory text appears to contemplate a service provider using the personal information it receives from a business for business purposes of both that business and where the use is otherwise consistent with the CCPA, such as on behalf of more than one business.²²

The draft regulations, however, improperly focus on the business purpose solely of the *business*, and ignore the fact that the statutory definition of "business purpose" also includes the use of personal information for the "service provider's operational purposes or other notified

¹⁹ *Id.* § 999.314(c).

²⁰ Cal. Civ. Code § 1798.140(t)(2)(c).

²¹ *Id.* § 1798.140(d).

²² *See id.* § 1798.140(v).

purposes.”²³ Indeed, other provisions of the statute make clear that the legislature contemplated service providers using information on behalf of more than one business. Several of the activities included in the statute’s enumerated list of business purposes – in particular “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**”²⁴ – typically require the combination and use of personal information received from and for the benefit of multiple businesses in order to provide those services to the business that provided the data. Focusing solely on the business purposes of the business, as the proposed regulations do, would both render the bolded language surplusage, as well as potentially render impermissible a number of the activities explicitly included on the list of permissible business purposes.

Because business purposes may include using personal information received from one business in a way that might also provide some benefit to other businesses, the CCPA should be interpreted to permit the service provider to use the personal information that it receives in a way that might provide some benefit to itself or to its business partners, as long as such use is consistent with the business purposes identified in the written agreement between the business and the service provider and otherwise permitted by the CCPA.

Section 999.314(d). Subsection (d) would require 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

²³ Proposed 20 CCR § 1798.140(d).

²⁴ Cal. Civ. Code § 1798.140(d)(5) (emphasis added).

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.²⁵ This requirement creates new burdensome obligations for service providers that are beyond and unsupported by the statutory text.

D. Requests to Opt Out of the Sale of Personal Information – Section 999.315

Section 999.315(c). Subsection (c) would require that a business “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.”²⁶ But no such signals currently exist, and efforts to establish industrywide signals historically have had significant limitations, preventing them from being effective. There is no reason to expect CCPA-based signals would be anything but of limited use to the extent they are feasible at all. Moreover, the CCPA never contemplates such a requirement, raising significant questions about whether the AG has authority to adopt it.

Section 999.315(g). Subsection (g) is also unworkable as well as overly burdensome. This subsection would enable a consumer to use “an authorized agent to submit a request to opt-out on the consumer’s behalf if the consumer provides the authorized agent written permission to do so.”²⁷ CTA members’ experiences in Europe suggest that this “authorized agent” provision has the potential to result in huge volumes of requests generated by third parties acting as

²⁵ Proposed 20 CCR § 999.314(d).

²⁶ *Id.* § 999.315(c).

²⁷ Proposed 20 CCR § 999.315(g).

“authorized agents.” That volume will create huge burdens, especially for small businesses, which would be particularly exacerbated by any limit in the time afforded to businesses to respond in the proposed regulations.²⁸

IV. THE PROPOSED REGULATIONS SHOULD AFFORD FLEXIBILITY IN ESTABLISHING VERIFICATION PROCEDURES – Sections 999.323-999.325

While CTA supports the notion of a risk-based approach to verification, the proposed regulations are far too prescriptive.²⁹ As a practical matter, prescriptive verification requirements risk requiring companies to maintain security practices that have been superseded by later technological advances.³⁰ Further, general security policy favoring reasonable data security safeguards takes into account, among other things, a business’s resources and capabilities. A large business, for example, may be able to institute a complex verification procedure that requires different pieces of information for different requests. A smaller business, however, may need a uniform approach, and in so doing, must balance making that process seamless enough that consumers can easily exercise their rights, but also establish sufficient safeguards to protect consumers from pretexting and other frauds.

In this regard, section 999.323(b)(3), which requires businesses to consider a number of specific factors in determining the method by which the business will verify the consumer’s

²⁸ CTA also has concerns about section 999.315(f), which would require that a business notify all third parties to whom it sold data to in the 90 days prior to a consumer’s opt out request, and instruct them to not further sell the information. This requirement, which is not supported by the statute’s text, can invalidate agreements under which the data was sold. It therefore may raise concerns about an unconstitutional taking.

²⁹ See *generally* Proposed 20 CCR §§ 999.323(b)-(c), 999.324, 999.325.

³⁰ For instance, regulations that require a “password” raise questions about whether authentication through biometrics or other cutting-edge verification techniques suffice.

identity,³¹ is unworkable in practice for many companies. This level of customization and specificity may be feasible for a business that only holds the same type of personal information about each consumer. But very large businesses hold different types of data about different consumers and, to that end, the proposed regulation as drafted would imply that a business must have a verification process that can be tailored for each request – based on the types of personal information the business holds about the relevant consumer. This would be impossible to implement at scale.

Rather than introduce additional uncertainty into what verification mechanisms would be appropriate in particular contexts by listing the delineated factors, the regulations should simply require businesses to employ a reasonable, risk-based verification method that aims to protect the consumer and prevent malicious and fraudulent from obtaining information about a consumer. A requirement based on risk and reasonableness also has the added advantage of effectively requiring companies to adapt as the risks change and verification methods improve.

The best approach to verification is to require companies to impose reasonable verification safeguards, offering guidance about the factors the AG would consider in determining whether a business's practices were reasonable, but avoiding actual prescriptive requirements.

V. PARENTAL CONSENT METHODS SHOULD TRACK FEDERAL LAW AND REGULATION – Section 999.330(a)

Section 999.330(a) would establish the process for parents to consent to the sale of personal information of their children under 13.³² Rather than promulgate specific (and

³¹ Proposed 20 CCR § 999.323(b)(3).

³² *Id.* § 999.330(a).

potentially California only) parental consent and opt-in mechanisms, the CCPA regulations instead should refer to, and incorporate by reference, consent mechanisms already approved by the Federal Trade Commission (“FTC”) under the Children Online Privacy Protection Act (“COPPA”) and the agency’s COPPA Rule.³³ This approach would ensure that the CCPA regulations stay consistent and current, as it would incorporate for the CCPA any new methods later approved by the FTC – and it would do so without the need for a new rulemaking process. And importantly, allowing businesses to rely on the same parental consent mechanisms for COPPA as for the CCPA ensures that the businesses can provide parents one, consistent way in which they can control and provide consent regarding the use and disclosure of their children’s information.

VI. THERE IS NO NEED TO ADOPT OVERLY BURDENSOME RECORDKEEPING REQUIREMENTS – Section 999.317

The proposed regulations include recordkeeping requirements that are burdensome and unnecessary.

Section 999.317(b). Subsection (b) requires business to “maintain records of consumer requests made pursuant to the CCPA and how the business responded to said requests for at least 24 months.”³⁴ There is no reason for businesses to maintain consumer requests for that long a

³³ See <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/verifiable-parental-consent-childrens-online-privacy-rule>.

³⁴ Proposed 20 CCR § 999.317(b).

time period, which conflicts with the CCPA’s typical 12-month timeframe for many of its personal information collection and disclosure lookback requirements.³⁵

Section 999.317(g). Subsection (g) requires 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” to compile various “metrics” from the previous calendar year.³⁶ As an initial matter, however, the metrics calculation provides little value because there’s no distinction between valid and invalid requests and these channels tend to have a high spam rate. Further, the proposed regulation does not make clear – nor would it be clear in all instances in practice – whether a business “complied with” or “denied” a request. For instance, would an unverified request be “complied with” or “denied”?

In light of these issues, any required metrics may not actually yield useful information about how well a business is processing requests. Moreover, such data could be misleading, particularly if a particular business ends up receiving a significant number of fraudulent opt-out requests. Concerns about misleading data could force businesses in turn to needlessly spend time and resources justifying large denial rates.

In the end, there is no justification for adopting this burdensome requirement, which has no basis in the law itself. Rather than adopt a metrics requirement, the AG should focus on

³⁵ *E.g.*, Cal. Civ. Code § 1798.130(2) (disclosure in response to a request to know shall cover the preceding 12-month period).

³⁶ Proposed 20 CCR § 999.317(g).

ensuring business' compliance through investigations and enforcement, as the CCPA contemplates.

VII. CONCLUSION


CTA is concerned that certain of the proposed regulations add to the significant compliance burdens and operational challenges already imposed on businesses by the CCPA, and do so without a commensurate benefit to privacy. Rather than impose additional burdens, given the extensive efforts already underway for companies to comply with the CCPA, CTA encourages the AG to provide clarifications to remaining ambiguous or conflicting aspects of the law as well as afford additional flexibility that will ease the compliance burdens of well-intentioned companies, including in particular small businesses.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: /s/ Michael Petricone
Michael Petricone
Sr. VP, Government and Regulatory Affairs

/s/ Rachel Nemeth
Rachel Nemeth
Director, Regulatory Affairs

1919 S. Eads Street
Arlington, VA 22202


December 6, 2019

Message

From: Melanie Tiano [REDACTED]
Sent: 12/6/2019 10:15:39 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CTIA Comment in Response to Proposed CCPA Regulations
Attachments: 12.6.19 CTIA CA AG CCPA Proposed Regulations Comment.pdf

To Whom It May Concern,

Attached please find CTIA's comments in response to the Attorney General's proposed CCPA regulations. Please let me know if you have any questions.

Thank you,

Melanie



Melanie K. Tiano
Director, Cybersecurity and Privacy
1400 16th Street, NW
Washington, DC 20036
[REDACTED] (office)
[REDACTED] (mobile)
[REDACTED]

Before the
CALIFORNIA OFFICE OF THE ATTORNEY GENERAL
Los Angeles, CA 90013

In the Matter of)	
California Consumer Privacy Act Regulations)	45-Day Comment Period for
)	Proposed Regulations
)	

COMMENTS OF CTIA

Gerard Keegan
Vice President, State Legislative Affairs

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th St. NW, Suite 600
Washington, DC 20036
(202) 736-3200
www.ctia.org

December 6, 2019

TABLE OF CONTENTS

Introduction	1
I. 999.305 – Notice at Collection of Personal Information	3
II. 999.306 – Notice of Right To Opt Out of the Sale of Personal Information	4
III. 999.307 – Notice of Financial Incentives and 999.337 – Calculating the Value of Consumer Data.....	6
IV. 999.308 – Privacy Policy	9
V. 999.312 – Methods for Submitting Requests to Know or Requests to Delete	9
VI. 999.313 – Responding to Requests to Know and Requests to Delete	11
VII. 999.314 – Service Providers	14
VIII. 999.315 – Requests to Opt Out	16
A. 999.315(c) – Opt-Out Mechanisms.....	16
B. 999.315(f) – Opt-Out Response Timeline	16
C. 999.315 – Relationship to Deidentification	17
IX. 999.316 – Request to Opt In After Opting Out of the Sale of Personal Information	18
X. 999.317 – Training and Recordkeeping.....	19
XI. 999.325 – Verification of Non-Account holders	20
XII. 999.330 and 999.331 – Rules Regarding Minors	22
Conclusion	24

Before the
CALIFORNIA OFFICE OF THE ATTORNEY GENERAL
Los Angeles, CA 90013

In the Matter of California Consumer Privacy Act Regulations)))))	45-Day Comment Period for Proposed Regulations
---	-----------------------	---

COMMENTS OF CTIA

INTRODUCTION

CTIA¹ welcomes the opportunity to provide comments on the California Attorney General’s proposed regulations to implement the California Consumer Protection Act of 2018 (“CCPA” or “Act”).² CTIA appreciates that the Attorney General is working under demanding statutory deadlines and commends the efforts of the Attorney General’s Office to clarify many of the Act’s provisions. CTIA members are committed to protecting the privacy of their customers. Consumer trust is essential for the continued growth of the mobile ecosystem, and appropriate privacy protections are integral to building and maintaining this trust. Members of the wireless industry therefore have strong incentives to develop robust privacy programs and

¹ CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association’s members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry’s voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry’s leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

² See generally Cal. Civ. Code § 1798.100 *et seq.*

practices.³ As a result, for years, recognizing that protections must not stop at compliance with existing regimes, the wireless industry has embraced a leadership role on privacy.

Nonetheless, CTIA's view is that many of the proposed regulations are impermissible under the CCPA and California law more generally. As detailed in these comments, several provisions are outside the CCPA's grant of rulemaking authority, inconsistent or in conflict with the CCPA, or either unnecessary or unduly burdensome to effectuate the purpose of the statute. Some proposals suffer from more than one of these flaws.

In addition, CTIA is concerned that several of the proposed regulations, if adopted in the form of the current proposal, would cause widespread harm to consumers and companies. CTIA takes as a guiding principle that the Legislature intended to strengthen California consumers' privacy by requiring stronger safeguards for personal information and enabling consumers to exercise greater control over their information.⁴ CTIA is concerned, however, that many of the proposed regulations will have the opposite effect and will instead undermine existing privacy and data security protections. Moreover, several proposed regulations would require disclosures based on underlying requirements that are poorly defined or require companies to reveal information that they would otherwise be entitled to keep confidential. These proposals will cause consumer confusion, expose companies to an array of new legal risks, and create

³ See Comments of CTIA, *In the Matter of Developing the Administration's Approach to Consumer Privacy*, Nat'l Telecoms. and Info. Admin ("NTIA"), Request for Comments, Docket No. 180821780-8780-01 (Nov. 8, 2018) ("CTIA's Nov. 8 Comment to NTIA").

⁴ See An Act To Add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, Relating to Privacy (AB 375), at §§ 2(h)-(i) (approved on June 28, 2018) (stating that "California consumers should be able to exercise control over their personal information, and they want to be certain that there are safeguards against misuse of their personal information" and "it is the intent of the Legislature to further Californians' right to privacy by giving consumers an effective way to control their personal information").

Unless otherwise indicated, these comments cite to the codification of the CCPA at Civil Code section 1798.100 *et seq.* prior to codification of the amendments that were approved by the Governor on October 11, 2019.

unnecessary operational challenges for many companies – all without substantially advancing the CCPA’s purposes.

CTIA’s most urgent concerns pertain to the following sections and subdivisions of the proposed regulations:

- 999.307 – Notice of financial incentives.
- 999.313 – Responding to requests to know and requests to delete.
- 999.315(c) – Requests to opt out and treatment of user-enabled privacy controls to communicate opt-out choices.
- 999.317(g) – Recordkeeping and reporting requirements for certain businesses.
- 999.337- Calculation of value of consumer data.

However, to facilitate review by the Attorney General’s Office, CTIA provides its comments on the proposed regulations in the order in which they were published. In addition, where appropriate, CTIA provides proposed regulatory language to address some of the issues identified.

I. 999.305 – NOTICE AT COLLECTION OF PERSONAL INFORMATION

CTIA asks the Attorney General to withdraw subdivision 305(a)(3) from the proposed regulations. This proposal requires a business that intends to use personal information for purposes not disclosed in the notice given to consumers at collection to meet two conditions: (1) provide direct notice to affected consumers; and (2) obtain *explicit consent* for the new purpose.

To start, this proposed consent requirement is an impermissible extension of the CCPA’s requirements. Specifically, Civil Code section 1798.100(b) requires only notice to use personal information for purposes beyond those disclosed to the consumer at the time of collection.⁵ This

⁵ See Cal. Civ. Code § 1798.100(b) (“A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.”).

statutory provision does not include any indication that a business must obtain consent for such additional purposes, and it is beyond the Attorney General’s authority to create one.

Moreover, the Attorney General’s proposal to require consent to use personal information for purposes beyond those disclosed at the time of collection is unnecessary. The Federal Trade Commission (“FTC”) advises companies to obtain “affirmative express consent” before making “material retroactive changes” to their uses of personal information, *i.e.*, using personal information in a “materially different manner than claimed when the data was collected.”⁶ This standard fully protects consumers’ privacy without requiring them to give “explicit consent” for *all* changes to the use of previously collected personal information – even insubstantial changes that have no impact on their privacy interests, such as internal uses to improve services.

Subdivision 999.305(b) could also have the unintended and unfortunate effect of encouraging companies to be vague in their privacy notices. This subdivision would require a business to disclose “the business or commercial purpose(s)” for which it will use the categories of personal information that it collects; requiring explicit consent to use personal information for *any* additional purpose will likely encourage businesses to state these purposes in terms that are as broad and general as is permissible.

II. 999.306 – NOTICE OF RIGHT TO OPT OUT OF THE SALE OF PERSONAL INFORMATION

CTIA asks the Attorney General to clarify subdivision 999.306(d)(2) of the proposed regulations. As drafted, this provision could be interpreted to prohibit businesses from selling the personal information of a set of consumers whose information was collected during periods when the business has posted a notice of opt-out of sale. This would be an impermissible

⁶ See Fed. Trade Comm’n, *Protecting Consumer Privacy in an Era of Rapid Change* viii, 57 (2012); 15 U.S.C. §§ 45(a), (n) (stating unfairness standard).

extension of the CCPA’s requirements, which allows the sale of consumers’ information (for consumers over the age of 15) pursuant to notice of the right to opt out, and costly to businesses that would be prevented from using consumers’ information in ways the CCPA allows.

Specifically, Civil Code 1798.120(b) requires businesses, which sell consumers’ personal information to third parties, to provide notice to consumers of their right to opt out of the sale of their information. Civil Code section 1798.135 specifies the requirements of that notice and requires businesses to honor the request of any consumer who exercises their opt-out rights. These sections do not apply to businesses that do not sell consumers’ information to third parties.

Subdivision 999.306(d)(2) addresses treatment of consumers who are not provided with a notice of right to opt out. The proposed regulation would require that any such consumer be “deemed to have validly submitted a request to opt out,” (and therefore a business could not sell personal information about that consumer). While this provision makes sense for information collected during any period of time when a consumer was not provided with an opt-out notice, it does not account for situations where a business that initially does not sell a consumer’s personal information to third parties, but later changes its business practices and begins to sell consumers’ personal information.

In such a situation, although the CCPA would allow for the sale of information collected about a consumer *after* a notice of opt-out was posted, subdivision 999.306(d) could be interpreted to apply to *any* information collected regardless of whether it was before or after an opt-out notice was posted.

To address this conflict with the CCPA, the Attorney General should revise subdivision 999.306(d) to read as follows:

999.306(d) A business is exempt from providing a notice of right to opt-out if:

- (1) It does not, and will not, sell personal information collected during the time period during which the notice of right to opt-out is not posted; and
- (2) 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.**

III. 999.307 – NOTICE OF FINANCIAL INCENTIVES AND 999.337 – CALCULATING THE VALUE OF CONSUMER DATA

CTIA asks the Attorney General to revise the proposed regulations that relate to financial incentives. In their current form, these proposals exceed the Attorney General’s rulemaking authority and would require businesses to disclose information that will likely mislead consumers and may implicate proprietary information for businesses.

As an initial matter, subdivision 999.307(b)(5)’s requirement to disclose (i) “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 (ii) the basis of that estimate, goes beyond the bounds of the CCPA. Civil Code section 1798.125 requires a business that offers consumers financial incentives to notify them of those incentives, and section 1798.185(a)(6) limits the Attorney General’s rulemaking authority to “establishing rules and guidelines regarding financial incentive offerings,” with an emphasis on the understandability, language, and accessibility of the notice.⁷ Nothing in these statutory provisions – or other provisions of the CCPA – authorizes the Attorney General to create new elements that would be required to be disclosed under subdivision 999.307(b)(5).

⁷ See Cal. Civ. Code § 1798.185 (granting the Attorney General authority to issue regulations that require businesses to provide notices “in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings . . .”).

Additionally, the disclosures contemplated under subdivision 999.307(b)(5) are impracticable and potentially misleading to consumers. As the *Initial Statement of Reasons* (“*ISOR*”) published in conjunction with the proposed regulations acknowledges, methods for calculating the value of personal information vary widely, and consumers tend to value their information in subjective, context-specific ways, which makes it effectively impossible to assign a meaningful value to an individual’s personal information.⁸ At the same time, personal information typically gains value as part of a larger collection of information. In addition, the financial incentives that businesses offer may bear a closer relationship to the cost of providing services, rather than the value of personal information. The fact that, from the consumer perspective, the value of personal information is subjective – such that no uniform value can be assigned to it – is borne out by the fact that, for any incentive of a fixed amount, some consumers will accept the incentive and others will decline it. Given this inherent subjectivity on the consumer side, the only way to determine a fixed value of personal information is to consider it from the perspective of the company offering the incentive. And this is a simple analysis: for the company offering the incentive, the value of the personal information is the value of the incentive. The company sets the amount of the incentive knowing that some consumers will decline the offer, a result the company is willing to accept because it is unwilling to assign any greater value to the personal information. Thus, the value of the incentive and the value of the personal information are the same. Still, the Attorney General proposes to require companies to disclose specific monetary valuations of personal information to put consumers “in a position to

⁸ See *Initial Statement of Reasons (ISOR) for Proposed Adoption of California Consumer Privacy Act Regulations* 38 (2019).

make informed decisions on whether to opt in to the offered financial incentives.”⁹ At best, this information will overwhelm and confuse consumers. At worst, in some instances, it could mislead consumers by creating a false sense of certainty about the value of their personal information.

