

Message

From: Zetoony, David [REDACTED]
Sent: 12/6/2019 11:07:10 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Maciejewski, Andrea [REDACTED]
Subject: Comment from Red Ventures Concerning Proposed Regulations to the CCPA
Attachments: Final 601361685_8.pdf

Please find attached comments submitted on behalf of Red Ventures concerning the Proposed Regulations to the California Consumer Privacy Act of 2018.

Kind regards,
-David



DAVID ZETOONY
Partner



BRYAN CAVE LEIGHTON PAISNER LLP
One Boulder Plaza, 1801 13th Street, Suite 300, Boulder, CO 80302-5386
T: +1 303 417 8530

1155 F Street NW, Washington, DC 20004-1357
T: +1 202 508 6030

bcdplaw.com

This electronic message is from a law firm. It may contain confidential or privileged information. If you received this transmission in error, please reply to the sender to advise of the error and delete this transmission and any attachments.

We may monitor and record electronic communications in accordance with applicable laws and regulations. Where appropriate we may also share certain information you give us with our other offices (including in other countries) and select third parties. For further information (including details of your privacy rights and how to exercise them), see our updated Privacy Notice at www.bcdplaw.com.

December 6, 2019

David A. Zetony, Partner
Christian Auty, Counsel
Andrea Maciejewski, Associate



Lisa B. Kim
Deputy Attorney General
Consumer Law Section – Privacy Unit
California Office of the Attorney General
300 South Spring Street, Fi

Stacey Schesser
Supervising Deputy Attorney General
California Department of Justice
Consumer Law Section – Privacy Unit
455 Golden Gate Ave., Suite 11000
San Francisco, CA 94102

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

VIA E-MAIL (PRIVACYREGULATIONS@DOJ.CA.GOV)

Re: Comment from Red Ventures concerning the Proposed Regulations

The law firm of Bryan Cave Leighton Paisner LLP ("BCLP") is pleased to submit this comment on behalf of Red Ventures (the "Company") concerning the following Proposed Regulations:

1. 999.313(c)(1) and 999.325(b)
2. 999.313(d)(1)
3. 999.315(c)
4. 999.315(f)
5. 999.317(g)

The Company highly values the role of the Office of the Attorney General to promulgate regulations that clarify and interpret the CCPA, and believes that appropriate regulation can benefit both consumers' privacy and the business community by clarifying an ambiguous and uncertain statute. As discussed below, however, there are serious concerns with the above-referenced Proposed Regulations.

I. **Proposed Regulation 999.313(c)(1) and 999.325(b).**

Proposed Regulation 999.313(c)(1) would create a conversion requirement for responding to access requests. In the event a business could not verify an access request for specific pieces of information, it would have to then reanalyze the request “as if it is seeking the disclosure of categories of personal information about the consumer...”¹

According to the Initial Statement of Reasons (“ISOR”), Proposed Regulation 999.313(c) is “necessary because [it] describes what a business must do when it cannot readily verify the identity of the consumer.”² The ISOR claims that the approach “balances the consumer’s right to know what personal information a business has about them with the danger of disclosing personal information to unauthorized persons, recognizing that unauthorized disclosure of specific pieces of personal information (for example, a specific medical diagnosis) is frequently more intrusive and harmful to the consumer than the disclosure of mere categories of personal information (for example, medical information).”³

Proposed Regulation 999.325(b) and Proposed Regulation 999.325(c) specify the verification requirements for each type of access request:

1. A business must verify an access request for specific pieces of personal information “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.”⁴
2. A business must verify an access request for categories of information collected “to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business, which the business has determined to be reliable for the purpose of verifying the consumer.”⁵

The ISOR states that Proposed Regulation 999.325 is intended to “provide further guidance to businesses on how to verify that the person making requests to know and requests to delete is the consumer about whom the business has collected information.”⁶

The approach proposed in Proposed Regulation 999.313(c)(1) and Proposed Regulations 999.325(b) and (c), whereby requests to obtain specific pieces of personal information would be subject to authentication requirements that would be greater than the authentication

¹ Text of the Proposed Regulation (“Proposed Regulation”) § 999.313(c)(1) available at <https://ccpa-info.com/>.
² ISOR at 18 available at <https://ccpa-info.com/wp-content/uploads/2019/10/ccpa-isor-appendices.pdf>.
³ Id.
⁴ Proposed Regulation § 999.325(c).
⁵ Proposed Regulation § 999.325(b).
⁶ ISOR at 31.

requirements for requests to know category-level information, raises significant practical and security concerns which are discussed below.

A. Proposed Regulation 999.325(b)'s lower verification requirement would increase the likelihood of unauthorized disclosures of sensitive information.

Proposed Regulation 999.325(b) incorrectly assumes that category-level information is not sensitive or private. According to the ISOR, the "unauthorized disclosure of specific pieces of personal information (for example, a specific medical diagnosis) is frequently more intrusive and harmful to the consumer than the disclosure of mere categories of personal information (for example, medical information)."⁷ Because this is not always true, as the word "frequently" concedes, a blanket reduction in verification requirements for category-level access requests is improper.

In many instances, the mere fact that an account exists is in-and-of-itself sensitive information. Take, for instance, the existence of an account for a drug rehabilitation center, a job search website, a pornography site, or a dating website targeted to those of a specific sexual orientation. An individual who knows minimal information may be able to satisfy the reduced verification requirements set forth in Proposed Regulation 999.325(b) and obtain information about whether another person has an account with such sites. The confirmation that an account exists is itself private, and verification that a company maintains category-level information about a person (e.g. name, medical diagnosis, account information) is itself sensitive.

Unless, and until, a record is developed that demonstrates that the lower verification bar required by Proposed Regulation 999.325(b) would benefit the public and would not increase the likelihood of unauthorized disclosures, the Attorney General should require the same verification for both category-level access requests and specific information access requests.

B. Proposed Regulation 999.325(b) would improperly weaken security precautions for categorical information access requests.

Proposed Regulation 999.325(b) reduces the verification standard for category level access requests from a "reasonably high degree of certainty" to a "reasonable degree of certainty."⁸ Although the reasonableness standard gives companies some discretion, it ultimately puts a cap on how comprehensive the reduced verification standard can be. The end result is that any business which recognizes the sensitivity of a consumer's category-level information, and aims to maintain a higher bar of verification, may be subject to a claim that its verification requirements are too burdensome on the consumer. Thus, a company may be compelled to disclose personal information in situations that they would, in any other circumstance, consider unauthorized.

The unauthorized disclosure of category-level information increases the likelihood of security incidents and opens consumers up to identity theft and phishing attacks. Scammers may use

⁷ ISOR at 18.

⁸ Proposed Regulation § 999.325(b-c)

any number of communication methods to trick consumers into giving them personal information, almost all of which are made easier if the scammer has basic information about the victim.⁹ A common scam may go as follows:

1. The scammer identifies potential victims *by finding companies that the victims regularly engage with or trust*.
2. The scammer poses as a representative from that company and asks for verification information (such as the consumer's Social Security Number or account password) in order to perform basic administrative or security functions (such as to verify unauthorized activity on an account).
3. The scammer uses the acquired information to steal additional information or assets from the victim.¹⁰

Proposed Regulation 999.325(b) obligates businesses to disclose basic category-level information, such as the existence of an account, by creating a legally required reduction in verification protocols. Ultimately, this weakens the overall security of consumers' personal information and makes the phishing attack easier to perpetrate by disclosing companies with which a victim has an existing account.