CTIA also objects to subdivision 999.307(b)(5) because it requires businesses to publish their own legal analysis of the financial incentives they offer. Specifically, under the proposal, a business must explain in its notice the basis on which it concluded that its financial incentive “is permitted” under the CCPA. This determination requires a business to apply Civil Code section 1798.125, among other provisions of the CCPA, to its specific financial incentive practices. In certain circumstances, this analysis may be subject to attorney-client privilege and, as a result, exempt from any disclosure requirement under the CCPA.¹⁰ In addition, subdivision 999.307(b)(5)’s disclosure requirements would likely require businesses to reveal trade secrets and proprietary information. Requiring businesses to reveal such information likely constitutes an impermissible taking of property.¹¹ Therefore, the regulations should specifically relieve businesses of complying with this requirement to the extent that doing so would reveal trade secrets or proprietary information, or any information subject to attorney-client privilege.

⁹ *ISOR* at 12.

¹⁰ See Cal. Civ. Code § 1798.145(b) (“The obligations imposed on businesses by Sections 1798.110 to 1798.135, inclusive, shall not apply where compliance by the business with the title would violate an evidentiary privilege . . .”).

¹¹ See, e.g., *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1012-13 (1984) (holding that a federal statute requiring public disclosure of trade secrets contrary to regulated companies’ “reasonable investment-backed expectation” was a taking under the Fifth Amendment).

IV. 999.308 – PRIVACY POLICY

CTIA asks the Attorney General to revise the detailed disclosures proposed under subdivision 999.308(b)(1)(d)(2) to better align with CCPA. To start, as drafted, this provision would require businesses to disclose in their privacy policies the categories of sources, the purposes of collection, and categories of third-party recipients for each category of personal information that they collect. This prescription goes far beyond the specific, limited categories of information that the CCPA requires businesses to disclose in their privacy policies and therefore exceeds the Attorney General’s rulemaking authority.

Subdivision 999.308(b)(1)(d)(2) also creates the potential for businesses to inadvertently disclose inaccurate information in their privacy policies. For many businesses, some of the details that are subject to disclosure (*e.g.*, the linkage between the type of personal information collected and the categories of third-party recipients) under this proposal may change frequently. It may be infeasible for businesses to update their privacy policies after each such change. To eliminate a significant burden and potential exposure of businesses to claims that they are deceiving consumers, the Attorney General should revise this proposal to better align with the CCPA.

Additionally, to ensure consistency with the statute, the Attorney General should be careful to use language that aligns with the statute. For example, to the extent that it remains in the final version, subdivision 999.308(b)(1)(d)(2) should be revised to use the word “sells” as opposed to “shares” as it is drafted in the current proposal.

V. 999.312 – METHODS FOR SUBMITTING REQUESTS TO KNOW OR REQUESTS TO DELETE

CTIA asks the Attorney General to revise subdivision 999.312(a) to reflect statutory amendments that were signed into law in October 2019. Among other things, this subdivision

specifically requires businesses to provide “two or more designated methods for submitting requests to know, including, at a minimum, a toll-free number”

This toll-free number requirement directly conflicts with Civil Code section 1798.130(a)(1). As amended by AB 1564, this statutory provision permits a “business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information” to provide an email address as the sole means by which consumers may submit requests to know. Accordingly, the Attorney General must revise subdivision 999.312(a) to exclude such businesses from the proposed toll-free number requirement.

In addition, the Attorney General should revise the two-step process that subdivision 999.312(d) would require in connection with requests to delete. It would require consumers first to submit a request that the business must verify. Only after a subsequent step in which consumers “confirm that they want their personal information deleted” would the proposed regulation allow the business to execute those requests.

This two-step process would impose unreasonable burdens on consumers and businesses. According to the *ISOR*, the intent behind the proposed regulation is twofold: to provide consumers with the opportunity to correct an accidental deletion request that may lead to an irrevocable deletion of personal information, and to provide businesses with additional assurance that consumers have made a clear choice to exercise their right to delete.¹² This intent is largely achieved through the requirement in subdivision 999.313 to confirm receipt of the request and provide information about how the request will be processed. This confirmation should provide sufficient notification to consumers about what was requested and provide an opportunity to change their minds if necessary. Mandating a two-step process, however, would disempower

¹² See *ISOR* at 16.

and frustrate consumers by adding steps that consumers must follow to exercise control over their personal information. Moreover, many companies have already developed interfaces through which consumers can request the deletion of personal information. For instance, some companies have developed “self-serve” dashboards and similar facilities for these purposes. Subdivision 999.312(a) should not wipe out the investments that businesses have made in these interfaces. The regulation should provide businesses with flexibility to implement these consumer-friendly approaches for requests to delete personal information, rather than mandating a rigid, two-step process.

VI. 999.313 – RESPONDING TO REQUESTS TO KNOW AND REQUESTS TO DELETE

CTIA urges the Attorney General to revise the unnecessarily and unreasonably stringent timing requirements proposed under subdivision 999.313. The Attorney General should also revise the impractical and burdensome requirements governing the substance and process of businesses’ responses to consumers’ requests to delete and requests to know.

Subdivision 999.313(a) would require businesses to confirm receipt of a request to know or request to delete within ten days of receipt. This time-period is too short and unnecessarily burdensome. The Attorney General should allow at least 10 *business* days to confirm requests to know or delete.

Subdivision 999.313(b) would also impose an unreasonably short deadline to respond to a request to know or request to delete. Specifically, this proposal would allow businesses 45 days *from the day of receipt* to respond to requests to know and requests to delete, irrespective of the time required to verify the request. Although the *ISOR* notes that 45 days is longer than historical

response times for notifying consumers of a breach,¹³ this comparison is inapposite. In the context of a breach, verification of an individual consumer’s identity before providing notice is typically unnecessary. This process differs significantly from responding to consumer requests to know and requests to delete. In the context of requests to know and requests to delete, individual identification is mandatory and an essential part of ensuring that consumer requests under the CCPA do not expose consumers to additional privacy and security risks. Moreover, the time required to verify requests will vary widely. It is reasonable to expect that verification for requests will take longer when a request implicates sensitive personal information.¹⁴ The 45-day timeline under subdivision 999.313(b) would place businesses in the position of balancing an artificial regulatory deadline with conducting verification to protect consumers’ privacy and security in connection with requests to know or delete. Accordingly, the Attorney General should amend the response period in subdivision 999.313(b) to run from the date the consumer is verified.

In addition, CTIA has two concerns about the substance of responses to consumers that the Attorney General proposes to mandate. First, subdivision 999.313(c)(5) would require a business that denies a request for specific pieces of information to “inform the requestor and explain the basis for the denial.” Similarly, subdivision 999.313(d)(6) requires a business to provide notice and an explanation of the basis of denial of a request for deletion. In many circumstances, however, it would be infeasible for businesses to provide such specific responses, and requiring specific responses could harm the public interest. Civil Code section 1798.145 makes clear that businesses’ obligations under the CCPA do not restrict their ability to comply

¹³ See *ISOR* at 17.

¹⁴ See, e.g., § 999.323(b)(3) (indicating that “more stringent verification process shall be warranted” when a request to know or a request to delete involves “[s]ensitive or valuable personal information” or a “greater risk of harm to the consumer”).

with requests relating to law enforcement investigations, cooperate with law enforcement agencies, or exercise or defend legal claims.

Subdivisions 999.313(c)(5) and (d)(6) not only conflict with this statutory provision but also call for companies to disclose information that could reveal the existence of, or compromise, law enforcement investigations. To address these concerns, the Attorney General should permit businesses to respond to denials of requests to know and requests to delete by directing the consumer to relevant information in the businesses' privacy policies.

CTIA's second concern about responses to consumers arises in connection with responses to requests to delete under subdivision 999.313(d)(1). This subdivision would allow a business that cannot verify a consumer who requests deletion to treat the request as a request to opt out of sale. According to the *ISOR*, "requiring a business to treat the request as a request to opt out of the sale of their personal information benefits the consumer by at least preventing the further proliferation of the consumer's personal information in the marketplace."¹⁵

This proposal is infeasible. If a business cannot verify the identity of a consumer who requests deletion, it necessarily lacks sufficient assurance to identify the consumer to whom to apply the opt-out request. Moreover, subdivision 999.313(d)(1) is phrased in a permissive manner: a business "may deny" a request to delete if the business cannot verify the identity of the requestor. This proposal conflicts with Civil Code section 1798.105(c), which requires compliance with a request to delete only if the request is verifiable. It is also inconsistent with consumer choice, which is a key purpose underlying the right of deletion. These aspects of subdivision 999.313(d)(1) leave this provision open to a significant potential for abuse and would impose serious operational burdens on businesses.

¹⁵ *ISOR* at 20.

VII. 999.314 – SERVICE PROVIDERS

CTIA urges the Attorney General to revise subdivision 999.314(c) to remove inconsistencies with the CCPA and the unreasonable burdens that this proposal would impose on service providers. As proposed by the Attorney General, subdivision 999.314(c) flatly prohibits service providers from using personal information obtained from different businesses or collected from direct interactions with consumers, unless the use is to “detect data security incidents” or “protect against fraudulent or illegal activity.”

This proposal conflicts with the CCPA in two ways. First, it conflicts with how the CCPA defines the relationship between businesses and service providers. A fundamental characteristic of a “business” is that it determines the “purposes and means of the processing of consumers’ personal information.” The absence of authority to determine the purposes and means of processing is equally fundamental to the definition of “service provider.” Subdivision 999.314(c), however, would preclude service providers from entering into contracts to serve multiple businesses, even if the businesses have given their approval for such arrangements (unless the purpose of processing fits within either of the subdivision’s exceptions).

In addition, subdivision 999.314(c) precludes consumers from providing consent to use their personal information in arrangements in which a service provider processes personal information on behalf of more than one business. The Legislature chose specific circumstances in which consumers may exercise consent, *e.g.*, the right to opt out (or opt in for consumers under the age of 16) of sale and the right to opt in to financial incentive programs.¹⁶ Other uses of personal information by businesses are not subject to limitations based on consumer consent.

¹⁶ See Cal. Civ. Code §§ 1798.120 and .125.

The Attorney General proposes impermissibly to override this statutory scheme by prohibiting a separate set of practices and leaving consumers with no ability to consent to those practices.

Moreover, subdivision 999.314(c) could have far-reaching negative effects on a company's ability to use personal information for beneficial data analytics applications (other than data security and anti-fraud). It also appears to prohibit service providers from combining personal information received from different entities to facilitate internal operations or improve the quality of their services. The Attorney General should not ban such uses, which generally benefit consumers and create little, if any, privacy risk.

To address conflicts with the CCPA and reduce operational and practical harms, the Attorney General should revise subdivision 999.314(c) to read as follows:

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. A service provider may, however, combine personal information received from one or more entities to which it is a service provider, **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.

CTIA also asks the Attorney General to withdraw subdivision 999.314(a) from the regulations. The CCPA defines a specific statutory boundary for entities that provide personal information processing services to other entities: only processing that is performed *on behalf of a business* is within this boundary.¹⁷ The processing of personal information of entities that are not businesses does not fall within the ambit of the CCPA. The Attorney General cannot redraw this clear statutory boundary, as subdivision 999.314(a) would do.

¹⁷ See Cal. Civ. Code §§ 1798.140(c) (specifying that a "business" must be operated "for the profit or financial benefit of its shareholders or other owners," among other requirements) and 1798.140(v) (providing that a "service provider" "processes information on behalf of a *business*," among other requirements) (emphasis added).

VIII. 999.315 – REQUESTS TO OPT OUT

A. 999.315(c) – OPT-OUT MECHANISMS

CTIA asks the Attorney General to withdraw proposals to expand the right to opt out under section 999.315 of the proposed regulations. Subdivision 999.315(c) would require businesses to treat user-enabled privacy controls, such as browser plug-ins, privacy settings, or other mechanisms, as valid requests to opt out. This mandate is a significant extension of, and is inconsistent with, the requirements of the CCPA. Civil Code section 1798.135(a)(1) specifies the one and only method by which consumers can convey their requests to opt out – through the “Do Not Sell My Personal Information Link” – as well as the processes that businesses must follow in response to such requests.

This statutory provision is unambiguous in its requirement and does not leave room for the Attorney General to mandate an entirely separate opt-out mechanism. Section 1798.135(a)(1)’s singular prescription stands in contrast to provisions governing the treatment of other consumer requests under the CCPA. For example, Civil Code section 1798.130(a) requires businesses to provide “two or more designated methods for submitting requests” in connection with the right to know or right to delete. Consequently, there is simply no support in the text of the CCPA for the Attorney General to create other mandatory opt-out mechanisms.

B. 999.315(f) – OPT-OUT RESPONSE TIMELINE

For similar reasons, proposed subdivision 999.315(f) exceeds the Attorney General’s rulemaking authority and is inconsistent with the CCPA. This proposal requires that, upon receipt of an opt-out request, a business must notify third parties to whom it sold the consumer’s information within the previous 90 days and instruct those third parties not to further sell the information. The business must also notify the consumer when the business has completed third-party notification.

These requirements are not only highly burdensome, but also conflict with the CCPA in two ways. First, Civil Code section 1798.135(a)(4) is forward-looking and, on its face, does not apply to sales of personal information that occur prior to the receipt of an opt-out request. Second, Civil Code section 1798.135(a)(4) clearly and expressly applies only to the business that receives the opt-out request. There is no suggestion here or elsewhere in the CCPA that businesses may have an obligation to forward these requests to entities to which they sold personal information.

CTIA also asks the Attorney General to extend the time within which businesses must execute opt-out requests. Subdivision 999.315(e) would require businesses to act on opt-out requests as soon as feasibly possible, but no later than 15 days from the date the business received the request. This time frame would create serious compliance challenges. Moreover, aside from stating that the 15-day deadline was chosen to “provide[] clarity” about a detail that is missing from the CCPA, the Attorney General offers no explanation for imposing such a short deadline. The Attorney General should consider a more flexible standard to define the deadline for executing opt-out requests, which would allow businesses to adapt their response times as opt-out technologies develop.

C. 999.315 – RELATIONSHIP TO DEIDENTIFICATION

Finally, CTIA urges the Attorney General to amend section 999.315 to clarify that none of its provisions require businesses to reidentify information. Civil Code section 1798.145(i) provides that the CCPA “shall not be construed” to require a business to “reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.”¹⁸ Although this rule of construction applies to the CCPA as a whole, it is

¹⁸ AB 1146 amended Civil Code section 1798.145(i) (to be recodified as section 1798.145(l)) to provide that a business does not need to “collect personal information that it would not otherwise collect in the ordinary course of

especially important in connection with the right to opt out – particularly given the proposal to require businesses to recognize additional opt-out mechanisms, as that could create greater privacy harms to consumers.

IX. 999.316 – REQUEST TO OPT IN AFTER OPTING OUT OF THE SALE OF PERSONAL INFORMATION

CTIA asks the Attorney General to withdraw subdivision 999.316(a) from the proposed regulations. Under this proposal, a consumer who wants to opt in to the sale of personal information (after previously opting out) must go through a two-step confirmation process. In the first step, the consumer would submit a request to opt in and, in a separate step, the consumer would have to confirm his or her request. The Attorney General asserts that this requirement is necessary “to correct an accidental choice to opt back into the sale of . . . personal information” and to “provide businesses with additional assurance that the consumer has made a clear choice to exercise their right to opt-in.”¹⁹

The Attorney General’s assertion of necessity does not justify this burdensome proposal. The Attorney General provides no support for the contention that customers will “accidentally” opt in to the sale of their personal information, or that businesses are in need of “additional assurances” about consumers’ opt-in choices.

Moreover, the two-step process proposed under subdivision 999.316(a) is inconsistent with the simple one-step process to opt out of sales provided under section 999.315. To respect consumers’ choices about sales of personal information – whether the choice is to opt in or opt out – the regulations should treat the two processes equally.

its business, [or] retain personal information for longer than it would otherwise retain such information in the ordinary course of its business” to comply with the CCPA. This amendment does not affect the provision concerning reidentification discussed above.

¹⁹ See *ISOR* at 26.

X. 999.317 – TRAINING AND RECORDKEEPING

CTIA asks the Attorney General to withdraw subdivision 999.317(g) from the proposed regulations. This provision would require businesses that annually buy, receive for commercial purposes, sell, or share for commercial purposes the personal information of four million or more consumers to compile and publish specific metrics in their privacy policies. These metrics include the following:

- The number of requests to know that the business received, complied with in whole or in part, and denied;
- The number of requests to delete that the business received, complied with in whole or in part, and denied;
- The number of requests to opt out that the business received, complied with in whole or in part, and denied; and
- The median number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt out.

The requirements in this section are burdensome, ill-defined, and do not advance the objectives of the CCPA.

Without identifying a specific source of statutory authority to mandate these reporting requirements, the *ISOR* simply asserts that subdivision 999.317(g) “is necessary to inform the Attorney General, policy makers, academics, and members of the public about business’ compliance with the CCPA.” Although the Attorney General may “fill in the details” of the CCPA through regulations, these proposed reporting requirements do not relate to any identifiable provision in need of clarification or elaboration. They are simply new requirements.

Additionally, these burdensome requirements are a poor fit for the *ISOR*’s stated goal of informing the Attorney General and various stakeholder groups about businesses’ compliance with the CCPA. The CCPA already provides the Attorney General with broad enforcement authority as the means to ensure that businesses comply with the law. Moreover, the high-level

statistics that businesses are required to report will shed little, if any, light on the many detailed judgments that will be necessary to determine compliance with any given provision of the CCPA.

Disclosing the metrics as required by this provision would undoubtedly lead to consumer confusion. For example, it is not clear what would constitute a request that is “complied with” or “denied.” Suppose that a business receives voluminous deletion requests from consumers but determines that the personal information covered by these requests is necessary to provide a service requested by the customer in the context of an ongoing business relationship, and the business therefore denies these requests. Under the proposed regulation, these decisions would be reported as blanket denials of consumers’ requests. As this example illustrates, subdivision 999.317(g)’s reporting requirements are likely to create a picture of CCPA compliance that is, at best, incomplete and, at worst, misleading.

To the extent that the Attorney General adopts subdivision 999.317(g), despite a lack of statutory authority, subdivision 999.317(g)(1)(d) should be modified to require disclosure of the “average” number of days within which the business substantively responded to requests to know, requests, to delete, and requests to opt out rather than the “median” number of days as the current proposal requires. The average is significantly easier to compute and provides a more accurate representation of how quickly a business responds to requests.

XI. 999.325 – VERIFICATION OF NON-ACCOUNT HOLDERS

Although section 999.325 helpfully clarifies how businesses can comply with verification requests from consumers who do not have password-protected accounts with the business, CTIA suggests that the Attorney General revise or eliminate the illustrative scenario described in subdivision 999.325(e)(1). This example involves retention practices that would violate industry standards.

Specifically, the scenario presumes that businesses may have payment card information on file and suggests that a business could conduct verification by requiring a consumer to “provide the credit card’s security code and identify a recent purchase made with the credit card to verify their identity to (sic) reasonable degree of certainty.” This verification method would require businesses to maintain credit card security codes (referred to as Cav2, CVC2, CVV2, or CID, depending on the payment brand). The Payment Card Industry Data Security Standard Council strictly prohibits this practice because of the extreme sensitivity of card security code data.²⁰ In addition, the retention practices that inform this example would violate best practices for data minimization and data segmentation.

Although the specific example provided in subdivision 999.325(e)(1) relies on and implicitly endorses poor data security practices, CTIA strongly supports the Attorney General’s use of examples to illustrate how businesses can comply with certain provisions of these proposed regulations. Indeed, the Attorney General should provide examples in additional sections of the regulations. For example, it would be extremely useful to provide examples that illustrate how the Attorney General will assess security and privacy risks when evaluating consumers’ requests to know or requests to delete information, as described in subdivision 999.323(b).

In addition, CTIA recommends that the Attorney General revise subdivision 999.325(c) to eliminate the suggestion that businesses must obtain declarations signed under penalty of perjury from consumers who request to know the specific pieces of personal information the business has collected about them. The proposed regulation imposes a high bar on businesses verifying such requests by subjecting them to a verification standard of a “reasonably high

²⁰ See <https://www.pcisecuritystandards.org/faqs>.

degree of certainty,” which may include matching at least three pieces of personal information provided by 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. Obtaining and maintaining a declaration from the individual making the request would be a costly burden on businesses, and would not provide additional protections for consumers, given that fraudsters are unlikely to be deterred by providing a declaration; the actual protection under this provision would come from the suggested information-matching process. The Attorney General should therefore revise subdivision 999.325(c) 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.~~ Businesses shall maintain all signed declarations as part of their record-keeping obligations.

XII. 999.330 AND 999.331 – RULES REGARDING MINORS

CTIA requests that the Attorney General revise subdivision 999.330(b) to allow businesses to obtain verifiable parental consent for the sale of personal information of children under 13 by using any of the methods for obtaining parental consent specified in the Federal Trade Commission’s (FTC) Children’s Online Privacy Protection Act Rule (“COPPA Rule”).²¹ Subdivision 999.330(a)(2) includes some, but not all, of the methods to obtain consent permitted by the COPPA Rule.

²¹ See generally 16 C.F.R. part 312; see also 16 C.F.R. 312.5 (defining verifiable parental consent standards under COPPA).

Modifying the proposed regulation to track the COPPA Rule promotes consistency and efficiency for businesses that have already developed and maintain COPPA compliance programs. Moreover, tying the California regulation to COPPA’s permitted methods would allow businesses to utilize any additional innovative verification methods for obtaining consent approved by the FTC. Indeed, the FTC is currently conducting a review of the COPPA Rule, and specifically asks whether “there are additional methods to obtain verifiable parental consent, based on current or emerging changes which should be added” to the Rule.²² Therefore, CTIA recommends replacing subdivision 999.330(a)(2) with the following proposed regulatory language:

999.330(a)(2). Methods that are reasonably calculated to ensure that the person providing consent is the child’s parent or guardian include any of the methods enumerated in the Children’s Online Privacy Protection Rule at 16 C.F.R. § 312.5.

CTIA also requests that the Attorney General clarify that subdivision 999.331(a)’s provision for opt-in consent by minors between the ages of 13 and less than 16 only applies if the business intends to sell such personal information. CTIA offers the following proposed regulatory language to address this issue:

999.313(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 intends to sell such personal information**, it 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.

²² See Request for Public Comment on the Federal Trade Commission’s Implementation of the Children’s Online Privacy Protection Rule, 84 Fed. Reg. 35,842, 35,845 (July 25, 2019).

CONCLUSION

CTIA appreciates the Attorney General's consideration of these comments and stands ready to provide any additional information that would help to inform the development of final regulations.

Respectfully submitted,

/s/ Gerard Keegan

Gerard Keegan
Vice President, State Legislative Affairs

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA

1400 16th St. NW, Suite 600
Washington, DC 20036
(202) 736-3200
www.ctia.org

December 6, 2019

Message

From: Else Feikje van der Berg [REDACTED]
Sent: 12/6/2019 5:50:29 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Datawallet comments on draft regulations pursuant to the CCPA
Attachments: Datawallet comments on draft regulations pursuant to the CCPA.pdf

Dear Mr. Becerra,

Please find attached comments from Datawallet Inc., regarding the Proposed Regulations from Oct. 10th.

Sincerely,

Else Feikje van der Berg

—
Else Feikje van der Berg
Head of Policy & Product Strategy
www.datawallet.com

About Datawallet

The Datawallet Consumer First Compliance platform is a comprehensive solution to help you easily and quickly achieve compliance with privacy regulations, including but not limited to CCPA and GDPR. Simultaneously, our platform provides a compelling experience for the consumer with Transparency and Control of the data they create with you. This builds Trust in your brand, a deeper relationship and long term Customer Retention.

Datawallet is:

1. A centralized single source of truth for both the consumer and the enterprise backed by immutable record Blockchain technology.
2. Simple to understand for the consumer and simple for the Enterprise to manage.
3. An architecture to capture Data Subject Requests (View, Download, Delete, Do Not Sell), create a workflow ticket and deliver the requested data in a secure manner, all recorded to the immutable Blockchain record.
4. An architecture to provide the consumer a transparent view into the Sources, Data and use cases for your Enterprise.
5. A Consumer Data Permissioning system where you provide a notification (no choices), a default opt/out, or default opt/in with the ability for the consumer to make an informed choice at a granular level.
6. A single source of Truth with Immutable Blockchain technology to very effectively facilitate audits and defend lawsuits.

The information contained in this email is intended only for its addressee and may contain confidential and/or privileged information. If the reader of this email is not the intended recipient, you are hereby notified that reading, saving, distribution or use of the content of this email in any way is prohibited. If you have received this email in error, please notify the sender and delete the email. We use updated antivirus protection software. We do not accept any responsibility for damages caused anyhow by viruses transmitted via email.

Diese Information ist ausschliesslich fuer den Adressaten bestimmt und kann vertrauliche oder gesetzlich geschuetzte Informationen enthalten. Wenn Sie nicht der bestimmungsgemaesse Adressat sind, unterrichten Sie bitte den Absender und vernichten Sie diese Mail. Anderen als dem bestimmungsgemaessen Adressaten ist es untersagt, diese E-Mail zu lesen, zu speichern, weiterzuleiten oder ihren Inhalt auf welche Weise auch immer zu verwenden. Wir verwenden aktuelle Virenschutzprogramme. Fuer Schaeden, die dem Empfaenger gleichwohl durch von uns zugesandte mit Viren befallene E-Mails entstehen, schliessen wir jede Haftung aus.



The Honorable Xavier Becerra
Attorney General
ATTN: Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

December 5th, 2019

Comments on draft regulations pursuant to the CCPA

Dear Mr. Becerra,

I represent Datawallet, a consumer first compliance platform that helps businesses easily achieve compliance with EU-GDPR, CCPA, and other US-privacy laws. We believe that the CCPA was born from a clear consumer-demand for disruption of the broken data-ecosystem, and the only approach to privacy is a consumer-centric approach. In the 21st century, businesses must go beyond the bare minimum of compliance and ensure an excellent customer journey—from the first contact, to DSR handling, and more—in order to succeed. We help businesses exceed consumer demands by providing real transparency and control about personal data.

I am writing to you to submit our comments and ask for clarification regarding the proposed Regulations. But first, I would like to commend you on the strong stance that has been taken on the protection of consumer data and privacy. On that note, here are two parts of the CCPA and the Draft Regulation that have our full support as consumers and personal data advocates.

1. Opt-in for new purposes (§999.305 (3))

We believe the opt-in provision to be absolutely essential because it removes the otherwise ever-present loophole that allows companies to simply collect and keep as much data as possible and—without the consumer's knowledge or consent—use that data in any number of ways, at any future time. Forcing companies to be explicit about the reasons and purposes at collection, and forcing them to ask for explicit opt-in consent for any new purposes, gives consumers the effective control over their personal data they deserve and need. We applaud this clause as real progress in terms of privacy and personal data protection.

2. Wide scope of the definition of personal information (1798.140)

With many data privacy initiatives, we've seen the focus on very specific verticals touching only certain parts of consumer data or strong lobbying efforts working to exclude whole industries.

The addition of the caveat “capable of being associated with” in the definition of PI is laudable and important. A broad scope of defining PI ensures that the CCPA is, in fact, protecting all consumer's data. We believe that a limitation of the definition of personal information in the Regulations, as has been requested by some commenters at the hearings, would reduce the effectiveness and broad level of protection of the CCPA.

In several recent proposals for federal privacy legislation (both from the [Democratic](#) and [Republican](#) sides), we have seen an explicit inclusion of content from messaging in the definition of personal information. By including these data, consumers would be better protected from messaging services, especially those that monetize data within “walled gardens” such as Facebook (which controls Facebook Messenger, WhatsApp, and Instagram). Among other benefits, it would put an end to businesses using private messages to serve consumers personalized ads without proper notice or recourse.

Below we list the issues where we believe clarification would strengthen the protection of consumers

3. Service providers

One point that we would be happy to see clarified is regarding the obligations facing service providers that are not also businesses. They are described in several provisions in the CCPA Bill Text and the Draft Regulations:

- Only one exemption in 1798.145 seems to be directed at service providers (“(3) *Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law*”), other global exemptions seem to only apply to businesses (“*The obligations imposed on businesses by this title shall not restrict a business's ability to...*”)
- Service providers may receive DSRs to know or to delete. If they choose not to comply with this request, they must explain the basis for the denial (§ 999.314 (d)) and inform the consumer to contact the business on whose behalf they operate.

- Service providers are liable for the fines for intentional violations (\$7,500, 1798.155) and for unintentional fines (\$2,500, 17206 of the California Business and Professions Code).
- Service providers do not seem to be liable for data breaches. 1798.150: “*Any consumer whose non-encrypted or non-redacted personal information (...) is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the **business**’ violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following (...)*”.

All clauses regarding notice rights, maintaining reasonable security measures, verification of requests, privacy policy, making available 2 methods for submitting requests, *etc.* seem to be only directed at businesses. Businesses are explicitly mentioned in these clauses, service providers are not.

We do not believe it would be acceptable if service providers do not need to verify the identity of data subjects (as per Article 4 of the Draft Regulations) nor check for exceptions (as per § 999.313 (c)(3)), but still have the freedom to deny or comply with requests for information, as per § 999.314 (d). It would also be unacceptable if they do not have to honor the non-discrimination clause nor need to maintain reasonable security measures, nor would they not be held accountable in case of data breaches (the \$100-\$750 fines do not seem to apply for them).

It would be helpful to clarify in the final regulations exactly which obligations service providers face, and what they need to do to achieve compliance.

4. User-enabled privacy controls as requests to opt-out

§999.314 (a) states that user-enabled privacy controls, such as a browser plugin or privacy setting or another mechanism, could be used by consumers to communicate an opt-out of sale request. These signals can be quite ambiguous. Many questions come to mind: Should “Do Not Track” signals, sent by browsers or plugins, be interpreted as opt-out of sale requests? What happens in case multiple settings are sending mixed signals (for instance: the Do Not Track signal is enabled, but cookie settings allow all cookies)? How should businesses handle the fact that there are no operational standards for these signals?

5. Exceptions to deletion requests

We would like to express concern about the broad exceptions a business may invoke to deny deletion-requests. The range of exceptions that can be invoked stands the risk of being abused for many different practices. Especially 1798.105 (d)(1), stating that a business does not need to delete information that is needed to provide a good or service requested by the consumer, is unnecessary. In this case, businesses should be obliged to point out that the data is needed to provide the service, however, if consumers insist they want their data deleted, the business should be forced to comply.

1798.105 (9) could also be interpreted widely (*“Otherwise use the consumer’s personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.”*) and therefore runs the risk of being used as a loophole. A narrower definition of these exceptions in the Regulations could help to avoid such abuse.

6. Purpose, business and commercial purpose

§999.305 (a)(3) and 1798.100 both mention that a business shall inform consumers of the purposes for the usage of personal information. This term “purpose” seems not to be related to the terms “commercial purpose” or “business purpose” as defined in 1798.140, and is therefore left rather open. An unambiguous clarification in the Regulations would be helpful.

We are pleased to see that the CCPA includes an exhaustive list of the term “business purpose” and defines “commercial purposes”, to leave little room for doubt about which use-cases are covered. However, the inclusion of the wording “providing advertising or marketing services” in 1798.140 (d)(5) gives businesses a lot of leeway in using personal information in ways that are usually not necessary for the business to operate, and that can have a massive negative impact on the consumer. The next problem is that taking “advertising or marketing services” out of the definition of a “business purpose” would offer the consumer less, instead of more, protection. The CCPA and Regulations only state that information about business purposes or commercial purposes must be granted upon a data subject request. It is unclear what should be done with purposes that don’t fall under either definition. We would propose allowing consumers to opt-out of the usage of their information for purposes that can’t be considered business purposes or commercial purposes. The term “purpose” in §999.305 (a)(3) and 1798.100 should remain broad so that consumers will always be notified of all purposes of PI usage.



7. Lack of clarity about Real-Time Bidding practices and “walled garden” personalized targeting for advertising

There is an ongoing debate about whether Real-Time Bidding practices, as often used by publishers, constitute a “sale”. Publishers submit certain pieces of specific information (such as IP addresses) to ad networks, this information flows to multiple downstream parties. The use of this PI increases the value of the impression, and therefore could be considered a “sale”. On the other hand, the information is not being sold directly and the publisher is not earning revenue due to the ad network paying for the information. Clarifying this point would give much-needed certainty to businesses in the ad industry. The same question should be asked regarding “walled garden” advertising platforms such as Facebook, LinkedIn, etc. — in most cases, these platforms make money by selling an advertisement to other companies utilizing the personal information they have gotten from their customers. They also allow other companies to upload personal information (including, but not limited to phone numbers, home addresses, email addresses, full names or birthdays) which is then matched to the relevant person on the platform so that a personalized and targeted advertisement can be sold. There is a case to be made, that this does constitute a sale of PI even if the data does not leave the platform itself.

We look forward to seeing the Final Regulations and want to thank you for all your work on the important topic of privacy and data protection.

Sincerely,

A handwritten signature in black ink, appearing to be 'Else Feikje van der Berg', written over a horizontal line.

Dr. Else Feikje van der Berg
Head of Policy & Product Strategy

Message

From: PJ Hoffman ([REDACTED])
Sent: 12/6/2019 3:02:20 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Electronic Transactions Association - Comment Letter - Privacy Regs
Attachments: ETA Comments - Privacy - AG Proposed Regulations.pdf

Good morning,

Please accept these comments on behalf of the Electronic Transactions Association.

PJ Hoffman
Director of Regulatory Affairs
Electronic Transactions Association
[REDACTED] Direct
[REDACTED]

Join Conversations and Make Connections On: [LinkedIn](#) [Facebook](#) [Twitter](#)

December 6, 2019

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

**RE: Strengthening Fraud Prevention Under the California Consumer Privacy Act
("CCPA")**

Dear Attorney General Becerra:

On behalf of the Electronic Transactions Association ("ETA"), we appreciate the opportunity to comment on the California Consumer Privacy Act of 2018 ("CCPA"). The payments industry makes dedicated efforts to use innovation to fight fraud and ensure that consumers have access to safe, convenient, and affordable payment services. ETA and its members strongly support privacy laws that allow companies to implement innovative tools to protect consumer privacy and data while fighting fraud. ETA supports efforts by policymakers to strengthen the fraud prevention components of the CCPA including through an express exception for use of data for purposes of fraud prevention.

ETA is the leading trade association for the payments industry, representing over 500 payments and financial technology ("FinTech") companies that offer electronic transaction processing products and services and commercial loans, primarily to small businesses. During 2018 in North America alone, ETA members processed over \$7 trillion in consumer purchases. ETA members include financial institutions, payment processors, FinTech companies, and all other parts of the payments ecosystem.

Executive Summary

ETA and its members support U.S. and international efforts to strengthen privacy laws to not only help industry combat fraud and but also disclose to consumers how their data is being used. As lawmakers and regulators explore additional ways to protect consumers, it is critical that government coordinate with the payments industry so that companies can continue to combat fraud and cybercrime and ensure consumers have access to safe, convenient, and affordable payment options and other financial services.

There are numerous existing consumer protection laws in the U.S. and around the globe that address data security and privacy, and which align with the payments industry's fraud fighting efforts. In the U.S., for example, financial information data is governed by federal laws, including the Gramm-Leach-Bliley Act and related Federal Trade Commission's Safeguards Rule and Consumer Financial Protection Bureau's Privacy Rule, as well as robust self-regulatory programs like the Payment Card Industry Data Security Standard, which sets forth requirements designed to

ensure companies that process, store, or transmit credit card information maintain a secure environment for such data. All of these laws and self-regulatory efforts recognize the critical role played by industry in combatting fraud, and they include provisions that allow for the targeted use and sharing of information by financial institutions and payments companies to protect consumers and to prevent fraud from occurring in the first instance.

Moving forward, ETA encourages policymakers to consider ways that law enforcement and industry stakeholders can continue to work together to develop new ways to combat rapidly evolving and increasingly sophisticated fraud and cybercrime. Working together, lawmakers, regulators, and the payments industry have kept the rate of fraud on payment systems at remarkably low levels. By continuing to collaborate, government and industry can provide consumers with access to safe and reliable payment services. Additionally, as different states and the federal government consider this important issue, it is important for policymakers to work together across state-lines to provide a consistent privacy framework without creating a patchwork of conflicting regulations.

Specific Comments

Notice at Collection of Information - §999.305(a)(3)

The proposed rule would add a new requirement that is above and beyond the statutory requirements laid out in the CCPA. Section 999.305(a)(3) of the proposed rule requires that if a company intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notices at collection, the business must directly notify the consumer of this new use and **obtain explicit consent from the consumer to use it for this new purpose.**

This requirement to obtain "explicit consent" for a new use goes well beyond the requirements of the CCPA which only requires, "A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section." 1798.100(b). In fact, this requirement could result in less specificity in privacy policies which goes against the purpose of the law.

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

Section 999.306(d)(1) of the proposed rule allows for a business to be exempt from providing a notice of right to opt-out if 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.

This requirement means that if a business did not sell personal information, and then did not have a "Do Not Sell" button, if it then chooses to sell personal information and has a button, then personal information collected about consumers during the time the button was not shown will be automatically subject to the opt-out. Accordingly, businesses will then have the option to request that consumers authorize the sale pursuant to 1798.135. First, this is counter to the text of the

CCPA, which allows for new uses of data pursuant to notice, whereas explicit consent is required under the proposed regulations. This is in contravention to the statute. In addition, there is 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.

Notice of Financial Incentive - §999.307(b)(5)

Section 999.307(b)(5) of the proposed rule requires an explication of why the financial incentive or price or service difference is permitted under the CCPA including: 1) An estimate of the value of the consumer’s data that forms the basis for offering the financial incentive or price or service difference; and 2) A description of the method the business used to calculate the value of the consumer’s data. This requirement is well above and beyond the requirements of the CCPA. ETA believes these requirements should not be included in the final rule, however, if these requirements are to be retained, this regulation should specifically relieve companies from having to reveal any trade secrets or proprietary information.

Privacy Policy - §999.308

The proposed regulations have inconsistent phrasing when compared to the statute. In Section 999.308(b)(1)(d)(2), the word “shares” is used when in the same context in the statute (1798.130(a)(5)(C)(i)) it refers to the work “sells”.

ETA recommends the following changes to the language to ensure consistency with the statute.

Section 999.308(b)(1)(d)(2) - “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~~^{sells} personal information. The notice shall be written in a manner that provides consumers a meaningful understanding of the categories listed.”

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

The proposed regulation needs to be revised to allow for businesses that interact with consumers online only to not have to have the toll-free number requirement, but instead to have an email option. This is specifically addressed in California Assembly Bill 1564 which passed in October 2019, which provides that a business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information is only required to provide an email address for submitting requests for information required to be disclosed.

In proposed regulations Section 999.312(d), a business is required 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. Mandating a two-step process 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; in some cases, it may make sense to have a two-step process, in other cases it may not.

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

Under the proposed regulations Section 999.313(a), a business must confirm receipt of a request within 10 days. Given the challenges with providing information on demand, ETA recommends that businesses have up to 10 business days rather than just 10 days.

In proposed regulations Section 999.313(c)(5), 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. If the request is denied only in part, the business shall disclose the other information sought by the consumer. Several exceptions relate to issues where disclosing the basis for the denial is not feasible: such as for law enforcement purposes, exercising or defending legal claims, regulatory investigation, or criminal inquiry. ETA asks that the regulations include clarification that if a company includes the CCPA exemptions in their privacy policy they can just point consumers to those exemptions on their privacy policy and note that they are not responding because of an exemption listed in the privacy policy per CCPA.

In proposed regulations Section 999.313(d)(1), for requests to delete, if a business cannot verify the identity of the requestor, the business may deny the request to delete. The business must inform the requestor that their identity cannot be verified and shall instead treat the request as a request to opt-out of sale. This requirement goes above and beyond the statutory language in the CCPA. Additionally, if a business can't identify identity for purposes of deletion, how can it effectuate an opt-out? This entire requirement runs counter to the verification requirements in the regulation.

In proposed regulations Section 999.313(d)(6)(a), where a business denies a consumer's request to delete the business must 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. A company is simply not required to comply with the law if an exemption applies and therefor it is not a "denial." This requirement should be clarified to allow for companies to direct consumers to their policies explaining possible exemptions.

Service Provider – Protecting Against Fraud - §999.314(c)

In proposed regulations Section 999.314(a), a person or entity that provides services to a person or organization is not a business so long as it 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 the purposes of CCPA. When a person or entity is providing services to an organization that is not a business under CCPA, it is illogical for any requirements to be imposed on such service providers. As such, ETA recommends the following language to replace Section 999.314(a):

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.

In proposed regulations Section 999.314(c), a service provider may combine personal information received from one or more entities to which it is a service provider, on behalf of such business, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity. ETA supports efforts to provide additional clarity and flexibility for the payments industry to use data to protect consumers by fight fraud. These types of clarifications help payments companies to continue to innovate and find new ways to detect, deter, and eliminate fraud on behalf of consumers and merchants. However, the proposed language is limiting as currently written and could 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 providers services that it provides for businesses generally. To that end, the text should be modified as recommended below:

Section 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. 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, 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.

In proposed regulations Section 999.314(f), a business must 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. This requirement is beyond the scope of CCPA. The CCPA does not have this requirement to notify anyone to whom data was sold in the prior 90 days. Additionally, this is not feasible in that businesses would not have control over how third parties treat the data.

Training- Record-Keeping - §999.317(g)

In proposed regulations Section 999.317(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, must compile a number of metrics from the previous calendar year and disclose that information in their privacy policy.

This is a new onerous requirement is outside of the scope of the CCPA's statutory language. It is also unclear what would constitute a request that is "complied with" or "denied." For example, if a consumer could not be verified, how would that be characterized? What about statutory exemptions? This requirement would be very hard to comply with and could produce numbers that do not accurately represent accurate numbers for consumers.

Verification for Non-Accountholders - §999.325

In proposed regulations Section 999.317(g), one illustrative scenario which is used is for a business to maintain the consumer's name and credit card number, the business may require the consumer to provide the credit card's security code and identifying a recent purchase made with the credit card to verify their identity to reasonable degree of certainty. However, according PCI Security Standards, it is prohibited for companies from maintaining the CVV code and storing it for future use.