Unless, and until, a record is developed that demonstrates that the lower verification bar required by Proposed Regulation 999.325(b) would benefit the public and would not increase unauthorized disclosures, and, as a result, the likelihood that consumers will be subjected to phishing attacks, the Attorney General should require the same verification for both category-level access requests and specific-information access requests.

C. Proposed Regulation 999.325(b) is inconsistent with existing data security laws.

Proposed Regulation 999.325(b) is not only bad for consumers, it is inconsistent with federal and state data security laws. On the state level, California law requires companies that maintain certain types of personal information about Californians 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."¹¹ Similarly, the FTC prohibits companies from committing "unfair or deceptive" acts.¹² The Federal Trade Commission ("FTC") has interpreted a company's failure to implement what it considers to be reasonable security protecting sensitive information to be "unfair."¹³ A security measure that allows a requestor access to potentially sensitive information despite a failed verification is unlikely to be considered "reasonable" by either California courts or the FTC. Proposed Regulation 999.325(b) not only allows the potential unauthorized access of personal information, but in some cases may inadvertently require it.

⁹ FTC, *How to Recognize and Avoid Phishing Scams* (May 2019), <https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>.

¹⁰ Id.

¹¹ Cal. Civ. Code § 1798.81.5 (emphasis added).

¹² 15 U.S.C. § 45(a) (2019).

¹³ F.T.C. v. Wyndham, 799 F.3d 236, 244-47 (3rd Cir. 2015).

Put differently, by implying that businesses should disclose category-level information when they have only a “reasonable degree of certainty” that the proponent of an access request is the consumer about whom the request has been made, even if they do not have a “reasonably high degree of certainty” that the requestor and the consumer are indeed the same person, may, itself, be an unreasonable security practice.

Unless, and until, a record is developed that demonstrates that the lower verification bar required by Proposed Regulation 999.325(b) would benefit the public and would not expose consumer information to heightened security risks, the Attorney General should require the same verification for both category-level access requests and specific-information access requests.

D. The Attorney General has not put forth facts or studies to support Proposed Regulation 999.313(c)(1) as required by California law.

Proposed Regulation 999.313(c)(1) is not supported by any facts, studies, or expert opinions as is required by the California Administrative Procedure Act (“APA”). California law requires that all regulations use a “necessity” standard, which is satisfied when:

the record of the rulemaking proceeding demonstrates by substantial evidence the need for a regulation to effectuate the purpose of the statute, court decision, or other provision of law that the regulation implements, interprets, or makes specific, taking into account the totality of the record. For purposes of this standard, evidence includes, but is not limited to, facts, studies, and expert opinion.¹⁴

The corresponding regulations further emphasize the APA’s evidentiary requirement by explaining that, in order to meet the “necessity” standard, a regulation “*shall include*, but is not limited to, facts, studies, or expert opinion.”¹⁵

The CCPA requires the Attorney General to promulgate regulations that facilitate a consumer’s ability to obtain information from a business.¹⁶ In response, the ISOR claims that Proposed Regulation 999.313 “should have the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business.”¹⁷ However, it does not cite any facts, studies, expert opinions, or other hard data that demonstrate how Proposed Regulation 999.313(c)(1) is necessary to further that goal.¹⁸ For example, the ISOR asserts that the “unauthorized disclosure of specific pieces of personal information (for example, a specific medical diagnosis) is frequently more intrusive and harmful to the consumer than the disclosure of mere categories of personal information (for example, medical information).”¹⁹ This assertion is purely conjecture and is not supported by any facts,

¹⁴ Cal. Gov. Code § 11349(a).

¹⁵ 1 Cal. Code Regs. 10(b)(1-2) (emphasis added).

¹⁶ Cal. Civ. Code § 1798.185(a)(7). The full text of the California Consumer Privacy Act (“CCPA”) is available at <http://www.ccpa-info.com>.

¹⁷ ISOR at 16.

¹⁸ See generally ISOR at 17-18.

¹⁹ Id.

expert opinions, or industry data put forward in the ISOR, or that was made part of the rulemaking record.

As there is no factual record indicating that Proposed Regulation 999.313(c)(1) will effectuate the purpose of the CCPA, the requirements of Proposed Regulation 999.313(c) amount to an arbitrary and capricious obligation on businesses. Unless, and until, a record is developed that demonstrates that the conversion of failed specific-information access requests to category-level access requests would benefit the public, and would not be harmful to consumers, Proposed Regulation 999.313(c)(1) should be abandoned.

E. Proposed Regulation 999.313(c)(1) exceeds the authority of the Attorney General.

The Office of the Attorney General cites Section 1798.185(a)(7) of the CCPA as the authority for the promulgation of Proposed Regulation 999.313(c).²⁰ Section 1798.185(a)(7) charges the Attorney General with:

Establishing rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business' determination that a request for information received by a consumer is a verifiable request, including ...providing a mechanism for a consumer who does not maintain an account with the business to request information through the business' authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.²¹

Notably, any regulation promulgated by the Attorney General under this grant of authority is required to:

1. Take into account security concerns. As discussed in Section I.B and I.C, Proposed Regulation 999.325(b) not only fails to adequately consider security concerns, it increases consumers' risk of unauthorized access, identity theft, and phishing attacks. For this reason, Proposed Regulation 999.313(c)(1)'s mandatory conversion requirement does not achieve the task set forth by the California Legislature.
2. Further the purposes of Section 1798.100. Section 1798.100 states that "a business shall provide [access request] information ... to a consumer only upon receipt of a verifiable consumer request. Proposed Regulation 313(c)(1) allows a business to provide information to requestors whose identity cannot be verified. For this reason, Proposed Regulation 313(c)(1) does not achieve the task set forth by the California Legislature.

²⁰ ISOR at 16.

²¹ Cal Civ. Code § 1798.185(a)(7).

To the extent that the Office of the Attorney General continues to delineate how a business should determine that a request for information is a verifiable consumer request, it should use a single verification standard for both specific-information access requests and category-level access requests.

II. Proposed Regulation 999.313(d)(1).

Proposed Regulation 999.313(d)(1) would create an obligation for a business to convert an unverifiable request to delete information into a request to opt-out of the sale of information. According to the Proposed Regulation, in the event that a business receives a consumer request for deletion, and cannot verify the identity of the requestor, the business "shall inform the requestor that their identity cannot be verified and shall instead treat the request as a request to opt-out of sale."²²

According to the ISOR provided by the Office of the Attorney General, Proposed Regulation 999.313(d)(1) is "necessary to instruct businesses on what they should do when they cannot verify the identity of the consumer."²³ It also purportedly "benefits consumers by requiring the business to view the request in a way that can best accommodate the consumer's intent to delete the information...by at least preventing the further proliferation of the consumer's personal information in the marketplace."²⁴

The approach set forth in Proposed Regulation 999.313(d)(1) raises significant practical and legal concerns which are discussed below.

A. *Proposed Regulation 999.313(d)(1) ascribes an intent to consumers that may not reflect consumer preference.*

The Proposed Regulation requires businesses to convert an unverifiable deletion request to an opt-out request based on the assumption that this best accommodates the consumer's intent.²⁵ This assumption is not substantiated by any evidence and is likely incorrect in many instances. For example, if an individual impersonates a consumer by submitting a deletion request, then the consumer never had the intent to delete their information, much less opt-out of the sale of their information.

This misplaced assumption would be further exacerbated should Proposed Regulation 999.315(f) be enacted. Proposed Regulation 999.315(f)'s flow-down obligations combined with Proposed Regulation 999.313(d)(1)'s conversion obligations would effectively mean that a consumer who tries to impersonate someone by submitting a fraudulent deletion request will not only cause a business to stop selling the person's information, but to instruct other businesses to whom the information was sold to stop selling the consumer's information. None of these actions on the part of the business, and on the part of the onward recipients of data, would reflect the intent of the consumer as all of them would be caused by an impersonator.

²² Proposed Regulation § 999.313(d)(1).

²³ ISOR at 19.

²⁴ ISOR at 19-20.

²⁵ See ISOR at 20.

If a business cannot validate a requestor's identity, the business should not ascribe any intent to the consumer, as it is unclear whether the consumer ever had any intent at all. Unless, and until, a record is developed that demonstrates that most, if not all, deletion requests that are denied because of a failure to authenticate the consumer do indeed come from the consumer, the Proposed Regulation should be abandoned.

B. The Attorney General has not put forth facts or studies to support Proposed Regulation 999.313(d)(1) as required by California law.

California law requires that an agency proposing a regulation must include in the record "facts, studies, or expert opinion" that demonstrate why a proposed regulation is "necessary."²⁶ Proposed Regulation 999.313(d)(1) is not supported by any facts, studies, or expert opinions as is required by the California APA.

The CCPA requires the Attorney General to promulgate regulations that, in relevant part, "facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, which addresses sections...1798.105."²⁷ Section 1798.105 speaks to a consumer's right to deletion, and explains that a business that receives "a verifiable consumer request from a consumer to delete the consumer's personal information...shall delete the consumer's personal information from its records."²⁸ In putting forth Proposed Regulation 999.313(d)(1), the Attorney General cites this grant of authority and states that the subdivision is "necessary to instruct businesses on what they should do when they cannot verify the identity of the consumer."²⁹

Although the Attorney General states that the Proposed Regulation is being put forth in order to "view the request in a way that can best accommodate the consumer's intent to delete the information," there is no record of evidence supporting this conclusion.³⁰ In fact, the Attorney General offers no facts, studies, or expert opinions establishing that the Proposed Regulation effectuates the purpose of the statute whatsoever. For instance, the CCPA gives no indication that one of the purposes of Section 1798.105 is to allow for the opt-out of the sale of information and the Attorney General offers no evidentiary explanation as to how Proposed Regulation 999.313(d)(1)'s conversion obligation otherwise effectuates Section 1798.105.

The ISOR also claims that Proposed Regulation 999.313(d)(1) will "at least prevent the further proliferation of the consumer's personal information in the marketplace."³¹ The Attorney General cites no evidence, record, or expert opinion supporting his or her conclusion that preventing the proliferation of a consumer's personal information in the marketplace is necessary to accomplish the purposes of responding to a deletion request under the CCPA.

²⁶ 1 Cal. Code Regs. 10(b)(1-2).

²⁷ Cal. Civ. Code § 1798.85(a)(7). Presumably, in proposing the regulation titled "Responding to Requests to Delete," the Attorney General is relying on Cal. Civ. Code § 1798.105.

²⁸ Cal. Civ. Code § 1798.105(c).

²⁹ ISOR at 19.

³⁰ ISOR at 17-18, 20.

³¹ ISOR at 20.

As there is no factual record indicating that the Proposed Regulation will further the purposes of the CCPA, the requirements of the Proposed Regulation amount to an arbitrary and capricious obligation on businesses. Unless, and until, a record is developed that demonstrates that the conversion of failed deletion requests to a request to opt-out would benefit the public, the Proposed Regulation should be abandoned.

C. Proposed Regulation 999.313(d)(1) exceeds the authority of the Attorney General.

The Office of the Attorney General cites Section 1798.185(a)(7) of the CCPA as the authority for the promulgation of Proposed Regulation 999.313(d)(1).³² Section 1798.185(a)(7) charges the Attorney General with:

Establishing rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business' determination that a request for information received by a consumer is a verifiable request, including ...providing a mechanism for a consumer who does not maintain an account with the business to request information through the business' authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.³³

As indicated in the text above, any regulation promulgated by the Attorney General under this grant of authority is required to "facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, which addresses sections...1798.105." As discussed in II.B, the CCPA gives no indication that one of the purposes of 1798.105 is to allow for the opt-out of the sale of information and the Attorney General offers no evidence that Proposed Regulation 999.313(d)(1)'s conversion obligation would facilitate the obtaining of information by a consumer, or would otherwise further the purposes of Section 1798.105.

As there is no factual record indicating that the Proposed Regulation will lead to the furtherance of any of the purposes identified in Section 1798.110 or Section 1798.115 of the CCPA, or will allow consumers to obtain information, the requirements of the Proposed Regulation amount to an arbitrary and capricious obligation on businesses. Unless, and until, a record is developed that demonstrates that the conversion of failed deletion requests to a request to opt-out would benefit the public, the Proposed Regulation should be abandoned.

³² ISOR at 16.

³³ Cal Civ. Code § 1798.185(a)(7).

III. Proposed Regulation 999.315(c).

Proposed Regulation 999.315(c) imposes an obligation on all entities engaged in the “sale” of personal information under the CCPA that is practically unworkable, and technically impossible.

As an initial matter, the CCPA provides consumers the right to opt-out from the “sale” of their “personal information.”³⁴ The statute obligates businesses that sell personal information to provide an “opt-out” link on the business’s website to allow California consumers to easily exercise that right.³⁵

Proposed Regulation 999.315(c) would require that, in addition to the opt-out link required by the statute, “[i]f a business collects personal information from consumers online, the business shall treat user-enabled privacy controls, such as a browser plug in 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.”³⁶ If made final and effective, this section would require businesses to treat any user-enabled privacy control, website plugin, browser plugin or privacy setting as a “valid request” to opt-out for that “browser, device or, if known, that consumer.”³⁷

The effect of this proposal is to foist a boundless, perpetual obligation on all businesses operating websites. A business would be required to recognize an unlimited and ever-evolving array of third-party software and settings for multiple browsers. Since businesses cannot control which settings, third-party software providers, or browsers will be utilized by California consumers, compliance with this obligation is functionally impossible, and businesses have no meaningful notice as to what electronic signals constitute a “valid request” under Proposed Regulation 999.315(c).