When it comes to card data protection, the payments industry took the lead in developing the Payment Card Industry Data Security Standards ("PCI-DSS") to ensure the safety of cardholder data. The PCI-DSS sets forth requirements designed to ensure companies that process, store, or transmit credit card information maintain a secure environment for such data. In addition, the PCI-DSS establishes a framework for implementation of those data security standards, such as assessment and scanning qualifications for covered entities, self-assessment questionnaires, training and education, and product certification programs.

According to the PCI-DSS FAQ, "PCI DSS does not prohibit the collection of card verification codes/values prior to authorization of a specific purchase or transaction. However, it is not permitted to retain card verification codes/values once the specific purchase or transaction for which it was collected has been authorized... All card verification codes/values must be completely removed from the entity's systems... A customer's request or approval for an entity to retain the card verification codes/values has no validity for PCI DSS and does not constitute an allowance to store the data."¹

ETA recommends that this scenario be removed from the final rule as it could be interpreted as a requirement.

The Role of the Payments Industry in Fighting Fraud

The payments industry is committed to providing consumers and merchants with a safe, reliable, and modern payments system. Indeed, consumers continue to choose electronic payments over cash and checks because of the protections afforded by electronic payments. These protections include, for example, zero liability for fraudulent charges, making electronic payments the safest and most reliable way to pay.

When it comes to credit cards, for example, a consumer can submit a chargeback request to his or her card issuing bank disputing a particular transaction. This process protects consumers and ensures that the financial institution bears ultimate responsibility for fraudulent transactions,

¹ PCI Security Standards Council FAQ, *Can Card Verification Codes/Values Be Stored On-File Or Recurring Transactions?*, Available at <https://www.pcisecuritystandards.org/faqs>. The PCI Security Standards Council is a global forum for the industry to come together to develop, enhance, disseminate and assist with the understanding of security standards for payment account security. The Council maintains, evolves, and promotes the Payment Card Industry Data Security Standards ("PCI DSS").

demonstrating the industry's strong interest in making sure fraudulent actors do not gain access to payment systems.

In addition, the payments industry has a long history of fighting fraud through robust underwriting and monitoring policies and procedures, and the use of advanced authentication technologies. With the benefit of decades of expertise, ETA members have developed effective due diligence programs to prevent fraudulent actors from accessing payment systems, monitor the use of those systems, and terminate access for network participants that engage in fraud. Working with its members and industry and government stakeholders, ETA has published various guidelines that provide underwriting and diligence best practices for merchant and risk underwriting, including the "Guidelines on Merchant and ISO Underwriting and Risk Monitoring" and "Payment Facilitator Guidelines," which provide information on anti-fraud tools, security, and related issues.

ETA members are constantly developing and deploying new technology and tools to detect, deter, and eliminate fraud. Just a few examples of these efforts include the following:

- **Data Encryption.** The payments industry has introduced point-to-point encryption (P2PE) and the tokenization of data to minimize or eliminate the exposure of unencrypted data in connection with a purchase.
- **Improved Authentication.** The use of new authentication methods to verify and authenticate transactions helps minimize potentially fraudulent transactions. These new tools include the use of the following types of advanced tools:
 - biometric authentication, including the use of thumbprints, facial, and voice recognition
 - geolocation that compares the merchant's location with the location of the consumers phone
 - behavioral biometrics (e.g., monitoring keystrokes)
- **Fraud Scoring / Suspicious Activity Monitoring.** The payments industry continues to refine tools for monitoring and analyzing payment data for suspicious activity. With improvements in machine learning and artificial intelligence, the payments industry gains additional tools for identifying suspicious patterns in transaction data.
- **Chip Cards and EMV.** The payments industry has worked to replace magnetic stripes for credit and debit cards with a computer chip card, also called EMV. Chip cards make our payments system stronger by protecting against theft, counterfeit cards, and unauthorized use of cards in stores.

These are just some of the tools that the payments industry has developed in recent years to fight fraud, protect consumers, and ensure the integrity of the payments ecosystem. These efforts have been remarkably successful in reducing fraud while ensuring that consumers have access to fast, reliable, and safe payment options.

ETA Supports a Regulatory Framework that Recognizes the Efforts of Industry to Fight Fraud and Protect Privacy

ETA and its members support U.S and international regulatory efforts that encourage and respect industry efforts to combat fraud and disclose to consumers how their personal information is being used. Working together, lawmakers, regulators, and the payments industry have had remarkable success in protecting consumers and providing them with access to safe and convenient payment systems. This is achievable because the existing legal framework for protecting consumer privacy recognizes the important role of industry efforts in preventing and fighting fraud.

In the U.S., for example, laws have been passed to protect health information (HIPAA) and financial information (Gramm-Leach-Bliley Act and Fair Credit Reporting Act), and marketing activities are regulated through federal and state competition laws, as well as industry and activity specific laws, such as the Telephone Consumer Protection Act, Telemarketing Sales Rule, and CAN-SPAM regulations. These laws recognize the important role that industry plays in combatting fraud and provide provisions that allow for the targeted use and sharing of data to protect consumers and to prevent actual or potential fraud from occurring in the first instance.

Just a few of these U.S. laws include:

Consumer Protection Laws and Provisions Related to Industry Fighting Fraud
Gramm Leach Bliley Act ("GLBA"): The GLBA requires financial institutions to explain their information-sharing practices to customers and safeguard sensitive data. The GLBA has an exception to its information-sharing restrictions for information disclosed to "protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability." ²
Bank Secrecy Act ("BSA"): The BSA establishes various requirements for covered financial institutions to assist the government in identifying and combatting money laundering and terrorist finance. The BSA includes numerous provisions governing the sharing of information between covered financial institutions and law enforcement, as well as sharing of information between financial institutions in order to identify and report activities that may involve terrorist activity or money laundering.
Health Insurance Portability and Accountability Act of 1996 ("HIPAA"): This law provides data privacy and security provisions for safeguarding medical information. Under the HIPAA Privacy Rule, a covered entity can disclose protected health information to detect fraud, abuse, or compliance violations.
California Financial Information Privacy Act ("CFIPA"): The CFIPA governs financial institutions in California handling nonpublic personal information of the State's residents, including provisions related to consumer notice and the sharing of this personal information. The CFIPA creates an exception to its restrictions to allow sharing of consumer information

² 12 C.F.R. § 1016.15(a).

Consumer Protection Laws and Provisions Related to Industry Fighting Fraud

with nonaffiliated third parties "to protect against or prevent actual or potential fraud, identity theft, unauthorized transactions, claims, or other liability."³

Federal Trade Commission ("FTC") Act: Section 5 of the FTC Act prohibits unfair or deceptive business acts or practices, including those relating to privacy and data security. The FTC has recognized the need for industry to share information in order to fight fraud. In a 2012 privacy report, the FTC identified "fraud prevention" as a category "of data practices that companies can engage in without offering consumer choice" because they are "sufficiently accepted or necessary for public policy reasons."⁴

The Fair Credit Reporting Act ("FCRA"): The FCRA establishes a framework for the use and sharing of consumer reports and requires covered entities to develop and implement an identity theft prevention program. While not an explicit exemption, it has traditionally been understood that consumer information disclosed for the purposes of fraud prevention is not "consumer report information" subject to the restrictions of the FCRA.⁵

Telephone Consumer Protection Act ("TCPA"): The TCPA was designed to safeguard consumer privacy by regulating telemarketing using voice calls, text messaging, and faxes. In 2015, the Federal Communications Commission exempted from the TCPA calls from financial institutions intended to prevent fraudulent transactions, identity theft, or data breaches.⁶

Likewise, the legal frameworks in Europe and Canada respect the need for industry to share personal information in order to protect consumers from fraud. In Europe, the recently enacted General Data Protection Regulation (GDPR) recognizes the important role that industry plays in fighting fraud and expressly permits (a) "processing of personal data strictly necessary for the purposes of preventing fraud,"⁷ and (b) decision-making based on profiling that is used for fraud monitoring and prevention consistent with law. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) allows for the sharing of personal information without consent if it is "made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect

³ Cal. Fin. Code § 4056. While the CCPA does not contain an express fraud prevention exception from the substantive rights and protections in the law as a whole, for purposes of the opt-out requirement for the sale of a consumer's personal information, there is an argument that a business's disclosure of personal information to prevent fraud affecting the consumer would not amount to the "sale" of such information because the information is not being disclosed "for monetary or other valuable consideration." As discussed further in this letter, such language should indeed be clarified in the CCPA to preserve this vital consumer protection.

⁴ FTC, Protecting Consumer Privacy in an Era of Rapid Change, available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> at 36 (2012); see also id. at 39 (reaffirming this preliminary conclusion following review of public comments).

⁵ This view was supported by the court's decision in *Kidd v. Thomson Reuters Corp.*, 299 F. Supp. 3d 400 (S.D.N.Y. 2017), which concluded that Thomson Reuters was not a "consumer reporting agency" by virtue of a service that disclosed information to customers for fraud prevention purposes.

⁶ See *In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 et al.* <https://www.fcc.gov/document/tcpa-omnibus-declaratory-ruling-and-order>, CG Docket No. 02-278, July 10, 2015 at ¶ 129.

⁷ European Union, GDPR, Recital 47.

that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud. . . .”⁸

As lawmakers and regulators continue to explore new ways to protect consumers, ETA and its members encourage them to collaborate with industry to ensure that new laws and regulations are appropriately tailored to address specific needs – this ensures a balance between protecting consumers and allowing industry room to innovate and develop new and beneficial security practices and fraud detection and mitigation tools.

Conclusion

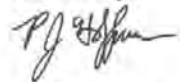
The payments industry never rests. We work tirelessly to fight fraud and protect consumers, including by developing new tools and solutions to prevent, identify and fight fraud by analyzing data. Privacy laws, such as the CCPA, should recognize these goals and the important role the payments industry plays in combatting fraud. By working together, lawmakers, regulators, and industry can protect consumers while providing them with access to the safest and most convenient payments system in the world.

* * *

Thank you for the opportunity to participate in the discussion on this important issue. If you have any additional questions, you can contact me or ETA Senior Vice President, Scott Talbott at

[REDACTED]

Sincerely,



PJ Hoffman
Director of Regulatory Affairs
Electronic Transactions Association

[REDACTED]

⁸ PIPEDA, Available at <https://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/118084/sc-2000-c-5.html>.

Message

From: Eric Goldman [REDACTED]
Sent: 12/6/2019 10:52:09 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Eric Goldman Comments to the California Department of Justice's (DOJ) Draft Regulations for the California Consumer Protection Act (CCPA)
Attachments: Eric Goldman Comments to CCPA Regulations Dec 2019.pdf

Eric Goldman
Professor, Santa Clara University School of Law
Co-Director, High Tech Law Institute & Supervisor, Privacy Law Certificate
Email: [REDACTED]
Personal website: <https://www.ericgoldman.org>
Blogs: <https://blog.ericgoldman.org> & <https://personal.ericgoldman.org>
Twitter: <http://twitter.com/ericgoldman>



Comments to the California Department of Justice's (DOJ) Draft Regulations for the California Consumer Protection Act (CCPA)

December 6, 2019

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

By email: PrivacyRegulations@doj.ca.gov

I am a tenured law professor at Santa Clara University School of Law, where I teach Internet Law. I submit these comments on the “proposed text of regulations” (the “regulations”) published by the California Department of Justice (DOJ) on October 11, 2019. These comments represent only my views and not the views of my employer or any third party.

The “Average” Consumer

Echoing California Civil Code 1798.185(a)(5), the regulations use the term “average consumer” five times (999.305(a)(2), 999.306(a)(2), 999.307(a)(2), 999.308(a)(2), and 999.315(b)). However, the term “average consumer” isn’t defined.

The “average consumer” standard does not represent the prevailing national approach in consumer protection law. The FTC expressly considered the appropriate standard for measuring consumer confusion in its 1983 Policy Statement on Deception. In that statement, the FTC adopted the standard of “a consumer acting reasonably in the circumstances.” This standard has served consumers and the FTC well for over three decades. Among other advantages, it avoids the indeterminacy of defining what constitutes an “average” consumer when a business caters to multiple heterogeneous consumer segments. The DOJ should define the term “average consumer” to track the FTC’s reasonable consumer standard.

999.301(s) defines a “typical consumer,” but its definition does not acknowledge either the “average” or “reasonable” consumer standard. The “typical consumer” definition should be harmonized with the “average consumer” definition and, like “average consumer,” should reflect the FTC’s “reasonable consumer” standard.

Exceptions to Requests to Know

999.313(c)(4) provides a list of items that pose too great a privacy/security risk if disclosed in response to a bogus request to know. The DOJ should consider expanding the list of undisclosable items that pose a heightened security risk.

Verifiable Consumer Requests and Rules vs. Standards

The legal requirements for verifiable consumer requests play a critical role in the CCPA. Businesses are legally required to honor verifiable consumer requests, but illegitimate requests can lead to major security violations that severely harm targeted victims. The regulations create legal liability for businesses in both directions: they face liability for dishonoring valid requests and liability for honoring some invalid requests. Because every consumer request creates potential legal exposure, businesses frequently will feel compelled to route consumer requests through customized legal review at substantial expense.

The DOJ can ameliorate the need for these expensive individualized determinations by providing concrete and specific bright-line rules of exactly what constitutes a verifiable consumer request, instead of requiring businesses to conduct fact-intensive, potentially irresolute, and expensive evaluations of legal “standards,” such as requiring “reasonable” behavior or balancing multi-factor tests.

The regulations for verifiable consumer requests represent a mix of rules and standards. The portions that are “rules” are helpful. For example, 999.325(b) and (c) provide bright-line rules for when businesses must disclose categories and specific pieces of personal information (indeed, these bright-line rules ought to apply to all consumer requests). Business’ ability to rely on password authentication is another helpful rule.

Elsewhere, the regulations adopt legal standards that will create substantial dilemmas for businesses trying to do the right thing. Most conspicuously, 999.323(b)(3) requires businesses to navigate a multi-factor test when evaluating consumer requests. The commentary in the Initial Statement of Reasons reinforces the imperative to get it right; the commentary says that “businesses have the responsibility to establish a reasonable method for verifying the identity of the person making the request.”

999.323(b)(3)’s multi-factor test creates many scenarios where well-meaning businesses won’t be sure what is the right decision. Further, those circumstances lend themselves to second-guessing by the DOJ. These dynamics will cause businesses to over-spend on these decisions. Thus, as a general proposition, with respect to what constitutes a “verifiable consumer request,” the DOJ should rely less on multi-factor tests and rely more on bright line rules.

Alternatively, the DOJ can provide more bright-line safe harbors, such as those in 999.325(b) and (c). As just one example, the DOJ could add a safe harbor for businesses that rely on an opinion of counsel about the reasonableness of their actions. However, opinions of counsel are expensive. Other safe harbors that businesses could implement at lower cost would benefit everyone.

Two other places where the DOJ imposes standards that should be converted to bright-line rules or subject to bright-line safe harbors:

- 999.313(c)(3) says that businesses should not honor a consumer request when disclosure creates a “substantial, articulable, and unreasonable” security risk. All three adjectives are standards, not rules, and they require substantial (and expensive) expertise and judgment to implement properly.
- 999.325(b) and (c) require businesses to verify a consumer’s identity with a “reasonable” and “reasonably high” degree of certainty. 999.325(d) then requires businesses to determine the applicable level of scrutiny “in good faith.” While many businesses will act in good faith, the indeterminacy of the “good faith” standard and fear of DOJ second-guessing will cause businesses to spend time and money preparing unnecessary documentation validating the good faith of their decision.

Note: 999.325(a) makes a cross-reference to a subsection (g) that does not exist.

999.325(b) requires some consumer requests to be made under “penalty of perjury.” In theory, this encourages submitters to submit only valid requests. However, will the DOJ devote any resources to prosecuting any perjured declarations? If not, the perjury declaration requirement will not adequately deter bogus requests. We’ve seen a similar dynamic with 17 U.S.C. § 512(c)(3), which specified the elements of proper copyright takedown notices. Per 17 U.S.C. § 512(c)(3)(A)(vi), the takedown notice sender must declare under penalty of perjury that he or she is the copyright owner or its authorized representative. However, in the two decades since the law’s enactment, I am not aware of any perjury prosecutions for misdeclarations. Perhaps not surprisingly, bogus copyright takedown notices are rampant. *E.g.*, Jennifer Urban et al, *Notice and Takedown in Everyday Practice*, Mar. 22, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628. If the DOJ expects the “penalty of perjury” declaration to discourage bogus consumer requests, it will need to commit resources to enforcement.

Rejecting Deletion Requests

999.313(d)(1) says that an unverifiable request to delete shall be treated as a request to opt-out of data sales. However, like other unverifiable consumer requests, the only proper outcome should be to disregard it. Otherwise, unrelated third parties—including malicious actors—can disrupt a consumer’s relationship with a business.

999.315(h) does not adequately mitigate this problem. A business can dishonor any request that it “has a good-faith, reasonable, and documented belief” is fraudulent. Unfortunately, there is a significant gap between *dubious unverified* requests and *obviously fraudulent* requests, even though dubious unverified requests may be pernicious. Due to 999.315(h)’s high legal standards and 999.313(d)(1)’s low legal standards, businesses will feel pressured to treat requests in that gap as opt-out requests even when pernicious to the victim.

The regulations could fix this by lowering the 999.315(h) standard or raising the 999.313(d)(1) standard. The better approach would be to scrap the concept entirely. The DOJ has assumed, without any supporting empirical evidence, that deletion requests are perfectly correlated with consumers' desire to opt-out of data sales. Unless and until the DOJ validates this assumption, the DOJ should not codify it.

Applying Deletion Requests to Archival Information

999.313(d)(3) says that businesses must process deletion requests on archival material upon its access or use. How will this work in practice? If a business wants to consult archival material for any reason, including for reasons that will never involve the data of consumers who have made deletion requests, the business must first process all prior deletion requests before doing anything else. This could add substantial and problematic time delays and expense to any attempts to access archival materials. Instead, the regulations should require businesses to process past deletion requests on archival materials only when the business' engagement with the archival materials relates to such consumers or when the business is converting archival materials into active usage.

“User-Enabled Privacy Controls”

999.315(a) and (c) require businesses to honor opt-out signals communicated by “user-enabled privacy controls,” an undefined term. Unfortunately, this proposal misunderstands the technology in two key ways.

First, though most consumers use one of only a few browser software programs, there are dozens or hundreds of other browser software programs in use, and new versions are constantly issued. Further, each software program independently decides how to indicate user preferences. Businesses cannot easily keep abreast of the complete universe of browsers and their idiosyncratic indications of consumer intent. Plus, honoring any new or changed browser signal takes time and money; it can't be implemented instantly.

Second, the browser software programs may ambiguously indicate consumer intent. The programs may give consumers a range of options, not just a binary yes/no to data sales. Or the program's way of characterizing its options to consumers may not clearly specify that it governs data sales, or the option may cover multiple unrelated topics.

Because the “user-enabled privacy controls” concept involves too much speculation about how browser software programs work, it's premature for the DOJ to adopt it. If the DOJ nevertheless retains the concept, it should (1) precisely define “user-enabled privacy controls,” (2) implement a formal certification process run by the DOJ (or DOJ-approved third party certification bodies) to validate which precise versions of browser software programs contain a “user-enabled privacy control” that unambiguously indicates its users' opt-out desires, (3) specify the technological details of each certified program so that businesses can accurately recognize and interpret the program's signals, and (4) provide a phase-in window for businesses to implement any newly certified programs.

Transparency Reports

999.317(g) creates a new obligation for bigger businesses to disclose various statistics about consumer requests. Disclosures like these are sometimes called “transparency reports.”

In general, I support transparency efforts. Transparency can encourage businesses to improve their behavior (because “what gets measured gets done”) and provide helpful data to researchers and government enforcers to identify problems with the existing laws and advocate for reform.

Unfortunately, I do not see how the regulation’s transparency report obligations will advance those goals. The regulations aren’t likely to improve business behavior (businesses are already obligated to comply with the law), nor is it clear who plans to mine the disclosed data and how the required disclosures will be helpful to them. Meanwhile, the transparency report obligations impose substantial additional expenses on businesses. The fact that larger businesses might have better financial capacity to bear the costs doesn’t obviate the need for cost/benefit justification.

The DOJ should eliminate the transparency report requirement from this version of the regulations and possibly reconsider it in future drafts when it’s clearer who plans to use the transparency reports and exactly what information those users need. If the DOJ nevertheless retains the requirement, it should include a phase-in requirement for businesses that newly cross the 4 million consumer threshold.

“Aggregate Household Information”

The DOJ should define the phrase “aggregate household information” as used in 999.318(a).

Non-Discrimination Provisions

Example 2 (999.336(c)(2)) did not make sense. How can a business keep providing price discounts to a consumer who deletes their identifying information?

Also, while the options in 999.337(b) are helpful, the validation requirements remain onerous overall. Many businesses, especially smaller businesses, lack precise data to take advantage of any of the options.

A GDPR Safe Harbor

In its Notice of Proposed Rulemaking Action, the DOJ indicates:

A less stringent regulatory alternative would, among other things, allow limited exemption for GDPR-compliant firms. Limitations would be specific to areas where GDPR and CCPA conform in both standards and enforcement, subject to auditing as needed. This approach could achieve significant economies of scale in both private compliance and public regulatory costs. The Attorney General rejects this regulatory alternative because of key differences between the GDPR and CCPA, especially in terms

of how personal information is defined and the consumer's right to opt-out of the sale of personal information (which is not required in the GDPR).