A. *The history of the “Do Not Track” Signal and its relevance to Proposed Regulation 999.315(c).*

Perhaps the closest analogue to the proposed “Do Not Sell” setting is the “Do Not Track” HTTP field (the “DNT Signal”).³⁸ The DNT Signal was originally proposed as a web browser setting that would allow a consumer to request that a web application disable its tracking of an individual user.³⁹ This proposal arose from a W3C working group.⁴⁰ After years of deliberation

³⁴ Cal. Civ. Code § 1798.120(a).

³⁵ Cal. Civ. Code § 1798.135(a)(1).

³⁶ Proposed Regulation § 999.315(c).

³⁷ Proposed Regulation § 999.315(c).

³⁸ See generally *CCPA Do Not Sell Rule: The Complete Guide*, COOKIEPRO (September 5, 2019), <https://www.cookiepro.com/blog/ccpa-do-not-sell-guide/>; *CCPA Consumer Rights & Do Not Sell Solutions*, ONETRUST, <https://www.onetrust.com/ccpa-consumer-rights-do-not-sell/> (last visited Dec. 5, 2019); *The CCPA Hidden Game Changer: “Do Not Sell My Personal Information”*, TRUYO, <https://insights.truyo.com/ccpa-hidden-game-changer> (last visited Dec. 5, 2019).

³⁹ See “All About Do Not Track”, Future of Privacy Forum, <https://allaboutdnt.com/>.

⁴⁰ *Tracking Preference Expression (DNT)*, W3C (January 17, 2019), (“...there has not been sufficient deployment of these extensions (as defined) to justify further advancement, nor have there been indications of planned support among user agents, third parties, and the ecosystem at large. The working group has therefore decided to conclude its work and republish the final product as this Note, with any future addendums to be published separately.”), <https://www.w3.org/TR/tracking-dnt/>.

and work at developing a universal standard for recognition and deployment of the DNT Signal, the project was abandoned due to insufficient deployment and support.⁴¹

The history of the DNT Signal is relevant to the Regulation because the DNT Signal likely is similar to a user-enabled privacy control (notwithstanding the inherent ambiguities associated with the term) in that both provide an automatic web-based mechanism to express a preference as to how data can be used.⁴² This functional similarity also suggests a similar developmental timeline. The DNT Signal was in development for 7 years before it was abandoned.⁴³ As such, it is, at a minimum, highly unlikely that a universal, recognizable Do Not Sell standard can be developed before July 1, 2020. Such a consensus requires the development of meaningful coalitions among disparate parties. Put simply, developing a workable consensus around a universally recognizable “Do Not Sell” signal takes time. But the Regulation ignores this reality entirely—instead, it foists an unworkable obligation onto businesses to incorporate a “Do Not Sell” button that recognizes *all* such signals. Indeed, the Initial Statement of Reasons published contemporaneously with the Regulation states exactly this.⁴⁴

B. Proposed Regulation 999.315(c) would be functionally unworkable without a universal standard.

Given the wide proliferation of different browsers, software settings, privacy settings and applications, some overarching, universal, and easily-recognizable standard must be imposed prior to obligating businesses to accept any signal whatsoever sent by any party indicating a “Do Not Sell” election. Indeed, it was this common sense observation that gave rise to efforts over the last decade to create a universal “Do Not Track” signal.

To the extent the Attorney General remains interested in creating a universal “Do Not Sell” signal, there is precedent for the development of such a standard. The W3C is an international community that seeks to develop web standards.⁴⁵ The development cycle of the W3C typically occurs as follows:

1. *Interest is generated on a particular topic.*⁴⁶ Members express interest in the form of member submissions, and a team monitors work inside and outside of W3C for signs of interest.⁴⁷ Also, W3C is likely to organize

⁴¹ *Tracking Preference Expression (DNT)*, W3C (January 17, 2019), <https://w3c.github.io/dnt/drafts/tracking-dnt.html>.

⁴² *Tracking Compliance and Scope* §1, W3C (January 17, 2019), <https://www.w3.org/TR/tracking-compliance/>.

⁴³ Ryan Paul, *W3C Privacy Workgroup Issues First Draft of Do Not Track Standard*, ARS TECHNICA (November 15, 2011), <https://arstechnica.com/information-technology/2011/11/w3c-privacy-workgroup-issues-first-draft-of-do-not-track-standard/?comments=1>; Tracking Protection Working Group, W3C, <https://www.w3.org/2011/tracking-protection/>

⁴⁴ ISOR at 24 (“This subdivision is intended to support innovation for privacy services that facilitate the exercise of consumer rights in furtherance of the purposes of the CCPA. This subdivision is necessary because, without it, businesses are likely to reject or ignore consumer tools.”).

⁴⁵ *About W3C*, W3C (last visited Dec. 5, 2019), <https://www.w3.org/Consortium/>.

⁴⁶ World Wide Web Consortium Process Document § 1: Introduction, W3C (March 1, 2019), <http://www.w3.org/2019/Process-20190301/> (emphasis added).

⁴⁷ *Id.*

a Workshop to bring people together to discuss topics that interest the W3C community.⁴⁸

2. *A Working Group is formed.*⁴⁹ When there is enough interest in a topic, the Director announces the development of a proposal for one or more new Interest Groups or Working Group charters.⁵⁰ W3C Members review the proposed charters.⁵¹ When there is support within W3C for investing resources in a topic of interest, the Director approves the group(s) and they begin their work.⁵²
3. *The Working Group is integrated with the rest of W3C and expectations are set.*⁵³
4. *The Working Group produces a Working Draft, which may ultimately become a Recommendation.*⁵⁴ Working Groups generally create specifications and guidelines that undergo cycles of revision and review as they advance toward W3C Recommendation status.⁵⁵ At the end of the process, the Advisory Committee reviews the mature technical report, and if there is support, W3C publishes it as a Recommendation.⁵⁶

The time it takes for W3C to develop a new web standard can vary widely. W3C states that the typical duration of a working group is *six months to two years*.⁵⁷ As stated above, work on the “Do Not Track” signal lasted many years, ultimately without conclusion. But in all events, the imposition of such an obligation—namely, recognition of a “Do Not Sell” signal—can only be feasibly accomplished once a consensus is reached across all browsers regarding the content and effect of the signal. To do otherwise would require businesses to anticipate hundreds or thousands of separate signals with no notice whatsoever.

C. Proposed Regulation 999.315(c) is unconstitutionally vague.

The Proposed Regulation violates both Federal and California due process requirements because it is unconstitutionally vague.⁵⁸ The Fourteenth Amendment due process guarantee against vagueness requires that laws provide adequate warning of the conduct prohibited.⁵⁹ Unconstitutional vagueness is applicable to civil enactments,⁶⁰ and the fact that the CCPA is not

⁴⁸ *Id.*

⁴⁹ *Id.* (emphasis added).

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² *Id.*

⁵³ *Id.* (emphasis added).

⁵⁴ *Id.* (emphasis added).

⁵⁵ *Id.*

⁵⁶ *Id.*

⁵⁷ World Wide Web Consortium Process Document § 5.2.6: Working Group and Interest Group Charters, (March 1, 2019), <http://www.w3.org/2019/Process-20190301/> (emphasis added).

⁵⁸ U.S. Const., 14th Amend; Cal. Const., art. IV, § 16.

⁵⁹ See *Maldonado v. Morales*, 556 F.3d 1037, 1045 (9th Cir. 2009) (quoting *Williams*, 553 U.S. 285, 304 (2008)).

⁶⁰ See *Fed. Comm’n v. Fox Television Stations, Inc.*, 567 U.S. 239 (2012) (Supreme Court found that the FCC’s interpretation of indecency did not give fair notice to Fox, even where the Commission declined to impose a forfeiture on Fox); see also *Bullfrog Films, Inc. v. Wick*, 847 F.2d 502, 513 (9th Cir.1988).

a criminal statute does not shield it from the purview of the vagueness doctrine. A provision may be unconstitutionally vague even if there is conduct that clearly falls within the provision's grasp.⁶¹ The standard for unconstitutional vagueness is whether the statute or regulation provides a person of ordinary intelligence with fair notice of what is prohibited, or whether the statute or regulation is so standardless that it authorizes or encourages seriously discriminatory enforcement.⁶²

Here, the terms "valid request" and "user-enabled privacy controls" are insufficiently definite to provide fair notice of the conduct proscribed because, *inter alia*, the Proposed Regulation's use of the term "user-enabled privacy controls" is boundless. Neither the CCPA nor the Proposed Regulations expressly define "user-enabled privacy controls." Furthermore, the term "user-enabled privacy control" does not have a common definition or a history of general usage.⁶³ Rather, the Proposed Regulation presumes that businesses will be able to determine when they are receiving a "Do Not Sell" signal from any given browser, plug-in, or application. Worse, while not formally defining "user-enabled privacy controls", the Regulation provides an illustrative, non-exhaustive, and spectacularly broad list of things that could constitute a user-enabled privacy control, including "browser plugin[s] or privacy setting[s], or other mechanism[s]." But these examples do nothing to clarify or restrict the scope of user-enabled privacy controls; they describe an unlimited array of existing categories, to say nothing of the future. As a result, businesses have no notice as to which opt-out mechanisms consumers might utilize.

The Regulation also automatically deems any such signal a "valid request" under the law. As a consequence, the Proposed Regulation expands the term "valid request" to include any signal generated by a "user-enabled privacy control," in essence adopting and importing an already fatally vague concept into the definition of "valid request."

Notice of what mechanisms will be used to communicate a preference is quite obviously required for a website to receive that preference. The operation and maintenance of a website is a complex undertaking, itself reliant of a multitude of software languages and third-party templates. Some websites use WordPress, others use JavaScript, others still are written in Ruby, *etc.* In many cases, websites have multiple domains and users do not always navigate to a business's "homepage." The Proposed Regulation ignores all of this, and fails to articulate even the bare minimum requirements of the proposed signal. This renders the Proposed Regulation unconstitutionally vague, and compliance functionally impossible.

⁶¹ Johnson v. United States, 135 S. Ct. 2551, 2561 (2015) (Supreme Court referred to its prior decision in Coates v. Cincinnati where it "deemed void for vagueness a law prohibiting people on sidewalks from conduct[ing] themselves in a manner annoying to persons passing by—even though spitting in someone's face would surely be annoying").

⁶² Maldonado, *supra*, 556 F.3d at p. 1045 (quoting Williams, 553 U.S. at p. 304).

⁶³ On November 15, 2019, a google search of the phrase "user-enabled privacy control" returned 3 results, two of which were articles restating the Proposed Regulations, while the remaining result was irrelevant. This tends to show that the phrase "user-enabled privacy control" is a term of art specific to the CCPA, and is not generally used or known to American businesses.

D. Proposed Regulation 999.315(c) does not provide "clarity" as required by California law.

California law requires that all regulations must use a "clarity" standard, which is satisfied when the regulation is "written or displayed so that the meaning of regulations will be easily understood by those persons directly affected by them." Specifically, a regulation shall be presumed to not comply with the "clarity" standard if, among other things, the "regulation uses terms which do not have meanings generally familiar to those 'directly affected' by the regulation, and those terms are defined neither in the regulation nor in the governing statute."

Here, businesses are required to treat "user-enabled privacy controls" as a "Do Not Sell" signal. The term "user-enabled privacy controls" is neither defined in the CCPA or the Proposed Regulations, nor is it a term that has any meaning in common parlance. Although the Proposed Regulation attempts to provide some clarity by offering a list of examples, the list is broad and effectively describes an infinite array of current and future mechanisms. As a result, there is no way for businesses that are "directly affected" by the Proposed Regulation to understand what specific mechanisms they must treat as "user-enabled privacy controls." Proposed Regulation 999.315(c) is unclear and does not fulfill California law's "clarity" standard.

As "user-enabled privacy controls" is not a term that has a meaning generally familiar to those directly affected by the regulation, Section 999.315(c) does not satisfy the requirements of the California APA and should be abandoned.

E. Proposed Regulation 999.315(c) inappropriately expands the CCPA by allowing non-consumer entities to "Opt-Out."

Under the plain language of the CCPA, the right to "opt-out" of the "sale" of "personal information" belongs solely to the consumer (or their authorized representative).⁶⁴ To be sure, a consumer may communicate this election electronically, through the use of a "Do Not Sell" link, but in each instance it is the consumer who is exercising this right.

The Proposed Regulation, however, appears to expand this right to devices. The Regulation states that "business[es] shall treat user-enabled privacy controls...as a valid request...*for that browser or device*, or, if known, for the consumer." This exceeds the scope of the original statutory right by essentially making an opt-out request not consumer-specific, but device-specific. Indeed, if an opt-out request is received from a "household" computer in this fashion, it is fundamentally unclear whether that request should be construed as being on behalf of one, all, or no members of the household. Moreover, it is unclear whether and how the "residency" of the device is to be determined. In short, by making a *setting* a valid opt-out request (as opposed to the affirmative act of a consumer as originally contemplated by CCPA), the Proposed Regulation creates more problems than it solves, and impermissibly expands the concept beyond the ample scope of the statute.

⁶⁴ Cal. Civ. Code § 1798.120(a) ("A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt out.").

F. Proposed Regulation 999.315 (c) would not benefit the Attorney General or the public.

The ISOR asserts that the Proposed Regulation is “necessary because, without it, businesses are likely to reject or ignore consumer tools.”⁶⁵ No evidence is provided for this assertion, nor could such evidence be offered since consumer tools that communicate an opt-out request currently do not exist.

As of December 5, 2019, there are no browsers that natively support a setting through which a consumer can signal a choice to opt-out of the sale of information. Additionally, as of December 5, 2019, there are no third-party plug-ins that offer similar functionality. While there are a several companies that advertise CCPA ‘do not sell’ solutions,⁶⁶ none of those advertised solutions appear to register opt-out communications through user-enabled privacy controls. As a result, if the Proposed Regulation is made final it would do nothing to benefit consumers. Moreover, the entire premise of the regulation—that businesses are likely to reject consumer tools—is wholly unsupported by any fact, study, or survey in the record.