The GDPR offers many protections for California consumers that the CCPA does not. Thus, it's likely that if consumers actually understood both laws, many California consumers would regard the GDPR as equal or superior to the CCPA at protecting their interests. Meanwhile, everyone—including consumers—would benefit from the “significant economies of scale” and associated cost reductions that would come from a GDPR-compliance safe harbor to the CCPA.

What's Missing

The following two suggestions, related to the definition of “business” in California Civil Code 1798.140(c)(1), would help reduce unnecessary compliance costs.

First, the regulations should specify that the DOJ will only enforce the CCPA against businesses that generate \$25M revenue *in California*. As currently drafted, the law requires full compliance from out-of-state businesses that have \$25M in global revenue and “do business in California” (a notoriously ambiguous phrase) but derive minimal or no revenue from California residents.

Second, the regulations should provide a phase-in period for businesses that cross the CCPA's quantitative thresholds, such as a business approaching \$25M in annual revenue. Right now, the law functionally requires that business to implement the law before reaching the threshold so that it will be in compliance if revenues actually cross the threshold. However, this means the CCPA affects companies expressly outside its scope. To avoid this outcome, the regulations should specify that CCPA compliance is only required 6 or 12 months after the business crosses the applicable threshold. The same issue arises with the 50,000 consumer threshold in (c)(1)(B) and the 50% threshold in (c)(1)(C).

Thank you for considering my comments.



Professor Eric Goldman
Co-Director, High Tech Law Institute
Supervisor, Privacy Law Certificate
Santa Clara University School of Law
500 El Camino Real
Santa Clara, CA 95053



<http://www.ericgoldman.org>

<http://twitter.com/ericgoldman>

Message

From: Tengel, Brian R. [REDACTED]
Sent: 12/6/2019 5:16:38 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Experian Comments to the California Attorney General on CCPA Proposed Regulations
Attachments: Experian Comments to the California Attorney General on CCPA Proposed Regulations.pdf

Attorney General Becerra:

On behalf of Experian, please find attached comments on the proposed CCPA regulations.

Thank you,

Brian Tengel

Brian R. Tengel, Esq. | Venable LLP
t [REDACTED] | f 202.344.8300 | m [REDACTED]
600 Massachusetts Avenue, NW, Washington, DC 20001

[REDACTED] | www.Venable.com

This electronic mail transmission may contain confidential or privileged information. If
you believe you have received this message in error, please notify the sender by reply
transmission and delete the message without copying or disclosing it.



December 6, 2019

Via electronic filing

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

Re: The California Consumer Privacy Act Proposed Regulations

Attorney General Becerra:

I am pleased to offer the enclosed comments on behalf of Experian regarding the proposed regulations to implement the California Consumer Privacy Act of 2018 (“CCPA”).

As we noted in our previous comments dated March 8, 2019, Experian is comprised of a family of companies that are tied together by two simple objectives: (1) helping organizations protect, manage, and understand their data; and (2) helping consumers make informed choices and live smarter lives. Among the many products and services we offer, we facilitate consumers’ access to credit, protect families from identity theft, provide consumers expert education on credit management, and provide numerous anti-fraud tools to businesses.

The success of our business relies strongly on consumer trust and being good stewards of information. Consumer privacy is central to Experian’s corporate values, and we applaud the California legislature’s goal of increasing consumer privacy and transparency with the passage of the CCPA, as well as the Attorney General’s recent efforts to further the CCPA’s purposes through the subject regulations. We believe, however, that certain provisions of the proposed regulations need to be clarified by the Attorney General to further the objectives of the CCPA and to ensure that the law does not result in harmful, unintended consequences to consumers or impose unnecessary burdens on California’s business community. In addition to these clarifications, we also highlight issues below that, in our view, should be addressed by regulation.

1. *Businesses Holding Exempt Data Should Not Be Required to Inform Consumers that Their Personal Information Is Subject to an Exemption Under the CCPA*

Under Section 999.313(c)(5) of the proposed regulations, if a business denies a consumer’s verified request to know specific pieces of personal information because of an exception to the CCPA, the business must “inform the requestor and explain the basis for the denial.”¹ We

¹ Cal. Code Regs. tit. 11, § 999.313(c)(5) (proposed Oct. 10, 2019).

respectfully contend that, by requiring businesses to inform consumers that they hold data subject to an exception under the CCPA, this proposed regulation directly contravenes the plain language of the law. While certain types of personal information are wholly exempted from the CCPA, the effect of the proposed regulation will be to read them back in to the CCPA to subject them to burdensome CCPA disclosure requirements.

The CCPA provides that certain kinds of data are exempt from its requirements, including data subject to federal statutes like the Fair Credit Reporting Act (“FCRA”), the Gramm-Leach-Bliley Act (“GLBA”), and the Health Insurance Portability and Accountability Act (“HIPAA”).² In creating these exemptions, the California legislature recognized that sufficient protections already exist for such data in the form of comprehensive and robust federal laws and regulations. By requiring a business to disclose to consumers that their data is subject to an exception under the CCPA, Section 999.313(c)(5) would impose on certain businesses otherwise exempt from the law a new disclosure requirement of the type from which the legislature sought to relieve these businesses. Moreover, because many of the federal data statutes do not provide consumers with access, deletion, or opt-out rights, consumers would gain no additional benefit from a notice explaining that their CCPA request was denied because their data is subject to one of these federal statutes.³ The most likely result will be consumer confusion—as the number of disclosures proliferates, there will be increased uncertainty about where consumer rights do and do not apply and burdens upon businesses to resolve consumer confusion as to rights not available to consumers under the exempt laws.

Section 999.313(c)(5) would also prove extremely burdensome for businesses to implement. If this proposed regulation were adopted, businesses otherwise exempt from the CCPA would have to expend considerable resources developing and implementing brand new tracking mechanisms and recordkeeping systems to disclose to consumers information about data to which CCPA rights do not apply. Many businesses, indeed, have relied upon the substantive requirements of the CCPA and invested significant resources in developing and implementing compliance systems with certain capabilities, but that do not have the ability to query data sets with exempt data without potentially undermining or compromising nearly completed systems. The proposed regulation would thus require businesses to create a new class of systems and processes to report on exempt data.

We request that the Attorney General not require in Section 999.313 that businesses holding exempt data inform consumers that their personal information is subject to an exemption under the CCPA. This would honor the intent of the CCPA while protecting businesses from unnecessary compliance obligations. At a minimum, the Attorney General should clarify that

² Cal. Civ. Code §§ 1798.145(c)–(e).

³ We would note that, under the FCRA, consumers do have robust access, correction, and other rights with respect to their information, and Experian fully intends to guide consumers to the facilities it maintains where consumers can exercise those rights under the FCRA.

businesses may comply with this disclosure requirement through a standard disclosure in their privacy policies stating that they maintain data that is not subject to the CCPA.

2. Businesses Should Not Be Required to Share Opt-Out Requests with Third Parties

Section 999.315(f) of the proposed regulations requires a business to notify all third parties to whom it has sold consumers' personal information (within 90 days prior to the business's receipt of the consumer's opt-out request) that the consumer has exercised this opt-out right and instruct the third parties not to further sell the information.⁴ In addition, the business must notify the consumer when this has been completed. We respectfully submit that these requirements—to share opt-out requests with third parties and to notify consumers of the same—exceed the scope of the CCPA and would prove extremely burdensome for businesses while producing few benefits for consumers.

The CCPA provides in relevant part only 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, unless the consumer subsequently provides express authorization for the sale of the consumer’s personal information.”⁵ The proposed regulation thus exceeds the law’s scope, imposing substantive obligations with no textual foundation in the CCPA, and does nothing to “further the purposes” of the law—as the California legislature has required of any regulations that the Attorney General promulgates.⁶

This proposed regulation would prove burdensome for businesses by imposing new tracking and disclosure obligations. It would require businesses to expend considerable resources to develop and implement new systems, processes, and delivery mechanisms to manage and track opt-requests sent to third parties while ensuring that consumers receive adequate notice of this process.

Finally, the proposed regulation provides no additional benefits for consumers, who already have ample notices and means to exercise opt-out of the sale of their personal information and can expect businesses to honor these opt-out requests promptly within CCPA-required timeframes. The result of this proposed regulation—major burdens on businesses with few

⁴ Cal. Code Regs. tit. 11, § 999.315(f).

⁵ Cal. Civ. Code § 1798.120(d); *see also id.* § 1798.135(a)(4) (providing that a business shall “refrain from selling personal information collected by the business about the consumer” for consumers “who exercise their right to opt-out of the sale of their personal information”).

⁶ *Id.* § 1798.185(a) (providing that the Attorney General “shall . . . adopt regulations to further the purposes of this title”); *id.* § 1798.185(b)(2) (providing that the Attorney General “may adopt additional regulations . . . [a]s necessary to further the purposes of this title”).

meaningful benefits for consumers—is at odds with the California legislature’s intent to appropriately balance the costs to businesses and benefits for consumers.

We request that the Attorney General revise Section 999.315 to clarify that businesses are not required to share consumers’ opt-out requests with third parties and to notify consumers when this has been completed. Such a clarification would accord with the CCPA’s aims and would spare businesses from having to comply with onerous new requirements that do not meaningfully enhance consumer privacy.

3. Businesses Should Be Able to Satisfy Requirements for Third-Party Notice of Collection Through Contractual Provisions for Compliance

The CCPA does not address how a business that does not collect data directly from a consumer, but instead from another business, can provide the required notice at the point of collection. Section 999.305(d) of the proposed regulations seeks to clarify this issue by allowing a business to either (i) 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,⁷ or (ii) contact the source of the personal information to (a) confirm that the source provided a notice at collection to the consumer and (b) obtain signed attestations from the source describing how the source gave the notice at collection and obtain an example of the notice.⁸ The business must retain these attestations for at least two years and must make them available to consumers upon request.

We respectfully submit that this approach to providing notice would pose serious implementation challenges for businesses that make this requirement unworkable in practice. As an initial point, both options—contacting the consumer directly or contacting the source to obtain a signed attestation and an example of the notice provided—presume that the business has a direct relationship with either the consumer or the precise entity that acquired the data from the consumer. As a practical matter, however, businesses are often several steps removed from both the consumer and the initial data collector. Requiring businesses to contact them directly would thus prove administratively burdensome, if not impossible.

Even if businesses could identify the initial data source, moreover, requiring them to obtain signed attestations describing how the source gave notice and including an example of the notice would pose a separate set of implementation challenges. Requiring businesses to provide these attestations to consumers upon request would burden businesses but deliver no corresponding benefits to consumers, who cannot go back in time to when the personal information was collected to make a different choice. The net effect of these and other obligations would be to cut off data transfers in the marketplace, resulting in unintentional and unnecessary restrictions on legitimate,

⁷ Cal. Code Regs. tit. 11, § 999.305(d)(1).

⁸ *Id.* § 999.305(d)(2).

lawful, and beneficial data transfers that have limited bearing on consumer privacy and serve as a crucial part of the digital economy.

We request that the Attorney General revise the proposed regulation to provide that businesses may comply with the notice requirement through contractual commitments with their direct data source—as opposed to the original source—that all CCPA requirements have been met. For example, businesses could be required as an initial matter to conduct reasonable due diligence of their data sources to ensure they have the background and qualifications necessary to comply with the law. Businesses could then enter into written agreements with their data sources restricting improper or unlawful data practices and requiring the sources to develop, implement, and maintain a comprehensive data security program meeting CCPA requirements. Businesses would conduct reasonable monitoring of the data sources to ensure compliance with the written agreement. And to the extent businesses serve as data sources for other businesses, the requirements for data sources would apply to them as well.

Alternatively, we request that the Attorney General consider other options for providing the required notice. For example, businesses could meet the requirements in Section 999.305(d) through providing notice to consumers in widely distributed media throughout California, including through an annual advertisement. Another option could be permitting businesses to satisfy the notice requirements through their data broker registration database and set of disclosures to the public. These options illustrate the kinds of practical alternative notice that could provide transparency and choice for consumers while preserving the flow of lawful and beneficial data transfers critical to the digital economy.

At a minimum, given the challenges that the proposed regulation would present, we request that the Attorney General consider delaying the effective date of Section 999.305(d) for at least one year while also clarifying that the regulation does not extend to existing or past data collected by businesses. This would give businesses the time they need to adapt to these new requirements and to develop and implement processes for compliance, which are time-consuming and resource-intensive tasks given that the requirements are generally inconsistent with current data marketing practices.

4. Businesses Should Be Able to Satisfy Category-Disclosure Requirements by Providing Disclosures About General Business Practices and Categories

Section 999.313(c)(9) of the proposed regulations provides that, 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 must provide an individualized response to the consumer as required by the CCPA.⁹ This section further states that the individualized response shall not refer the consumer to the business's general practices outlined in its privacy policy unless

⁹ Cal Code Regs. tit. 11, § 999.313(c)(9).

its response would be 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. For its part, Section 999.313(c)(10) states that a business responding to requests to know categories of personal information shall provide for each identified category of personal information it has collected about the consumer (a) the categories of sources from which the personal information was collected; (b) the business or commercial purpose for which it collected the personal information; (c) the categories of third parties to whom the business sold or disclosed the category of personal information for a business purpose; and (d) the business or commercial purpose for which it sold or disclosed the category of personal information.¹⁰

We respectfully submit that requiring businesses to provide an “individualized response” to each consumer about categories of personal information, categories of sources, and categories of third parties, rather than disclosing to consumers general business practices and categories, exceeds the scope of the CCPA and would prove unduly burdensome while providing at best marginal benefits for consumers. Because many businesses do not track personal information elements in this manner, businesses would have to expend significant time and resources, including substantial coding efforts, to build out the technical capabilities to associate personal information by source, customer, and uses in order to enable businesses to provide responses specific to each individual consumer. And this assumes that such efforts would prove successful—it is very difficult to align generalized categories to what is happening with a specific consumer, and so it remains unclear whether and to what extent any coding efforts could reliably produce the type of individualized category response that the proposed regulation would demand. The expenditure of time and resources required to pursue this difficult goal would serve only to disrupt the important work that many businesses do every day to help organizations and consumers protect, manage, and understand their data.¹¹

Further, these burdensome requirements could omit information that is meaningful to consumers. For example, if a business sells data to 15 categories of third parties as a general practice but a particular consumer receives an “individualized” disclosure showing that his or her data has only been sold to five of those categories in the past 12 months, that consumer may not have a complete understanding of the possible uses of their data. He or she would only be aware of the categories to whom their data has been sold but unaware of the 10 other categories of third parties to whom their data *could* be sold. Providing a disclosure of all of the categories of third parties to whom a business sells data as a general practice would provide a more meaningful disclosure about the possible uses of that consumer’s data, allowing her to make a more informed decision regarding her rights under the CCPA.

¹⁰ *Id.* § 999.313(c)(10).

¹¹ At a minimum, if this proposed regulation were to become final, businesses would need additional time to comply.

We request that the Attorney General revise Sections 999.313(c)(9) and (c)(10) to clarify that businesses may satisfy the category-disclosure requirements by providing consumers with disclosures about general business practices and categories.

5. CCPA Access Requests Extend Only to Data that a Business Has Collected

The CCPA grants a consumer the right to request that a business that collects personal information about the consumer disclose to the consumer certain information about its data practices, including the “categories of personal information it *has collected* about that consumer,” the “categories of sources from which the personal information *is collected*,” and the “specific pieces of personal information it *has collected* about that consumer.”¹² The CCPA thus makes clear by its terms that consumer access requests extend only to personal information that has been “collected.” As a result of imprecise drafting, however, Section 999.301(n)(1) of the proposed regulations defines “request to know” in a manner that could be construed to sweep more broadly. That provision states that “request to know” includes a request for “[s]pecific pieces of personal information that a business *has* about the consumer.”¹³

By omitting the word “collected” in this provision, the proposed regulation could be read to mean that a business must disclose in response to an access request not only data that the business has “collected” about a consumer but also data that a business “has” about a consumer—potentially a far broader category of data that could include internally generated data that does not necessarily qualify as data that the business has collected. Such an interpretation would disrupt the reporting systems of companies that rely on internally generated data about consumers for business purposes and would create additional compliance burdens that the CCPA itself does not impose.

We request that the Attorney General revise Section 999.301(n)(1) to clarify that requests to know extend only to specific pieces of personal information that a business has collected about the consumer. Such a clarification would accord with the purposes of the CCPA while shielding companies from onerous requirements that the law does not intend.

6. CCPA Deletion Requests Extend Only to Data that a Business Has Collected

The CCPA gives consumers the right to request that a business “delete any personal information about the consumer which the *business has collected* from the consumer.”¹⁴ Consistent with this provision, the CCPA proposed regulations define “request to delete” as “a consumer request that a business delete personal information about the consumer that the *business*

¹² Cal. Civ. Code § 1798.110(a)(1)–(2), (a)(5) (emphases added).

¹³ Cal. Code Regs. tit. 11, § 999.301(n)(1) (emphasis added).

¹⁴ Cal. Civ. Code § 1798.105(a) (emphasis added).

has collected from the consumer, pursuant to Civil Code section 1798.105.”¹⁵ The privacy policy provisions of the proposed regulations, however, describe the right to deletion in a manner inconsistent with the CCPA. Section 999.308(b)(2)(a) provides that, in explaining the right to deletion, businesses’ privacy policies must “[e]xplain that the consumer has a right to request the deletion of their personal information collected *or maintained* by the business.”¹⁶

In light of this inconsistency with the statutory language, the Attorney General should revise Section 999.308(b)(2)(a) to clarify that requests to delete extend only to personal information that a business has collected about the consumer.

7. Businesses Should Not Be Required to Compile and Publicly Disclose Metrics About Consumer Requests Under the CCPA

Section 999.317(g) of the proposed regulations provides 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 must compile and disclose within its privacy policy or on its website certain metrics about requests to know, requests to delete, requests to opt-out, and the median number of days within which the business substantively responded to these requests.¹⁷ By requiring businesses to compile and publicly disclose detailed information like the number of requests to know they have received, complied with in whole or in part, and denied, this proposed regulation would create new public recordkeeping requirements with no textual basis in the CCPA that impose substantial obligations and add an extra layer of complexity to CCPA compliance. To compile and report the metrics that this regulation would demand, businesses would need to expend considerable resources developing and implementing internal tracking and monitoring systems to enable them to categorize and publicize each consumer request they receive and the disposition of the request. These requirements would create major costs for businesses while producing few meaningful benefits for consumers.

We request that the Attorney General revise Section 999.317 to clarify that businesses need not compile and publicly disclose these metrics about consumer requests. This clarification would accord with the CCPA, which does not provide authority for such a requirement, and would have no discernible effect on consumer privacy but would spare businesses from having to comply with additional requirements not intended by the CCPA.

* * * *

¹⁵ Cal. Code Regs. tit. 11, § 999.301(o) (emphasis added).

¹⁶ *Id.* § 999.308(b)(2)(a) (emphasis added).

¹⁷ Cal. Code Regs. tit. 11, § 999.317(g).

In addition to requesting that the Attorney General clarify the proposed regulations as set forth above, we also request that the Attorney General promulgate new regulations to address certain unintended consequences that could result from reasonable interpretations of the CCPA. As noted in our previous comments and as we have discussed, these new regulations would further the CCPA's purposes and ensure that businesses like Experian have the information they need to provide commercial credit reports as well as anti-fraud tools and services. Promulgating these regulations would also be consistent with the recent actions of the California legislature, which likewise recognized and sought to address certain unintended CCPA consequences for businesses when it amended the law earlier this fall to exclude personal data collected in the employment context and in a business-to-business context, until January 1, 2021.¹⁸

8. *Promulgate a New Regulation Clarifying that the CCPA's Reference to "Professional or Employment-Related Information" Excludes Business-Related Information in Commercial Credit Reports*

The CCPA's definition of "personal information," which helps set the boundaries for the scope of the law, includes the undefined concept of "professional or employment-related information."¹⁹ This language presumably reflects the judgment that sometimes an individual's profession or job helps define that person when marketers, retailers, or others offering consumer products or services are seeking to segment the consumer market. For example, certain generalizations made about blue-collar workers versus white-collar workers may hold true and be helpful for marketing purposes. However, as a result of imprecise drafting, this phrase in the CCPA could be construed to include any business or employment-related data regardless of whether or not the individual to whom the data is linked is acting in a consumer capacity. Such an interpretation would mean that all business-related information about an individual, and any associated information about the business (including financial information, business records, and other non-consumer information), potentially could be deleted or prevented from being shared under the CCPA.

There is a difference between the professional and consumer lives of individuals. The professional activities of Sally Smith, a hypothetical senior executive at Experian, need no privacy protection. Nor do the business activities of her spouse, Anthony Acosta, the sole proprietor of the Main Street Bike Shop. On the other hand, the CCPA reflects a consensus that the consumer activities of both Sally Smith and Anthony Acosta deserve privacy protection. Yet, commercial credit reports that Experian and other companies have provided to the market for decades include business and employment-related information and, therefore, may have inadvertently been swept

¹⁸ Cal. Civ. Code § 1798.145(h)(1)(A)–(C), (n)(1).