IV. Proposed Regulation 999.315(f).

Proposed Regulation 999.315(f) would create an obligation for a business responding to a consumer’s request to opt-out of the sale of information to, among other things, “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.”⁶⁷

According to the ISOR provided by the Office of the Attorney General, Proposed Regulation 315(f) is “necessary to further the purposes of the CCPA in giving consumers control over the sale of their personal information and to address, in part, concerns raised by the public during the Attorney General’s preliminary rulemaking activities that consumers may not know the identity of the companies to whom businesses have sold their information in order to make an independent request.”⁶⁸

The approach set forth in Proposed Regulation 999.315(f) raises significant practical and legal concerns which are discussed below.

⁶⁵ ISOR at 24.

⁶⁶ See generally Ashlea Cartee, *CCPA Do Not Sell Rule: The Complete Guide*, COOKIEPRO (September 5, 2019), <https://www.cookiepro.com/blog/ccpa-do-not-sell-guide/>; *CCPA Consumer Rights & Do Not Sell Solutions*, ONETRUST (last visited Dec. 5, 2019), <https://www.onetrust.com/ccpa-consumer-rights-do-not-sell/>; *The CCPA Hidden Game Changer: “Do Not Sell My Personal Information”*, TRUYO, <https://insights.truyo.com/ccpa-hidden-game-changer>.

⁶⁷ Proposed Regulation § 999.315(f).

⁶⁸ ISOR at 25.

A. Bundling opt-out requests pursuant to Proposed Regulation 999.315(f) would not benefit consumers.

The language of Proposed Regulation 999.315(f) neither requires the business to disclose the identities of third parties it has sold a consumer's information to, nor does it allow a consumer to make an independent request.⁶⁹ The CCPA already provides consumers with notice of third parties who are reselling the consumer's information. Under the Act, any third party to whom a consumer's information was sold is prohibited from reselling that information "unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out."⁷⁰ The end result is that Proposed Regulation 999.315(f) does nothing to strengthen the CCPA's control mechanism, and merely undercuts the ability of a consumer to choose who should or should not sell their information.

Also, in the event the Attorney General can put forth evidence that Proposed Regulation 999.315(f) would give consumers control over their information, businesses will be unable to because the Proposed Regulation is contrary to the text of the CCPA. The CCPA states that a business "that has received direction *from a consumer* not to sell the consumer's personal information...shall be prohibited...from selling the consumer's personal information."⁷¹ At no point does the CCPA state that a business that has received direction *from another business* not to sell the consumer's information shall be prohibited from selling the consumer's information. The end result is that, per the language of the CCPA, a business that receives an opt-out instruction from another business may not honor that request.

B. The Attorney General has not put forth facts or studies to support the Proposed Regulation 999.315(f) as required by California law.

As is discussed in Section I.D, the APA requires that the Attorney General include "supporting facts, studies, expert opinion, or other information" in a rulemaking record to explain the necessity of a proposed regulation.⁷²

Under the CCPA, the Attorney General is required to promulgate regulations establishing rules that "facilitate and govern the submission of a request by a consumer to opt out of the sale of personal information" and to "govern business compliance with a consumer's opt-out request."⁷³ The ISOR does not provide any evidence that Proposed Regulation 999.315(f) is necessary to achieve either of these goals nor does it cite any facts, studies, or expert opinions in support of the Proposed Regulation.⁷⁴ The ISOR bases its support of Proposed Regulation 315(f) entirely on conjecture such as "[t]he realities of today's data-driven marketplace leave most consumers ignorant about what information is being collected about them..." and

⁶⁹ ISOR at 25.

⁷⁰ Cal. Civ. Code § 1798.115(d).

⁷¹ Cal. Civ. Code § 1798.120(d) (emphasis added).

⁷² 1 CCR 10(b)(1-2).

⁷³ Cal. Civ. Code § 1798.185(a)(4)(A-B).

⁷⁴ See generally ISOR at 23-25; see generally CAL. DEP'T OF JUSTICE, STANDARDIZED REGULATORY IMPACT ASSESSMENT: CALIFORNIA CONSUMER PRIVACY ACT OF 2018 REGULATIONS ("SRIA") 25-26 (2019), http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

conclusions such as “[t]his subdivision is necessary to further the purposes of the CCPA in giving consumers control over the sale of their personal information...”⁷⁵ No hard evidence is offered in support of these statements.

As there is no factual record indicating that Proposed Regulation 999.315(f) would effectuate the purpose of the CCPA, the requirements of Proposed Regulation 999.315(f) amount to an arbitrary and capricious obligation on businesses. Unless, and until, a record is developed demonstrating that flow down opt-out requests will provide more information to consumers about what information is being collected about them, or give consumers more control over the sale of their personal information, the Proposed Regulation should be abandoned.

V. Proposed Regulation 999.317(g).

Proposed Regulation 999.317(g) would apply a disclosure requirement upon a business that “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.”⁷⁶ Among other things, such businesses would have to compile and disclose within their online privacy policy the following metrics concerning consumer requests:

1. With regard to requests to know:
 - a. the number of requests to know received by the business,
 - b. the number of requests to know complied with, in whole or in part, by the business, and
 - c. the number of requests to know denied by the business.
2. With regard to requests to delete:
 - a. the number of requests to delete received by the business,
 - b. the number of requests to delete complied with, in whole or in part, by the business, and
 - c. the number of requests to delete denied by the business.
3. With regard to requests to “opt-out” of the sale of information:
 - a. the number of requests to opt-out received by the business,
 - b. the number of requests to opt-out complied with, in whole or in part, by the business, and
 - c. the number of requests to opt-out denied by the business.

⁷⁵ ISOR at 24-25.

⁷⁶ Proposed Regulation § 999.317(g)(1).

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

According to the Initial Statement of Reasons ("ISOR") provided by the Office of the Attorney General, Proposed Regulation 999.317(g) is "necessary" to "inform the Attorney General, policymakers, academics, and members of the public about businesses' compliance with the CCPA."⁷⁷

The approach set forth in Proposed Regulation 999.317(g) raises significant business and practical concerns which are discussed below.

A. Businesses are unable to determine with reliability whether Proposed Regulation 999.317(g) applies to them.

Many businesses will be unable to determine with a high degree of reliability whether Proposed Regulation 999.317(g) applies to them for four primary reasons. First, the term "annually" is vague and ambiguous. Second, the Attorney General did not provide clarity as to what activities "advance a person's commercial or economic interest." Third, it is impossible for most businesses to determine with reliability whether or not they are collecting personal information from California residents. Fourth, the amount of data collected by most businesses does not equate to the number of unique consumers about whom that data relates. The net result is that Proposed Regulation would create significant uncertainty as to which businesses are, and which businesses are not, required to report annual metrics.

1. The time period in which a business is required to examine the threshold volume of data is vague, ambiguous, and not susceptible to implementation.

If enacted, Proposed Regulation 999.317(g) would be triggered based upon the quantity of consumers whose information is collected "annually."

The term "annually" is not defined in Proposed Regulation 999.317(g), although its plain meaning is "every year."⁷⁸ While some businesses habitually collect information about more than 4 million Californians each and every year, and, therefore, would be subject to Proposed Regulation 999.317(g), many businesses may only periodically reach that threshold.