¹⁹ "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," including "[p]rofessional or employment-related information." Cal. Civ. Code § 1798.140(o)(1)(I).

into the law.²⁰ If commercial credit reports are covered by the CCPA, all data within those reports would be jeopardized because individuals and businesses may be able to use rights afforded by the CCPA to delete information in or prevent the sharing of information contained in them.²¹

The following are just a few of the many examples of the unintended consequences of interpreting the CCPA to cover the business-related information in commercial credit reports: (1) federal and state government agencies that use commercial credit reports (and their service providers) will not be able to conduct proper due diligence on their private sector contractors; (2) private sector efforts to fight fraud and money laundering through knowledge of banking customers gleaned through commercial credit reports will be hindered; (3) bank regulators that use commercial credit reports to understand banking relationships will not be able to reliably undertake safety and soundness checks; (4) businesses that use commercial credit reports for due diligence purposes will struggle to make informed decisions about service providers and partners; and (5) furnishers of business credit information may stop providing data, a move that would potentially result in unintended consequences for businesses, particularly small businesses and sole proprietors, whose good business credit histories afford opportunities that may otherwise be unavailable.

While we note, and applaud, the limited exceptions (until 2021) for personal information reflecting communications between the business and the consumer, and for personal information collected about a natural person in the employment context,²² we further request that the Attorney General promulgate a new regulation to clarify that the phrase “[p]rofessional or employment-related information” in the CCPA’s definition of personal information excludes information about individuals acting in their business capacities, *i.e.*, personal and related business information used in commercial credit reports. In particular, the Attorney General has specific authority to adopt rules to “updat[e] as needed additional categories of personal information.”²³ Clarifying through a new regulation that the phrase “[p]rofessional or employment-related information” excludes business representatives and sole proprietors listed in commercial credit reports creates an additional category of personal information pursuant to the law, as it delineates clearly the type of professional and employment information covered by the CCPA.²⁴

²⁰ This information includes data elements such as an individual’s name, address, birthdate, and tax ID number, as well as any judgments instituted against the individual, d/b/a information, and information from various Secretaries of State on commercial licenses the individual may hold, among other data points.

²¹ Although personal information contained in *consumer* credit reports is expressly exempted from the ambit of the CCPA, no such exception is made for data in *commercial* credit reports. Cal. Civ. Code § 1798.145(d).

²² Cal. Civ. Code § 1798.145(h)(1)(A)–(C), (n)(1).

²³ *Id.* § 1798.185(a)(1). As previously noted, the California Attorney General also has general authority to adopt rules to “further the purposes of this title.” *Id.* §§ 1798.185(a), (b)(2).

²⁴ Although there are material differences between the two statutes, it is noteworthy that California law already distinguishes between consumer and business data and the protections each deserves, insofar as the California Consumer Credit Reporting Agencies Act also makes a distinction between consumer data and business data,

9. *Promulgate a New Regulation Clarifying that the CCPA Exempts Data Processing for Anti-Fraud Purposes and Protects the Ability to Create Legitimate Fraud Prevention Tools*

The CCPA's exemptions do not fully exempt data processing for anti-fraud purposes. First, although the fraud exemption in the CCPA's data deletion requirement clearly covers users of fraud tools (who "maintain the consumer's personal information in order to . . . protect against . . . fraudulent . . . activity"),²⁵ arguably, the exemption does not cover Experian's data suppliers that provide information necessary to create those fraud tools because those data suppliers do not necessarily maintain the information in order to protect against fraudulent activity. The exemption also may not enable Experian's use of data to create and enhance anti-fraud tools because Experian does not just use these tools to protect Experian from fraud, but sells these tools in the marketplace for gain to enable businesses to protect themselves from fraud. Second, even though the CCPA clearly exempts data processing for anti-fraud purposes from the scope of the deletion right, the law is far less clear regarding an analogous exemption to the opt-out right for such anti-fraud data processing. As a result of the imprecise drafting in the CCPA, the law could inadvertently restrict the ability to gather the information needed to create, provide, enhance, or deliver anti-fraud tools and services, impacting the government and private sector actors that rely on these tools.

Since the CCPA provides consumers the right to request deletion of their personal information and/or opt-out from having a business share their personal information, consumer personal information that would otherwise be included in these fraud prevention tools may be deleted or prevented from being shared and used for anti-fraud activities that the CCPA endeavors to protect. Without the data needed to create, enhance, and update anti-fraud tools, users of these tools may not be able to prevent fraud. As an example of the many uses of these tools, the State of California uses Experian's fraud prevention tools to verify the age of lottery participants for the California Lottery and to review the California DMV's list of individuals owning a disabled person parking placard to ensure deceased individuals are removed from the program. Similarly, California hospitals and health providers use Experian's anti-fraud tools to perform identity checks on persons who use online patient portals to interact with California healthcare providers. These tools also underpin important federal programs: the Internal Revenue Service, for instance, uses Experian's tools to prevent fraud in its disbursement of tax refunds. Lenders and online merchants across the country also use the tools to reduce financial and marketplace fraud, including identity theft. If data about a particular consumer is not available to allow an entity to validate the identity of that consumer, this may impede the consumer's access to those services or benefits.

We request that the Attorney General promulgate a new regulation to clarify (1) the scope of the fraud exemption to the deletion right and (2) that such an exemption also exists for the opt-

classifying commercial credit reports as separate from consumer data in consumer credit reports. *See* Cal. Civ. Code § 1785.41.

²⁵ Cal. Civ. Code § 1798.105(d)(2).

out right in the CCPA. In particular, we request that the Attorney General clarify that the CCPA fraud exemption to the consumer deletion right covers the collection, use, and sharing of personal information to create and distribute fraud prevention and detection tools. We also ask the Attorney General to clarify that a parallel exemption exists for the opt-out right so consumers may not opt out of a business's sharing of personal information for fraud prevention purposes. We submit that these clarifications would further the purposes of the CCPA, as the CCPA already recognizes the importance of fraud prevention, the clarifications would ensure this policy outcome is achieved, and they would create a consistent policy position on anti-fraud data processing and tools throughout the CCPA.

* * * *

Thank you for this opportunity to provide input on the California Consumer Privacy Act rulemaking. Please contact me at [REDACTED] or by email at [REDACTED] with any questions or requests for additional information. We look forward to continuing to work with your office on these important matters.

Regards,



Jason Engel
Senior Vice President and General Counsel
Experian North America

Message

From: M. Forer [REDACTED]
Sent: 12/7/2019 12:55:28 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: privacy [privacy@doj.ca.gov]
Subject: Final Comments to State of CA, Dept. of Justice, Offices of the Attorney General - -Consumer Law Section-Privacy Unit before 12/6/19@5:00pm(PT)

To: Privacy Regulations Coordinator
California Office of the Attorney General
300 S. Spring St., Ste. 1702
Los Angeles, CA 90013
E: PrivacyRegulations@doj.ca.gov

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

Fri, December 6, 2019@4:55pm(PT)

To Whom It May Concern:

This last comment, by the undersigned, and a Safe at Home member, but also a member who is a "Former: Judge Pro Tem, Practicing Attorney w/Admission to the U.S. Supreme Court," is carefully, thoughtfully and factually supported and intended to convey and communicate before the strike of five o' clock Pacific Time occurs- -when comments to the DOJ are no longer allowed and welcomed by members of the public regarding AB 375 or the California Consumer Privacy Act- -the critical importance of reigning in, controlling and enforcing Alphabet, Inc. and Google, Inc. to respect and obey CA' s Government Code Sections 6205-6217, on behalf of the Safe at Home program participants throughout the State of California.

Call To Action by DOJ to Alphabet, Inc. and Google, Inc. for Safe at Home Program Participants:

With many concrete examples of written evidentiary proof over the years that the undersigned has collected and has in her possession, that could be shared with the DOJ, Google has shown a universal mitigated gall, lack of respect, and a failure to both respect the applicable CA Government Code Sections (see above) on behalf of Safe at Home members and/or keep the personally identifiable information ("PII") of Safe at Home members protected from being shared online for their security, safety, privacy for the protection of the individual members and also the members' family and/or relatives.

Enough disrespect and illegalities is enough.

With Google, the burden is on the Safe at Home members and never with Google. With Google, there are too many exhausting steps with overwhelming script to read, follow and adhere to. With Google, it' s always "contact the site host." With Google, it' s never what' s in the best interests of the Safe at Home members, but what' s in the best interest of Google (& accordingly Alphabet, Inc.).

Google is disrespectful toward a class of members that is legally protected to be physically and telephonically protected.

Google is negligent. Google is definitely not following the letter of the law or the substantive of the law in the applicable CA Government Code Sections.

Google must be reigned in and made mandatory to change their universal behavior in California, but also for each and every state in the USA on behalf of ALL Safe at Home members. Consider a class action lawsuit, if necessary.

Thank you for your time and anticipated thoughtfulness reading this comment and then taking illustrative steps for enforcement. Feel free to contact me for further information if you wish.

Enough is Enough.

Respectfully,
Michele Forer, JD
Safe at Home Member

Submitted on Fri, December 6, 2019@4:55pm(PT)

Message

From: Celine M. Guillou [REDACTED]
Sent: 12/6/2019 7:36:02 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Chiara Portner [REDACTED]
Subject: General Comments on CCPA Proposed Text Regulations

Dear Attorney General Becerra:

As data privacy attorneys representing a range of technology and non-technology clients, we seek additional guidance on the following points based on current feedback from many of our clients:

- With respect to the private right of action in the event of a data breach where a business fails to maintain reasonable security procedures and practices appropriate to the nature of the information being protected, there is a great deal of uncertainty as to how “reasonable security procedures and practices” will be measured. Clearly, the AG’s 2016 report drew relevant conclusions, but this report is more than 3 years old. We would appreciate (a) confirmation of the 2016 report conclusions or (b) additional clarifications with specific and practical guidance for companies of all sizes.
- With respect to the submission of requests to know by CA consumers, it would be helpful to clarify once and for all what methods must be made available by businesses that operate online or via mobile apps. The current language contained in s. 999.312 of CCPA Proposed Text Regulations is ambiguous at best.
- With respect to s. 999.314(c), additional clarifications would be extremely helpful. In addition, the use of PI by a service provider for internal analytics purposes only is not just common in current business arrangements, but a necessity for software platforms, which rely on internal analytics in order to improve their business and measure the effectiveness of certain tools.
- The definitions of “business”, “service provider” and “third parties” really ought to be further clarified and delineated, as many businesses operate on multiple levels. I draw your attention to the GDPR which provides for data controllers and data processors and lays out their respective obligations, while making clear that some companies may operate as both depending on their processing operations. Under CCPA, if a platform operates primarily as a service provider and collects PI on behalf of its multiple customers (and otherwise meets the first or second threshold), it is not clear where it stands.
- Some companies that operate on a B2B level feel that their collection of PI in connection with those relationships is exclusively subject to the limited exemption in section 1798.145(o). We would appreciate further clarification on the parameters of this exception.
- Finally, the multiple notice requirements appear to negate the intention of CCPA to provide clarity and an ease of understanding to consumers. If we follow the letter of the proposed regulations, the number of privacy notices to be posted will multiply and the length of these notices will double. Many of our clients operate on a global level and therefore subject to various privacy regulations. With CCPA, they now find themselves having 20+ pages of privacy-related language in order to comply. Any additional clarity on simplifying the notice requirements would be much appreciated.

Respectfully,

Céline Guillou, CIPP/E
Of Counsel

hopkins carley

Hopkins & Carley | A Law Corporation
San Jose | Palo Alto
200 Page Mill Road, Suite 200 | Palo Alto, CA 94306
Direct: [REDACTED] | Main: 650.804.7600
Fax: 650.804.7630

Any tax advice contained in this correspondence (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding tax-related penalties under federal, state or local tax law or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein. This email and any attachments thereto may contain private, confidential, and privileged material for the sole use of the intended recipient. Any review, copying, or distribution of this email (or any attachments thereto) by others is strictly prohibited.

If you are not the intended recipient, please contact the sender immediately and permanently delete the original and any copies of this email and any attachments thereto. For more information about Hopkins & Carley, visit us at <http://www.hopkinscarley.com/>.

Message

From: Famigletti, Rob ([REDACTED])
Sent: 12/6/2019 11:45:13 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Wugmeister, Miriam ([REDACTED]); Rich, Cynthia ([REDACTED])
Subject: Global Privacy Alliance's Comments on Proposed CCPA Regulations
Attachments: Global Privacy Alliance - Comments on Proposed CCPA Regulations - December 6, 2019.pdf

To Whom It May Concern:

Attached please find comments on the Attorney General's proposed implementing regulations for the California Consumer Privacy Act, submitted on behalf of the Global Privacy Alliance.

We appreciate the opportunity to submit this comment letter and welcome the opportunity to discuss any issues raised herein.

Best Regards,
Rob Famigletti

ROBERT FAMIGLETTI

Privacy Analyst | Morrison & Foerster LLP
250 West 55th Street | New York, NY 10019-9601
P: [REDACTED]
mofo.com | [LinkedIn](#) | [Twitter](#)

This message may be confidential and privileged. Use or disclosure by anyone other than an intended addressee is prohibited. If you received this message in error, please delete it and advise the sender by reply email. Learn about Morrison & Foerster LLP's [Privacy Policy](#).

December 6, 2019

Writer's Direct Contact
*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

**GLOBAL PRIVACY ALLIANCE
COMMENTS ON PROPOSED
CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS**

We write on behalf of the Global Privacy Alliance (GPA). We welcome the opportunity to submit comments on the implementing regulations (“Proposed Regulations”) for the California Consumer Privacy Act of 2018 (CCPA) proposed by the California Attorney General (AG).

The GPA is comprised of a cross-section of global businesses from the automobile, aerospace, communications, computer and computer software, consumer products, financial services, logistics, retail and e-commerce, and travel/tourism sectors. The GPA works to encourage responsible global privacy practices that enhance consumer trust. Members of the GPA take their privacy obligations very seriously. The views expressed herein generally represent the views of the members of the GPA. While all members support the overall approach presented in this letter, some of the individual points raised may not be relevant to all members.

The California Consumer Privacy Act of 2018

The CCPA is the most expansive generally applicable consumer privacy law in U.S. history. It established several core privacy rights for California residents (“consumers”) and imposes corresponding obligations on businesses. The CCPA was the product of an expedited legislative process and, as a result, contains errors, ambiguities, and contradictions. While several of these were subsequently corrected or clarified by legislative amendments, a number of uncertainties remain, rendering the AG’s implementing regulations particularly important.

December 6, 2019

Page Two

The California Attorney General's Proposed Implementing Regulations

The AG's Proposed Regulations, released on October 10, 2019, clarify certain aspects of the law and provide some helpful operational guidance, including with respect to the required contents of a business's privacy policy and the mechanics of handling consumers' requests. The Proposed Regulations, however, introduce several new ambiguities and, perhaps more troubling, several entirely new obligations not contemplated by the CCPA that will significantly affect businesses' compliance burdens without conferring added consumer benefits or protections.

These comments address provisions of the Proposed Regulations that the GPA recommends the AG revise or remove prior to issuing final regulations.

EXECUTIVE OVERVIEW

Consent

Imposing a blanket opt-in consent requirement for all new uses of personal information runs counter to the global trend in data protection law - *away* from a reliance on consent as the primary legal basis for processing and *toward* providing reasonable exceptions to consent for uses of data that consumers would reasonably expect to occur. This approach places a substantial burden on organizations without conferring added privacy protections on individuals. The final regulations should provide for common-sense exceptions to consent for certain new uses of individuals' personal information, consistent with other global privacy laws.

Consumer Requests

The Proposed Regulations' designated methods and processes for handling consumer requests create entirely new obligations that are logistically impossible and/or commercially nonviable. For example,

- Businesses are not equipped to implement mechanisms to receive consumer requests at each point of consumer interaction. Instead, businesses should be permitted to centralize the mechanisms by which they receive consumer requests. This approach will reduce businesses' barriers to compliance and help to ensure that consumers receive prompt responses to their requests.
- The proposed new and untenable, 10-day timelines by which businesses must respond to consumer rights requests. The timelines should instead adhere to the 45-day statutory requirement.
- The requirement to communicate a consumer's do-not-sell request to third parties to which the business sold the consumer's personal information is impractical and at odds with the concept of "sale." When data are sold, the seller does not maintain authority over the buyer's use of the data and should not be subjected to additional obligations.

December 6, 2019

Page Three

Service Providers

The Proposed Regulations' provisions regarding service providers' use of personal information will burden businesses and have unintended consequences that adversely impact both industry and consumers. A business and its service providers should have flexibility to contractually agree to uses of personal information, especially in light of the fact that those uses must be disclosed to consumers and with respect to which consumers have certain choices. Moreover, the requirement on service providers to respond directly to a consumer's CCPA request is overly burdensome and likely contrary to businesses' wishes. The final regulations should make clear that an entity responding as a service provider rather than a business has fewer obligations to respond to consumers and need only notify the consumer of the categories of sources of the personal information.

Notice

Several of the Proposed Regulations' notice obligations are unworkable and counterproductive to the notice principle. In particular, with respect to the timing of offline businesses' required notices to consumers, the Proposed Regulations' notice obligations will disproportionately burden retailers and other businesses that operate traditional "brick-and-mortar" establishments. The offline world is very diverse, and it is far from clear how offline companies could effectively provide notice at or before the collection of personal information (other than via an online privacy notice). Moreover, requiring a business to provide separate disclosures for each category of personal information it collects, and to include a *forward-looking* commitment not to sell consumers' personal information in its privacy policy to avail itself of the opt-out notice exemption, run counter to the notice principle.

Big Buyers/Sellers

Requiring big buyers and sellers of personal information to publish statistics is prone to error and not consumer-protective. The final regulations should eliminate this requirement or, at most, require such businesses to maintain the statistics and furnish them to the AG upon request. The final regulations should also clarify the method for calculating the statistics that big buyers or sellers must maintain and/or publish.

Verification Methods

The final regulations should give businesses the flexibility to craft risk-based approaches tailored to the types of personal information that the businesses collect.

Minors' Personal Information

The final regulations should specify that only businesses that intend to *sell* the personal information of minors should be required to establish opt-in processes for the sale of such information.

December 6, 2019

Page Four

Effective Date

The AG should exercise its statutory authority to provide for a later effective date for the final regulations.

Exceptions

The final regulations should establish exceptions necessary to comply with state or federal law relating to trade secrets, proprietary information, and intellectual property rights.

DETAILED COMMENTS

1. Imposing a blanket opt-in consent requirement for all new uses of personal information runs counter to the global trend in data protection law.

The CCPA dictates that “a business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with *notice* consistent with this section.” §1798.100(b). The Proposed Regulations expand this use limitation, requiring that “if the business intends to use a consumer’s PI for a purpose that was not previously disclosed to the consumer in the notice at collection, the business must directly notify the consumer of this new use and *obtain explicit consent* from the consumer to use it for this new purpose.” §999.305(a)(3).

In this respect, the Proposed Regulations mark a problematic departure not only from the CCPA, but also from the global trend *away* from a reliance on consent as the primary legal basis for processing and *toward* providing reasonable exceptions to consent for uses of data that consumers would reasonably expect to occur. Other jurisdictions have correctly concluded that an overreliance on consent results in “consent fatigue” (whereby individuals simply click “yes” without reading the underlying information) and, consequently, places a substantial burden on organizations without conferring added privacy protections on individuals. Most privacy laws worldwide, including the EU General Data Protection Regulation (GDPR), therefore provide for common-sense exceptions to consent for certain new uses of personal information.

For example, numerous global privacy laws, including the GDPR, do not require organizations to obtain an individual’s consent where his or her personal information is used for scientific research purposes. Under these laws, a company in the healthcare sector would *not* be required to obtain an individual’s consent to use his or her personal information, collected in the context of a clinical trial years ago, to subsequently use that data in a longitudinal study assessing the efficacy of pharmaceutical drugs and other treatment modalities. As drafted, the Proposed Regulations would require new consent in this context. This would often prove logistically impossible and detrimental to both public health and scientific innovation.

December 6, 2019

Page Five

The current provision would incentivize businesses to provide consumers with detailed and exhaustive lists of all theoretical uses of their personal information, solely in order to avoid the risk of having to obtain new consent. For example, consumers would not be able to identify the actual uses that the business plans for the information, as distinct from the theoretical uses that the businesses disclose in order to ensure that a future use would not be foreclosed.

Moreover, obtaining explicit consent for any new use of personal information is logistically difficult, given that a business may not have more than one opportunity to interact with a consumer. For example, a business that collected personal information in the context of a clinical trial and wishes to use that information for a related study would need to locate the individual, provide a new notice, and obtain a new consent. Similarly, a business might place a pop-up window on its website to solicit consent for a new use of a consumer's personal information, but not every consumer will visit the website after the consumer's initial interaction with the business. In addition, a business may not have current or accurate contact information for every consumer and may thus be unable to seek consent.

Finally, the Proposed Regulations' consent regime would require businesses to implement and maintain systems and processes to treat different consumers' personal information differently, not based on the sensitivity or classification of personal information, but based on the purposes of use to which each consumer consents. Such a standard is unreasonably onerous and unworkable in light of the negligible protection that it would afford consumers.

Accordingly, this provision of the Proposed Regulations should be revised for consistency with other prevailing privacy laws to provide for other permitted uses of personal information, including where such use is necessary to fulfill contractual obligations to the individual, required or authorized by law, or necessary to protect the individual or a third party's vital interests (*see, e.g.*, GDPR Articles 6 and 9). There should also be exceptions for scientific research or other uses that are in the public interest.

2. The Proposed Regulations' designated methods and processes for handling consumer requests create entirely new obligations that are logistically impossible and/or commercially unviable.

- a. Businesses are not equipped to implement mechanisms to receive consumer requests at each point of consumer interaction.*

While the CCPA dictates that a business must "make available to consumers two or more designated methods for submitting requests for information required to be disclosed, including, at a minimum, a toll-free telephone number" (§1798.130(a)(1)(A)), the Proposed Regulations would require some businesses to implement additional methods. Specifically, "at least one method offered shall reflect the manner in which the business primarily interacts with the

December 6, 2019

Page Six

consumer, *even if it requires a business to offer three methods for submitting requests to know.*” §999.312(c).

As an introductory matter, the CCPA’s requirement that every business (save for those that operate “exclusively” online)¹ maintain a toll-free telephone number to receive consumers’ requests will create issues for many companies. Implementing and maintaining a call center solely for receipt of consumer requests under the CCPA will prove prohibitive for many businesses, with respect to both cost and resources. The regulations should, instead, stipulate that if a business maintains a call center for other purposes, a toll-free number must be one of its designated methods for receiving consumer requests, and if not, the business may designate two other methods.

The Proposed Regulations only compound this burden by additionally requiring that a business’s designated methods reflect the nature of its interactions with consumers. Indeed, most businesses are not equipped to receive individual rights requests at each point at which they interact with consumers. For example, many businesses do not have the technological capabilities to create and implement fillable web forms by which to receive consumer requests. Also, as drafted, a consumer would be permitted to make an individual rights request at the cash register in a retail establishment. Such an approach is not contemplated by the CCPA nor by any other privacy law in the world. Instead, businesses should be permitted to centralize the mechanisms by which they receive consumer requests. Under the GDPR, for example, businesses are permitted to direct individuals to centralized methods for exercising their individual rights, regardless of whether those are the methods by which the consumer primarily interacts with the business. The benefits of such a model are twofold: it reduces businesses’ barriers to compliance and helps to ensure that consumers receive prompt responses to their requests. On the other hand, requiring businesses to implement individual rights request processes at each consumer touchpoint is nearly certain to result in some of those requests slipping through the cracks due to the volume of incoming requests, employee training and turnover, and human error, among other factors.

b. Businesses should not be required to monitor consumer requests submitted outside of their designated channels.

The Proposed Regulations introduce a burdensome requirement regarding businesses’ responses to non-compliant and possibly unexpected consumer requests. Specifically, “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.” §999.312(f).

¹ Assem. Bill 1564, 2019-2020 Reg. Sess., ch. 759, 2019 Cal. Stat.

December 6, 2019
Page Seven

Functionally, this will require businesses to monitor every channel through which a consumer could conceivably submit an individual rights request or contact the business. This requirement essentially reads out of the statute the obligation to have two designated methods of submission and imposes a new obligation on a business to honor every request, no matter how it is received. Establishing two designated methods for consumer requests is adequate; businesses should not be further required to staff and monitor all possible communications channels to recognize and route these requests or otherwise face liability.

c. The Proposed Regulations introduce new, untenable timelines by which businesses must act upon consumer rights requests.

The Proposed Regulations introduce an entirely new requirement that a business, upon receipt of a consumer's request to know or a request to delete, "confirm receipt of the request within 10 days and provide information about how the business will process the request." §999.313(a). Similarly, upon receipt of a consumer's request to opt of the sale of his or her personal information, a business must "act upon the request as soon as feasibly possible, but no later than 15 days from the date the business receives the request." §999.315(e).

There is no basis to add additional response steps and timelines to businesses' existing obligations under the CCPA. The new timeframes should be omitted from the final regulations, which should instead adhere to the statutory requirement that a business "disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable request from the consumer." §1798.130(a)(2). At a minimum, the final regulations should express any timelines by which a business must confirm and/or act upon consumer requests in *business* days.

Additionally, the requirement that a business provide a consumer with information about how it will process his or her request provides no value to the consumer and does not further the intent of the Act. The business's compliance with the Act should suffice; the business should not be further required to explain its *method* of compliance to the consumer.

d. Requiring businesses to communicate consumers' do-not-sell requests to other businesses is impractical and at odds with the concept of "sale."

The Proposed Regulations introduce another new requirement that "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." §999.315(f).

Imposing an obligation to inform other businesses of a consumer's do-not-sell request is impractical and inconsistent with the concept of a sale of data. When data is sold, the seller does not maintain authority over the buyer's use of the data. Furthermore, the CCPA already accounts

December 6, 2019

Page Eight

for the scenario that likely inspired this new provision; the statute requires businesses to respond to a consumer's right to know request by disclosing the third parties to which it has sold the consumer's personal information. Once the business so informs the consumer, the consumer may submit a do-not-sell or a deletion request to any such third party.

e. The final regulations should require verification of consumers' opt-out requests.

The Proposed Regulations specify that "a request to opt-out need not be a verifiable consumer request," but a business may deny such a request if it has a "good-faith, reasonable, and documented belief" that the request is fraudulent and notifies the requestor of the denial. §999.315(h).

This standard is ill advised and should be omitted from the final regulations. The CCPA's opt-out rights extend to data sales that are, in fact, vital fraud prevention or identity authentication services. As such, limiting a business's ability to verify or authenticate an opt-out request will allow malicious actors to fraudulently opt planned victims out of data services designed to protect the actual consumer.

f. Requiring a two-step process for consumers' online deletion requests is unduly burdensome on businesses and disempowers consumers.

The Proposed Regulations require a business 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." §999.312(d).

This two-step requirement should be removed from the final regulations. Dictating a business's process flow is beyond the scope of the regulations. Further, mandating a two-step process actually disempowers consumers, as many companies may operate a "self-service" process whereby consumers can make their own choices regarding the information to be deleted. Consequently, as drafted, the current requirement will likely frustrate consumers. Businesses should instead have the flexibility to determine process flows; a two-step process may be appropriate in certain instances and not in others.

g. Requiring businesses to convert unverifiable deletion requests into do-not-sell requests has no basis in the CCPA.

The CCPA requires a business that receives a verifiable deletion request to delete the personal information from its records and direct any service providers to do the same. §1798.105(c). The Proposed Regulations go one step further and impose an obligation not found in the CCPA, requiring that "when a business cannot verify the identity of an individual for the purpose of deletion, the business shall treat the request as an opt-out of sale." §999.313(d)(1).

December 6, 2019

Page Nine

This requirement does not honor consumers' intent or their ability to control how their personal information is used. Indeed, it may result in the wrong consumer being opted of sales if, for instance, a consumer with a similar name submits an unverifiable deletion request. The first consumer may appreciate a business's discounts, interest-based advertising, and other benefits attendant to the sale of his or her data, but be opted-out of sale on the basis of another consumer's request. In this respect, conflating the right to deletion and the right to opt out of sale subverts consumers' ability to make granular choices regarding their personal information and thus runs counter to the CCPA's overall objective (*see, e.g.*, §2(h-i), which states that "California consumers should be able to exercise control over their personal information" and outlines consumers' specific rights under the law, including separate rights to opt out of the sale of their personal information and to direct a business to delete their personal information).

h. Requiring a business to notify consumers of its deletion methods is duplicative.

The Proposed Regulations dictate that "in its response to a consumer's request to delete, the business shall specify the manner in which it has deleted the personal information." §999.313(d)(4). The issues with such a requirement are manifold. First, it is immaterial to consumers, who are likely concerned primarily with the *outcome* of deletion rather than the *methods* by which such deletion is achieved. Second, it represents regulatory overreach. The CCPA's preamble specifies that the law "would grant a consumer the right to request deletion of personal information and would require the business to delete upon receipt of a verified request." The business's obligation is to delete the consumer's personal information, not to respond to the deletion request or to explain to consumers *how* it will comply with the request. Finally, the requirement is vague, as it is unclear what is being sought; is the question whether the data was shredded or a physical disk was degaussed? What would be a reasonable response with respect to data in a database? What is the "method" for deleting data from a database? And what if the business's deletion methods change over time?

i. Treating browser signals as opt-out requests is premature.

The Proposed Regulations introduce a new requirement that "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 ... for that browser or device, or, if known, for the consumer." §999.315(c). Such a requirement is premature. The AG should wait until industry framework is further developed, and possible technical solutions clarified, before drafting a regulation to this effect. Notably, the Interactive Advertising Bureau (IAB) and its standard-setting organization, the IAB Technology Laboratory, have already issued a draft CCPA compliance framework for publishers and technology companies to address the challenges of the CCPA's do-not-sell requirements as they relate to interest-based advertising, as well as initial technical specifications to implement that framework. Likewise, in late November 2019, the Digital Advertising Alliance (DAA) amended

December 6, 2019

Page Ten

its “Self-Regulatory Principles and Guidelines” to address how companies in the digital advertising supply chain should address consumers’ do-not-sell requests, and announced web- and app-based tools to effectuate such requests.

- j. A business should not be required to explain the specific basis for denying a consumer’s access or deletion request.*

The Proposed Regulations state that, “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.” §999.313(c)(5). The Proposed Regulations similarly require a business that denies a consumer’s request to delete his or her personal information to “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.” §999.313(d)(6).

Several statutory exceptions relate to circumstances that would prevent disclosing to the consumer the specific basis for denying his or her request, including: cooperation with law enforcement; the exercise or defense of legal claims; or compliance with a regulatory investigation or criminal inquiry (*see* CCPA §1798.145(a)). Requiring businesses to disclose the specific bases for denying consumer requests will cause them to violate their confidentiality obligations and, in many instances, undercut their legal positions. Accordingly, the final regulations should require a business to list the statutory exceptions in its privacy policy and specify that thereafter, the business need only include in its notice of denial that an exception applies, directing the consumer to the relevant provision of the privacy policy.

3. The Proposed Regulations’ provisions regarding service providers’ use of personal information will burden businesses and have unintended consequences that adversely impact both industry and consumers.

- a. Requiring a person or entity to comply with the CCPA’s requirements for service providers when the business it services does not constitute a “business” under the CCPA is illogical.*

The Proposed Regulations state that, “to the extent that a person or entity provides services to a person or organization that is *not* a business, 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. §999.314(a).

This provision is illogical and should be removed from the final regulations. When a person or entity provides services to an organization that is *not* a business as defined by the CCPA, that person or entity should not be subject to the obligations that the CCPA imposes on service providers.

December 6, 2019

Page Eleven

b. The Proposed Regulations excessively limit service providers' use of personal information.

The Proposed Regulations state that “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 to detect security incidents or prevent fraudulent or illegal activity. §999.314(c).

This limitation is inconsistent with the CCPA, which is, in its essence, a notice and individual rights regime. Accordingly, a business and its service providers should have flexibility to contractually agree to uses of personal information, especially in light of the fact that those uses must be disclosed to consumers and with respect to which consumers have certain choices. The limitation is also too narrow and does not reflect business realities. Instead, the regulations should be amended to reflect that service providers may use personal information for multiple clients and for circumstances beyond detecting security incidents or fraud, provided that such use is consistent with their service offerings and permitted by their agreements with their clients. For example, a service provider should be able to use information for benchmarking or analytics purposes or for improving its products or services. These are standard uses of personal information and should not be limited by the CCPA. Such services are central to certain industries’ business models, and the Proposed Regulations’ narrow drafting would have dramatic and likely unintended consequences for businesses in those industries. By way of example, service providers in the consulting and human resources sectors use personal information to provide clients with valuable benchmarking including, for example, advising on industry standards for executive search timelines. And, as aforementioned, service providers in the healthcare sector provide personal information to entities that use the data to assess the efficacy of medical treatments. These service providers use data received from one person or entity to provide services to another, and while their services do not constitute incident detection or fraud prevention, they are often central to the service provider’s businesses and, in many instances, produce cross-industry and/or societal benefit.

c. Requiring service providers to respond directly to consumers is overly burdensome on the service providers and likely contrary to businesses’ wishes.

The Proposed Regulations introduce a new requirement that “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, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial. The service provider shall also inform the consumer that it should submit the request directly to the business on whose behalf the service provider processes the information and, when feasible, provide the consumer with contact information for that business.” §399.314(d).

This provision suggests that a service provider must respond directly to a consumer’s CCPA request and redirect the consumer to the appropriate business (*i.e.*, the appropriate customer of

December 6, 2019

Page Twelve

the service provider). Practically speaking, this would require a service provider to implement a process by which to tie individual consumers to the applicable customer. Most customers do not wish to have their service providers interact directly with their consumers and contractually prohibit them from doing so, so that the business is able to maintain a single point of contact with consumers and control over its communications with them.

Instead, the regulations should make clear that an entity responding as a service provider rather than a business has fewer obligations to respond to consumers and need only notify the consumer of the categories of sources of the personal information. This is consistent with how the CCPA treats service providers. Specifically, a business that receives a delete request must pass it on to the business's service providers. A service provider has no obligation under the law to direct its customer to delete personal information.

4. Several of the Proposed Regulations' notice obligations are unworkable and counterproductive to the notice principle.

- a. The Proposed Regulations' notice obligations will disproportionately burden businesses that operate predominantly offline.*

In their current form, the Proposed Regulations would significantly expand the CCPA's obligations with respect to the timing of offline businesses' required notices to consumers. The CCPA states that "a business that collects a consumer's personal information shall, ***at or before the point of collection***, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used." §1798.100(b). Departing from this standard, the Proposed Regulations stipulate that "the notice at collection... shall be visible or accessible where consumers will see it ***before any personal information is collected***." §999.305(a)(2)(e). The Proposed Regulations impose a similar obligation with respect to offline businesses' opt-out notices. They stipulate that such notices must be provided "by an offline method" that may include "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." §999.306(b)(2).

On its face, the proposed obligation represents a significant and unworkable expansion of the CCPA's notice obligation for retailers and other businesses that operate traditional "brick-and-mortar" establishments. As a practical matter, the only way that such businesses can feasibly provide a privacy notice to all consumers in all contexts would be to post the notice on its website. As an illustrative example, expecting a retailer or fast food establishment to distribute a privacy notice to each point-of-sale customer from whom it collects personal information would be impractical and unrealistic. Such an obligation would dramatically increase the duration of transactions and prove prohibitive from both staffing and employee training perspectives. In fact, imposing such an obligation would result in a requirement similar to that under HIPAA, whereby covered health care providers must distribute a notice explaining individuals' rights with respect

December 6, 2019

Page Thirteen

to their personal health information prior to the provision of services. While it may be reasonable to require such notice in connection with the collection of sensitive health information, information collected in connection with retail transactions does not raise the same privacy concerns. Accordingly, retailers should not be subject to the same level of notice obligations applicable to HIPAA-covered entities.

The Proposed Regulations provide that posting conspicuous signage that directs consumers to the business's online privacy notice—as opposed to distributing the notice itself—will satisfy the CCPA's notice requirement. §999.305(2)(e). While this would provide a theoretical solution for businesses looking to address the challenges of providing notice before in-person interactions, it is arguable whether this would provide a meaningful benefit to consumers, who likely already know to look to a business's website for the business's privacy policy.

Moreover, the “offline” world is very diverse. It is far from clear how companies could effectively provide notice at or before the collection of personal information (other than via an online privacy notice) with respect to personal information that is obtained over the telephone, by fax, or by mail. In many contexts, the provision of notice would be impossible.

If the Proposed Regulations are finalized in their current form, businesses would necessarily come up with different and creative solutions to the notice obligation, to the extent possible. The manner in which notice is presented would thus be likely to differ dramatically across businesses. Ultimately, we believe that consumers would benefit from having a single, uniform place to find a company's CCPA disclosure (i.e., its online privacy policy). This approach would be consistent with what we understand to be consumers' existing understanding that they should check the footer of a company's website to find its privacy policy. While some small businesses may not maintain websites, a solution targeted at those exceptions would be more appropriate than allowing the exception to define the rule.

b. Requiring businesses to provide separate disclosures for each category of personal information that they collect runs counter to the notice principle.

The Proposed Regulations expand upon the CCPA's notice requirement by specifying that a business's notice at collection must contain, “*for each category of personal information, the business or commercial purpose(s) for which it will be used.*” §999.305(b)(2). They further specify that a business's privacy policy must include, “*for 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.*” §999.308(b)(1)(d)(2).

These requirements run counter to the general notice principle: that individuals should receive easy-to-understand notices regarding the collection of their personal information. A notice that includes the required information for each category of personal information will likely be

December 6, 2019

Page Fourteen

duplicative, unnecessarily long, and difficult for consumers to understand. Moreover, a single piece of information, even just a consumer's name, may fall within multiple of the statutorily prescribed categories of personal information, making the notice even more unwieldy and difficult for a consumer to understand. Moreover, consumers are likely interested in the sources of their personal information in general, not broken down by category.

Accordingly, these provisions of the Proposed Regulations should be revised to require that the notice at collection and privacy policy include the categories of personal information to be collected and, as applicable, the *cumulative* categories of sources from which personal information are collected; business or commercial purposes for which personal information will be used; and/or categories of third parties to whom personal information may be *sold* (note that the reference to "shared" in the Proposed Regulations should be replaced with "sold," for consistency with the CCPA's other provisions).

Similarly, the Proposed Regulations require a business to provide, in response to a verified access request, the following information *for each category* of personal information it has collected about a 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 disclosed the category of personal information." The final required element—the business or commercial purpose for which the business sold or disclosed the category of personal information—is a new requirement not included in the CCPA itself. It should be struck from the final regulations, which should focus on clarifying the law, not substantively amending it. Additionally, and for the reasons identified above, the final regulations should permit a business to include the required contents of its response on a cumulative basis; it should not be required to segment its response according to the category of personal information collected.

c. A business should not be required to include a forward-looking commitment not to sell personal information in its privacy policy to avail itself of the opt-out notice exemption.

The Proposed Regulations dictate that "a business is exempt from providing a notice of right to opt-out if 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." §999.306(d)(2). The forward-looking ("and will not sell") clause of this provision should be removed from the final regulations.

First, this additional requirement extends beyond the scope of the CCPA, which only requires a business to provide a consumer with notice of his or her right to opt-out of the sale of his or her personal information if the business in fact "sells" personal information. §1798.120(a). There is

December 6, 2019

Page Fifteen

no statutory requirement for a business to provide notice if it does not presently sell a consumer's personal information but may do so in the future.

Second, requiring a business to treat a consumer whose personal information was collected when a notice of right to opt-out of sale is not posted as having opted out is unreasonable for businesses, forcing those that do not sell personal information to be prescient as to their future plans. This issue is further compounded by the CCPA's broad definition of "sale"; a businesses likely may not know today whether it will sell personal information in the future. Further, the requirement is not consumer-protective. If a business does not currently sell personal information, from what is the consumer opting out? The consumer has no information with which to determine whether he or she wishes to opt out.

Third, the current provision incentivizes businesses to act as though they presently sell consumers' personal information even if they do not. Businesses are encouraged to post opt-out-of-sale links in order to future-proof their activity in the event their business model changes or the complex definition of sale is later determined to include an existing or future business practice.

Lastly, and most importantly, consumers are harmed by this expansion of the opt-out notice requirement. Because a business that does not currently sell consumers' personal information is essentially forced to behave as though it does and provide the requisite notice, its consumers who exercise their right to opt out will be taking a futile and hollow action. The consumers will be opting out of a sale that does not take place and will need to be informed, when opting out, that the business does not sell their personal information and their opt out has no impact. This will create confusion for consumers who think they are exercising a right under the statute when they are essentially opting out of nothing, and also undercut the efficacy of the opt-out regime, causing consumers to view the CCPA as devoid of substance.

If the AG does not strike the clause in question, he should, at a minimum, clarify it to make clear that 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*.

d. Requiring a business to quantify the value of consumers' personal information in its notice of financial incentives will result in inconsistencies and confusion.

The Proposed Regulations introduce a new requirement that a business include in its notice of financial incentives "an 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." §999.307(b)(5).

December 6, 2019

Page Sixteen

Not only would this requirement impose an obligation not contemplated by the CCPA, but it is difficult to see how the requirement would advance the CCPA's goal of giving consumers control over their personal information. A business's compliance with the law should suffice; requiring it to further justify to consumers why its offering is permitted under the law is an overreach that does not comport with the CCPA's stated aim. Furthermore, quantifying the value of personal information is subjective, and each business will thus likely derive a different way to quantify the value, leading to inconsistency among businesses and corresponding confusion—rather than benefit—to consumers. In addition to removing this new requirement, the regulations should be re-drafted to permit businesses to rescind a financial incentive, or a pro rata portion thereof, in the event that a consumer revokes his or her consent to the collection or sale of his or her personal information.

5. Requiring big buyers and sellers of personal information to publish statistics is prone to error and not consumer-protective.

The Proposed Regulations introduce an entirely new requirement for businesses that annually buy, sell, or receive or share for commercial purposes, the personal information of four million or more consumers. Such businesses must publish the following metrics in their privacy policies or on their websites: the number of requests to know, requests to opt out, and requests to delete that the business has received, complied with in whole or in part, and denied; and the median number of days within which the business substantively responded to such requests. §999.317(g).