For example, if a company collected data regarding approximately 2 million California residents in year 1 and year 2, but collected data regarding 4 million California residents in year 3, the business certainly would not qualify as "annually" collecting the level of information required to trigger Proposed Regulation 999.317(g). If in year 4 the same business collected data about 3 million California residents, but in year 5 collected information about 4 million California residents, it is not clear whether the collection of information about 4 million California residents in two of the preceding five years (i.e., 40% of the time) would, or would not, be considered by the Office of the Attorney General as "annually" collecting a sufficient quantity of

⁷⁷ ISOR at 27.

⁷⁸ *Annually*, CAMBRIDGE DICTIONARY, <https://dictionary.cambridge.org/us/dictionary/english/annually> (last visited Oct. 27, 2019).

data to trigger the statute. The multiple interpretations, which could lead to diverging outcomes, violates the requirements of the California APA which mandates that a regulation must have sufficient “clarity” such that it does not, on its face, lend itself to “have more than one meaning.”⁷⁹

The term “annually” also raises confusion concerning whether it refers to a “calendar year” or “a 12 month period.” The difference is more than an academic exercise as it would directly impact whether (and when) some companies would be required to report data subject request statistics. For example, if during 2020 a company collected data about 2 million residents only in December, and during 2021 the same company collected data about 2 million residents only in May, under an interpretation of the regulation that looks to the calendar year the company would not be required to report any statistics as it had collected a total of 2 million data points in 2020, and 2 million data points in 2021. Conversely if “annually” refers to a 12 month period, the company would not be required to report statistics in December of 2020, or January, February, March, or April of 2021 as, during that time period, the company would have collected a total of 2 million data points in the preceding 12 month periods). At the end of May of 2021, the company would be required to report statistics as its total collection over the prior 12 months would hit 4 million. That condition would continue for the months of June, July, August, September, October, and November. Beginning in December of 2021, its 12 month rolling data collection would recede back to 2 million negating the requirement to disclose any statistic. The fact that “annually” lends itself to two interpretations, which would have diverging outcomes concerning whether a company need report any statistics (or the months in which such statistics need to be reported), also violates the dictate of the California APA that a regulation have sufficient “clarity” so that it does not have “more than one meaning.”⁸⁰

Given the ambiguity in Proposed Regulation 999.317(g), to the extent that the Office of the Attorney General continues to explore the idea of requiring companies to publish metrics, it should, among other things, solicit public comment concerning the time period over which a company must continuously collect data about Californians in order to trigger the requirements of Proposed Regulation 999.317(g).⁸¹

2. The lack of clarity regarding what activities constitute a “commercial purpose” would lead to divergent reporting.

Proposed Regulation 999.317(g) refers to consumer personal information which is “receiv[ed] for the business’s commercial purposes.” The CCPA defines a “commercial purpose” as something that:

⁷⁹ 1 Cal. Code Regs. 16(a)(1).

⁸⁰ Id.

⁸¹ To the extent that the Office of the Attorney General intended the Proposed Regulation to be triggered any time that a company collects personal information of 4 million California residents (e.g., “in a 12 month period” as opposed to “annually”) the Office of the Attorney General should amend the Proposed Regulation and seek additional comments as such a modification would substantially impact the scope of the Proposed Regulation. Among other things, the Attorney General should indicate in revised text whether the requirements of the Proposed Regulation would be triggered by data collected from a rolling 12 month period, data collected during the prior calendar year, data collected during the prior fiscal year, or data collected using another metric.

Advance[s] a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. "Commercial purposes" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.⁸²

Proposed Regulation 999.317(g) does not provide any additional clarity concerning the types of activities that the Attorney General believes do, or do not, "advance a person's commercial or economic interest."

Some activities clearly fall within the definition. For example, if a business receives consumer personal information and intends to subsequently sell that data for money, it clearly has received the data in order to advance its economic interest. Other activities clearly fall outside of the definition. For example, every time a California consumer visits the website of a business their IP address may be included in a log that reflects access to the business's website. Such logs are typically created and maintained to help manage websites, to track malicious activity, and to identify website-related errors or bugs.⁸³ Web log creation should certainly not be counted toward the 4 million threshold as it is used to support basic website functionality, not further a commercial or economic interest.⁸⁴

While the above are clear use-cases in which data advances a commercial or economic interest, or does not advance a commercial or economic interest, there are many use-cases in which the position of the Attorney General is unclear. For example:

- Does the Attorney General view personal information used by a company only for analytics purposes as advancing a commercial or economic interest?
- Does the Attorney General view personal information used by a company only to improve its products or services as advancing a commercial or economic interest?

⁸² Cal. Civ. Code § 1798.140(f).

⁸³ In addition, while the CCPA refers to "Internet Protocol address" among the types of data that might form the basis of "personal information," for it to do so IP address would need to be "reasonably linked, directly or indirectly, with a particular consumer." Cal. Civil Code § 1798.140(o)(1)(A). The Office of the Attorney General has provided no guidance in its Proposed Regulations, or otherwise, suggesting a view that IP addresses that are not linked to a consumer's name should be treated as "personal information." Any such interpretation would require an additional rulemaking pursuant to California Civil Code § 1798.185(a)(1) and would raise significant concerns. Among other things, it is well known that almost half of all web traffic comes from internet bots, which can visit a single site multiple times every day. This leads to the collection of IP addresses that, while ostensibly originating from California, are not associated with human users at all. Thus, a website that received 4 million "visits" associated with California IP addresses would have no way of knowing whether those "visitors" were people, let alone California residents.

⁸⁴ Other types of routine information collection similarly do not "advance" the economic interest of a business. For example, if a California consumer emails a business with a complaint, the personal information that they provide to the business (e.g., their email address) would hardly "advance" the business's commercial or economic interest. To the contrary, such communications may very well be about activities or issues that are not aligned with the interest of a company (e.g., a refund of a product, or a demand for reimbursement).

- Does the Attorney General view personal information used by a company to monitor the safety of its products or services as advancing a commercial or economic interest?
- Does the Attorney General view personal information used by a company to monitor the performance of its products or services as advancing a commercial or economic interest?

As the Attorney General has not identified the types of activities that it believes constitute “commercial purposes,” businesses will be unable to determine with certainty whether the 4 million threshold has been met. In the absence of guidance, each business would have to apply its own interpretation of that term which would lead to significant divergence concerning which companies do, and do not, report statistics under Proposed Regulation 999.317(g).

Given the ambiguity in Proposed Regulation 999.317(g), to the extent that the Office of the Attorney General continues to explore the idea of requiring companies to publish metrics, it should, among other things, solicit public comment concerning the types of activities that constitute “commercial purposes” and propose regulations that would clarify those activities.

3. Data that is collected for a “commercial purpose” is often not tied to residency.

Proposed Regulation 999.317(g) assumes that businesses track which data they collect from “consumers” – a term defined under the CCPA to mean California residents.⁸⁵

Residency information is typically not tracked by most businesses because such information is not necessary for most commercial transactions. For example, a restaurant located inside of LAX might execute 5 million credit card transactions every year, during which it collects customers’ names and credit card numbers as part of processing credit card transactions.⁸⁶ While credit card information is almost certainly collected for a “commercial purpose,” the restaurant would have no way of knowing whether its customers are residents of California or residents of another state (or country). Indeed, it is arguably prohibited under California law from soliciting such information.⁸⁷

The lack of data about residency is not limited to brick-and-mortar establishments. Businesses that collect personal information online rarely collect residency information. Take, for example, a company that solicits name and email address as part of distributing promotions, discounts, information, or coupons concerning its products. Email address does not, of course, suggest the residency of an online user. While theoretically a business might be able to identify the IP

⁸⁵ Cal. Civil Code § 1798.140(g) (defining consumer as a “natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations . . .”).