This requirement has no basis in the CCPA, and publishing such metrics in a business's privacy notice is prone to error and therefore misrepresentation claims. Further, while such aggregate metrics may be of interest to the AG in connection with its enforcement efforts, it is unclear what, if any, value they would provide to consumers. Similarly, requiring a business to furnish such statistics to consumers does not further the CCPA's overarching purpose of giving consumers greater *control* over their personal information. Accordingly, the regulations should either eliminate this requirement or require big buyers and sellers of personal information to maintain statistics and furnish them to the AG upon request.

If the AG ultimately determines that big buyers or sellers must publish certain statistics or maintain and furnish them to the AG upon request, the methods of calculating such statistics should be clarified. Specifically, it is unclear what would constitute a request that is "complied with" or "denied," particularly in relation to unverifiable consumer requests or those that are subject to a statutory exception. These should not count toward a business's total number of requests received, and thus not require classification as having been complied with or denied. Additionally, the final regulations should replace "median" to "average" with respect to the number of days within which a business responds to consumer requests.

December 6, 2019

Page Seventeen

6. The verification methods set forth in the Proposed Regulations are insufficient and ineffective.

The Proposed Regulations set forth required methods for verifying a consumer's request. Specifically, with respect to verifying consumers who do not maintain an account with a business, the business would be required to verify the identity of a consumer making a request to know categories of personal information to a reasonable degree of certainty (such as by matching at least two data points provided by the consumer with data points maintained by the business). By contrast, a business would be required to verify a consumer's request to know specific pieces of personal information to a reasonably high degree of certainty (such as by matching at least three data points provided by the consumer with data points maintained by the business, together with a signed declaration). §999.325(b) – (c).

As an initial matter, we believe that the Proposed Regulations fail to clearly articulate that the process for verifying a consumer's request should involve two separate steps: (1) verifying the identity of the individual making the request; and (2) verifying that the business maintains personal information relating to that individual. In our view, the first step is critical for consumer protection. It is an unfortunate reality that malicious actors will attempt to abuse the new access right. While "matching" standards may be appropriate for verifying that the business maintains personal information relating to an individual, "matching" standards are an ineffective tool for verifying identity generally. Although the Proposed Regulations would not mandate that a business follow its "matching" standard, many businesses seeking to ensure compliance with the rules would likely follow the verification examples provided by the AG. Moreover, notwithstanding proposed §999.325(c), the Proposed Regulations fail to effectively account for the fact that businesses will have to process requests from individuals with whom they do not have a relationship or have not had meaningful interactions—scenarios that create significant challenges for identity verification.

The Proposed Regulations imply that a business should be able to verify a consumer's request (presumably including verifying that the consumer is who he or she purports to be) simply by matching data provided by the requestor with data maintained by the business. This type of standard may be effective in contexts in which the business has previously collected from a consumer information that only the consumer should know (*e.g.*, name, Social Security number, and account balance). However, this type of standard is inappropriate in many, if not most, scenarios, particularly where the business has limited identifiers relating to an individual. For example, many types of logical data elements used for matching purposes are easily obtained from public sources, such as name, name, zip code, and phone number. Such an arbitrary standard is ripe for fraud and abuse, which is harmful both to consumers and to businesses. In fact, in many contexts, a business will not have three data points that are not publicly available that would serve as useful identifiers. Regardless, it is unclear how matching three data elements versus matching two data elements somehow provides a meaningfully higher degree of certainty that the requestor is who she says she is.

December 6, 2019

Page Eighteen

In this regard, the Proposed Regulations also would provide that businesses should “generally avoid requesting additional information from the consumer for purposes of verification.” The AG should remove this statement from the final rules; it ignores the reality that logical data elements that a business will have to use for verification in many contexts will be publicly available information, such as name and contact information. Moreover, this statement would disincentivize businesses from using third-party identity verification services that ask consumers “out-of-wallet” questions and that typically require the consumer making the request to provide, for example, her name and Social Security number. In addition, at the time that a consumer submits a request, a business may not know the types of information that it maintains about the consumer (if any) in order to take steps to “match” data elements at the time the request is made. The AG should not create standards that require the businesses to adopt consumer-specific verification processes based on the type of information that they maintain about separate consumers and that have the effect of prolonging the verification process because businesses will not know what information they maintain about a consumer at the time of the request. This type of process will not accrue to the benefit of either consumers or businesses.

Moreover, a signed attestation is functionally useless and does nothing to heighten the verification standards, given that most of these documents will be submitted electronically and most businesses do not have consumer signatures on file with which to compare them. In this regard, a signed attestation will not provide a practical deterrent to fraudsters who will be more than willing to provide such an attestation. Moreover, while the AG’s Initial Statement of Reasons indicates that the signed attestation will allow businesses recourse against fraudsters, a business will have significant practical challenges in pursuing fraudsters (assuming it has the appetite for such litigation), including challenges in identifying the fraudsters and because, in many cases, the fraudsters will be located in non-U.S. jurisdictions. Regardless, the standards for verifying consumer’s requests should be aimed at protecting consumers from fraudulent access to their personal information and not at providing recourse for businesses to pursue fraudsters who are able to abuse inadequate, but compliant, verification processes.

Ultimately, the AG should instead give businesses the flexibility to craft risk-based approaches, whereby they utilize verification methods designed to address the relative risks associated with providing access to, deleting, or selling the types of personal information that they process to an imposter.

7. Only businesses that intend to *sell* the personal information of minors should be required to establish opt-in processes for the sale of such information.

The Proposed Regulations state that “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 shall establish, document, and comply with a reasonable process for allowing such minors to opt-in to the sale of their personal information.” §999.331(a).

December 6, 2019

Page Nineteen

This provision should be re-drafted to specify that only businesses that collect or maintain the personal information of minors at least 13 and less than 16 years of age *and intend to sell such personal information* are required to implement opt-in procedures for such sales. A business should not be required to implement and maintain an onerous opt-in procedure if it does not plan to sell minors' personal information.

8. The AG should provide for a later effective date than that which would apply under the California Code.

When an agency's implementing regulations are finalized, the California Code provides that they become effective on one of four quarterly dates, depending on when the regulations are filed with the California Secretary of State. Namely, absent an exception, the regulations take effect on:

- January 1st, if filed between September 1st and November 30th;
- April 1st, if filed between December 1st and February 29th;
- July 1st, if filed between March 1st and May 31st; or
- October 1st, if filed between June 1st and August 31st. Cal. Gov't Code §11343.4(a).

Accordingly, the earliest date on which the AG's implementing CCPA regulations could become effective, based on the timing of the current comment period, is April 1, 2020. However, the standard quarterly approach would *not* apply if a later date is prescribed by the state agency in a written instrument filed with, or as part of, the regulation. §11343.4(b)(2). In light of the onerous obligations that the AG's regulations are likely to impose, a two-to-four-month compliance window from the date such regulations are finalized is inadequate. The AG should provide for a later effective date—no earlier than January 1, 2021—in its final regulations.

9. The AG should establish additional exceptions to the CCPA.

The CCPA provides that the AG shall adopt regulations, including “establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights.” §1798.185(a)(3). The Proposed Regulations are, however, devoid of such exceptions. The AG should confirm via its final regulations that the CCPA does not require the forfeiture of trade secrets, proprietary information, or intellectual property rights. For example, information related to customer preferences, which would otherwise fall within the scope of a business's disclosure requirement, often constitutes a retailer's most valuable and heavily guarded trade secret information.

December 6, 2019

Page Twenty

Once again, the GPA appreciates the opportunity to submit comments on the AG's proposed implementing regulations for the CCPA, and we would be happy to discuss further any of the issues we have raised.

Very truly yours,

A handwritten signature in black ink, reading "Miriam H. Wugmeister". The signature is written in a cursive, flowing style with a large initial "M".

Miriam H. Wugmeister.

Message

From: Rudolph, Matthew [REDACTED]
Sent: 12/6/2019 10:56:59 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: HERE Technologies comments regarding the CCPA draft regulations
Attachments: HERE CCPA Regulatory Comments.pdf

To: Privacy Regulations Coordinator (Office of the California Attorney General):

We respectfully submit the attached comments pertaining to the proposed regulations concerning the California Consumer Privacy Act.

Should you require any further information, please do not hesitate to let us know.

Best Regards,

Matthew Rudolph on behalf of HERE Technologies



Matthew Rudolph

Privacy Officer

M: [REDACTED]

HERE Technologies
425 W. Randolph St., Chicago, IL 60606
[41° 53' 55" N -87° 38' 19" E](#)



HERE CCPA Regulations Comments

HERE TECHNOLOGIES – COMMENTS ON DRAFT REGULATIONS FOR THE CALIFORNIA CONSUMER PRIVACY ACT

This document outlines the comments of HERE Technologies regarding key aspects of the California Consumer Privacy Act (the "CCPA") draft regulations. It expresses our concerns about some crucial elements of the CCPA draft regulations and the negative impact they might have on the functioning of the location services provided by HERE Technologies, their impact on innovation and therefore on the benefits of these services for end users.

About HERE Technologies

HERE Technologies ("HERE") is a global leader in digital location technology. Our products and services enable people, enterprises and cities around the world to harness the power of location and create innovative solutions that make our lives safer, more efficient, productive and sustainable. We transform information from devices, vehicles, infrastructure and many other sources into real-time location services that play a key role in how we move, live and interact with one another. HERE's vision is to create an autonomous world for everyone, based on open availability of the vast amounts of data that will be generated by the hundreds of billions of connected devices in our increasingly connected world.

HERE Technologies is fully committed to respect privacy and to comply with all applicable laws covering data protection and privacy. As a company which is already subject to robust privacy regulations such as the European General Data Protection Regulation (the "GDPR"), we support and are prepared to comply with consumer privacy protections like those represented in the CCPA. We are, however, concerned that some elements of the proposed CCPA regulations will have detrimental effects on the functioning of our location services and on the benefits of these services for our end users. Moreover, some of the proposed requirements risk hampering innovation and may therefore have a negative impact on the further development and maximization of location services in California.

We wish to highlight the following key aspects of the CCPA draft regulations that are of particular concern to HERE Technologies and the location services we provide:

I. Alignment of CCPA Program with Global Program Requirements

As a company that has already implemented the GDPR globally, which includes extending right such as access and deletion to all users of our services, in California and elsewhere, we have encountered

HERE CCPA Regulations Comments

a number of problems in trying to align the requirements of the CCPA with the need to operate a global privacy program.

One challenge for businesses that operate globally and are implementing the CCPA is that in many instances the business will not know or will not need to know whether the request relates to a California consumer. This is particularly the case for businesses that operate online only, and frequently will not collect information from users relating to their state of residence, as such information is often not relevant to provide the service. We do not believe that the intent of the CCPA would be to collect additional information solely to be able to identify the user or their residency in situations where such information is not required in the first place to provide the service. State residency information is frequently not collected due to an interest in minimizing the collected data to what is necessary to provide the relevant service.

There are several requirements within the draft regulations which require specific actions to be taken that are unique to responding to requests from California. These requirements become problematic because in some cases they will directly conflict with mandatory legal obligations in other jurisdictions. As an example, the two-step deletion process required by § 999.312(d) would not permit deletion of an account, while under other laws such as the GDPR a single step deletion request is valid and mandatory. Other examples are requirements that responses specifically cite to California law, restrictions on types of data that can be disclosed, varying required periods for maintaining evidence of compliance, and differing notification and communication requirements.

Because these requirements directly conflict with data protection laws of other jurisdictions, businesses cannot apply them globally. One workable solution would be to permit businesses to establish California-specific designated methods for submitting requests, and then only apply the CCPA requirements where the request is sent to those designated methods or the consumer has otherwise indicated that they are from California, or through other reasonably designed mechanisms for differentiating requests from California consumers from those related to other jurisdictions. HERE respectfully requests that regulatory guidance be provided regarding what a business's responsibilities are with regard to identifying requests related to California consumers.

II. Restrictions Regarding Service Providers

Section § 999.314(c) of the draft regulations imposes restrictions on a service provider's ability to use personal information it processes on behalf of a business. HERE is concerned that the restrictions put in place in this section of the draft regulations exceed what is required by the statutory language of the CCPA in a way that would excessively burden multitenant online platform providers, without providing a commensurate benefit to consumers.

The draft regulations place restrictions on use of personal information collected in the context of providing services to one customer in a way which benefits other customers, except that a business may aggregate personal information to the extent necessary to detect data security incidents or protect against fraudulent or illegal activity. Providers of online platforms typically architect their platforms in such a way that error events, usage behaviors, and other interactions with the online platform generate operational data which may contain personal information. The specific content of this operational data may vary, but would typically include usage events for individuals on the platform such as actions taken and queries sent.

HERE CCPA Regulations Comments

HERE believes it would be beneficial both to consumers and businesses to clarify that broader internal usage of platform services' operational data is permissible for purposes of operating, maintaining, and improving the platform services. The narrow focus on security and fraud excludes potential threats such as IT incidents that impact the accuracy and availability of the personal information, which like security threats are more readily addressed on a platform-wide basis.

HERE recommends modifying the draft regulations to permit service providers to use operational data for some or all of the additional "business purposes" described in § 1798.140(d) of the CCPA, while still prohibiting service providers from reselling or using the data for any "commercial purpose". HERE believes that this broader usage is consistent with the statutory text of the CCPA, because maintaining a platform in good operating condition is inherently part of performing a service for a customer. Additionally, the CCPA permits disclosure to service providers to perform a business purpose, which as defined by the CCPA includes using the information for additional internal operational purposes such as "debugging to identify and repair errors that impair existing intended functionality".

Further, if service providers are expected to implement additional segmentation of operational information, this will require fundamental changes to how their platforms operate. These types of fundamental changes take significant time to implement, which may not be possible within the short timeline between when the regulations are adopted and when they are effective. HERE urges that any issuance of regulations which will require significant re-architecting of online platforms be done in a way which permits businesses adequate time to implement the required technologies.

III. Verification of Sale Opt-Out Requests

HERE has concerns regarding the requirement that a request to opt-out does not need to be a verifiable consumer request. Without information beyond the initial request, a business may not have sufficient information to determine whether or not the request is fraudulent.

As an example, HERE maintains directories of business names and addresses. If a business must document an affirmative reason to believe that a particular request is fraudulent, it would be easy for an individual to take down a competitor's business listing, sale solicitation, or directory information simply by submitting an opt out request in the other person's name.

This issue applies broadly to any kind of directory or sale listing service, where the impact of an opt-out request and a deletion request are functionally indistinguishable (i.e. they result in the individual's removal from the directory), yet under the draft regulations opt-out requests are not subject to any of the protections granted for deletion requests.

Due to the potential adverse impacts to consumers, HERE respectfully requests that businesses be permitted to conduct reasonable verification of an opt out request following similar risk-based procedures as those for other consumer requests, particularly as it pertains to directory or listing services.

IV. "Browser Setting" as Opt-Out Request

HERE CCPA Regulations Comments

HERE has concerns regarding the requirement in § 999.315(c) related to treating a browser plugin or privacy setting as an effective opt-out request due to status of currently available technologies. While multiple industry groups are currently working towards “do not sell” technology frameworks that are designed to address user requests in the online advertising environment, there are significant issues with these frameworks both in terms of scope and timing.

In terms of scope, a direct reading of the current draft regulations seems to indicate that a browser setting would have opt-out effects beyond the information transferred in that browsing session. Specifically, that if the specific consumer can be identified, that browser setting would need to be respected as a general request to opt-out of data sales. To the extent that this opt-out is intended to apply beyond information transferred in that specific browsing session, this is not addressed either in current or planned technologies, and would be a massive undertaking to design and implement. There are also significant user transparency and choice problems with this approach, such as where a user may inadvertently exercise an opt-out simply due to a global setting with their browser.

Even within the context of information transferred within a particular browsing session there are numerous problems with this requirement. There is currently not an agreed technological framework or standard for transmitting an opt-out request. Without an agreed standard, businesses would be potentially subject to multiple competing standards which would be impractical to track and implement.

HERE respectfully requests that this requirement be withdrawn.

V. Opt-Out Time Limits

HERE believes that the 15 day opt-out request fulfillment period set out in § 999.315(e) of the draft regulations is too short for many businesses to feasibly implement, particularly those which maintain publishing and quality function for versioned data sets. To maintain quality processes (such as under ISO 9001 industry standards) for their products, businesses must have defined procedures for creation and publication of their products, which can frequently take more than 15 days to operate. The difficulty is further extended for businesses which create physical products or other goods which must work through a chain of publication processes. For example, if a directory is printed on media and then sold, it would not be possible to issue a new version within 15 days of each request. This also raises the issue of what would be done with existing but unsold inventory following the receipt of an opt-out request.

Even outside the concerns of data publishers, 15 calendar days will frequently be too short for businesses to comply, and in particular for small and midsize businesses that do not have the capacity to staff during weekends and holidays to address privacy requests. Maintaining separate time periods for opt-out requests also adds complexity to businesses’ internal processes where they have to track multiple different fulfillment periods, in some cases relating to the same request where an individual exercises multiple rights simultaneously.

HERE respectfully requests that this 15 day opt-out request fulfillment period be extended to 45 days in all cases for operational simplicity and to provide adequate processing time, and for

HERE CCPA Regulations Comments

versioned published data sets, allowance should be made for businesses to update subsequent versions of the data set to omit the data in question.

VI. Metrics Collection and Publication

HERE requests additional clarity regarding the metrics collection requirements of § 999.317(g). Specifically:

- What update cadence is required for compilation of these metrics. HERE would propose that they be updated on an annual basis in accordance with § 1798.130(a)(5) of the CCPA.
- When the initial publication of these metrics will be required. For businesses with a high volume of requests, it will take time to implement the required tracking and reporting elements. Because this requirement for metrics collection does not exist within the CCPA statutory text and the regulations imposing this requirement have not yet been finalized, HERE respectfully suggests that an implementation period be defined in the regulation to permit businesses to establish the systems and procedures for collecting this information.
- Whether these metrics are to be based off of requests sent to the business's CCPA designated method for submitting requests, or some other metric. Many businesses offer customers multiple methods for deleting their information, such as self-service portals, or contact channels for requests related to other global privacy laws. Because of this difficulty in attributing requests to a California consumer (particularly where the business may not know that the individual making the request is a California resident), HERE would propose that these metrics should be based only on requests sent to the business's designated methods for submitting requests under the CCPA, or by other reasonably designed mechanisms for differentiating requests from California consumers from those related to other jurisdictions.

VII. Additional Opportunities to Provide Clarification

There are several areas where we believe businesses would benefit from additional clarifications in the regulations. These include:

- "Categories of third parties": HERE seeks clarification that any entity which qualifies as a "service provider" under the CCPA is not considered a "third party" with respect to the regulations. Several of the examples provided for third parties, such as operating systems and platforms, typically act as a service provider. This would help address an ambiguity in the CCPA statutory language where the definition of "third party" appears to exclude entities under the type of contract that is required for "service providers" but does not directly state that "service providers" are not "third parties".
- Alignment to updated statute: It has been assumed in submitting these comments that the regulations will be updated to take into account the amendments to the CCPA which were signed into law in October 2019.
- Obligations regarding purchasers in event of an opt out request: The requirement in § 999.315(f) to inform purchasers of personal information of a consumer's request to opt-out of sale does not include a required timeline for informing those purchasers of the opt-out request. It is also unclear what impact this notification to those purchasers is intended to have, since the purchasers are in any event subject to restrictions related to resale. If this

HERE CCPA Regulations Comments

requirement remains within the regulations, HERE respectfully requests that a reasonable timeline, such as the 45-day timeline permitted for other types of requests, be applied to this communication requirement.

- **Safe Harbors:** Given the ambiguities present in the CCPA statutory text, both businesses and consumers would benefit from establishment of “safe harbors” or similar defined examples of compliant behavior. In particular, the following would be beneficial:
 - Examples or guidance related to description of the categories of personal information. The draft regulations require that the categories be described in a way that is clear and not legalistic, but the statute requires businesses to use the specific categories described in the statutory text, which overlap each other in a way that will be confusing to consumers (e.g. multiple categories can include contact information or electronic information), or are a bare reference to other bodies of law. These requirements are in clear tension which could be alleviated through additional guidance, examples of practices which are deemed to be compliant, or even re-definition of the categories of personal information.
 - Guidance for businesses in the event of inadvertent or erroneous sale of personal information. If a business seeks not to sell personal information and has implemented reasonable measures to prevent such sales, inclusion of a “do not sell” link provides a misleading impression to consumers about how the business uses and discloses their data. One option to address this instance is to establish regulations stipulating that a business which takes reasonable measures to not sell personal information, and promptly acts to correct any identified or reported instances, is not treated as “selling” personal information.
 - Establishment of criteria for “reasonable security procedures”, such as through reference to commonly accepted industry standards (e.g. ISO 27001 or NIST). This would encourage businesses to increase their level of security through adoption of these standards.

HERE is pleased to submit these comments on the Draft Regulations for the California Consumer Privacy Act and we would be happy to provide additional information or to answer any questions the Attorney General’s Office may have.

For further information or queries, please contact Leo Fitzsimon at [REDACTED] or HERE Technologies at privacy@here.com.