⁸⁶ Over 800 million people passed through LAX in 2018. See *generally Statistics for LAX*, LOS ANGELES WORLD AIRPORTS, <https://www.lawa.org/en/lawa-investor-relations/statistics-for-lax> (last visited Oct. 25, 2019). When an individual swipes or chip-inserts a credit or debit card, the individual’s name and credit card number are transmitted to the business. The zip code and address are generally not included.

⁸⁷ The Song-Beverly Act, Cal. Civ. Code § 1747.08(a)(1), states that a company may not “require as a condition to accepting the credit card as payment in full or in part for goods or services, the cardholder to write any personal identification information upon the credit card transaction form or otherwise.”

address of an online visitor at the time that they provided an email address, an IP address also does not identify the residency of an online user. At most it suggests that the user's access to the internet has some sort of connection to the state of California. This could indicate that the user is physically located within the state (e.g., on vacation, travelling for business, etc.). It also could indicate that the user is outside of the state, but using resources (e.g., a VPN connection, load balancer, or server) that is assigned a California IP address. In either case, any attribution concerning the residency of the individual is speculative at best.⁸⁸

To the extent that the Office of the Attorney General continues to explore the idea of requiring companies to publish metrics, it should, among other things, amend Proposed Regulation 317(g) to make clear that it applies only to companies that have "actual knowledge" that they have collected personal information for commercial purposes about 4 million California residents.⁸⁹

4. The quantity of data collected by a business does not always reflect the number of unique California residents whose data is collected.

Assuming that a business is able to identify (1) which types of data collected advance its commercial or economic interest, and (2) which data points derive from California residents, it then must identify the total quantity of California residents about whom it collects information annually. In many cases identifying the total quantity of unique individuals about whom it has collected information is extremely difficult, if not impossible.

For example, a brick-and-mortar retailer may be able to identify with relative ease that it processed 5 million credit card transactions in a year. It may be far more difficult, if not impossible, to identify the number of *unique* credit cards transacted during that same time period. Specifically, while the retailer may have had 5 million transactions, those transactions could be generated through the use of 1 million unique credit cards that, on average, were used five times at the retailer over the course of a year. Assuming that the retailer is able to de-duplicate transactions to derive the quantity of unique credit cards, that does not, in of itself, tell the retailer how many unique customers it had during the course of the year as most Americans own more than one credit card.⁹⁰ The net result is that identifying the number of unique individuals about whom a business collects information may, in many cases, require analytics that businesses do not currently possess.

For website operators, IP address collection presents a similar problem. Assuming that a business collected IP addresses for a "commercial purpose" (e.g., the IP addresses of individuals who registered to receive promotions, coupons, or mailings), and assuming that the

⁸⁸ Indeed, even if a business has a mailing address or billing address associated to an individual, neither of those data points establishes residency under 18 California Code of Regulations 17014, nor does it establish whether the individual is a "consumer."

⁸⁹ Alternatively, to the extent that the Attorney General decides to continue seeking the type of metric described in Proposed Regulation 317(g), the Attorney General should consider revising Section 317(g) to include an objective trigger that would be known by business and would be relevant to the type of metrics being disclosed. For example, the Attorney General might consider requiring businesses that receive a large number of requests to know, or requests to delete (e.g. more than 500 requests in the preceding calendar year) to publish statistics.

⁹⁰ While Americans on average own 2.69 credit cards, the quantity of credit cards owned can differ significantly depending upon a number of demographic variables including socio-economic status. See <https://www.creditkarma.com/credit-cards/i/how-many-credit-cards-does-the-average-american-have/> (last visited Oct. 27, 2019).

business has “actual knowledge” that a certain IP address relates to California residents,⁹¹ the business still cannot assume that each IP address corresponds with a unique individual. Many devices utilize a dynamic IP address, which means that the IP address assigned to a user or device changes over time. A single user might visit a website a dozen times over the course of a year (e.g., registering multiple email accounts for an online promotion, or checking the status of an online order from different computers). Identifying the number of unique individuals about whom the business collected information may ultimately be impossible.

The Standardized Regulatory Impact Assessment (“SRIA”) asserts that there is no incremental cost for collecting the information for reporting.⁹² This incorrect conclusion is based off the assumption that all data is linked to a unique individual whose residency is known. As discussed throughout this Section, uniqueness and residency information are not, as the SRIA assumes, immediately apparent nor easily accessible. In reality, businesses will have to develop methods and technologies to collect additional data or de-duplicate existing data in order to estimate this information. As the above indicates, such an investment still cannot account for the simple fact that there is not any method or technology which could currently be utilized to de-duplicate multiple IP addresses used by a single consumer, or to de-duplicate IP addresses used by bots and web crawlers. As such, the process of simply determining whether or not IP addresses collected by a business meet the threshold could take hundreds or thousands of man hours. Further costs would be needed to examine other types of data (e.g., email addresses, marketing databases, client databases, etc.) The net result is that the cost of simply identifying whether a company is subject to Proposed Regulation 999.317(g), *far* exceeds the SRIA’s \$500-\$1000 estimated cost of compliance.

In regard to cost, Bryan Cave consulted with The Crypsis Group, an incident response, risk management and digital forensics firm routinely engaged by Fortune 500 organizations to provide privacy and cybersecurity expertise, to further understand the cost and labor outlay required to meet the Proposed Regulation. Per Crypsis, the *minimum* amount of labor needed to provide the required metrics, assuming IP logs, PCI database exports, marketing information and all other sources of personal information are kept in a consolidated location, would be approximately 160 hours. However, the *likeliest scenario* is that generating the metrics would be a multi-month effort, requiring numerous internal resources who would be pulled from their day-to-day work, given the amount of research, consolidation, and quality control needed to produce such metrics. With automation and business analytics tools, those hours could potentially be reduced, but the cost of implementing automation and/or analytics would need to be considered. In either scenario, technology, automation, and labor could cost a business anywhere from several thousands to hundreds of thousands of dollars, depending on the size of the organization.

The Crypsis experts agreed that the SRIA’s \$500-\$1000 estimated cost of compliance could not be achieved by any organization that meets the requirements set forth in the Proposed Regulations.

⁹¹ As discussed in Section II(3), rarely does a business know whether an IP address relates to a California resident.
⁹² SRIA at 27.

To the extent that the Office of the Attorney General continues to explore the idea of requiring companies to publish metrics, it should, among other things, amend Proposed Regulation 999.317(g) to make clear that it applies only to companies that have “actual knowledge” that they have collected personal information for commercial purposes about 4 million California residents. Alternatively, it should revise the SRIA to accurately reflect the expected cost for businesses to identify whether they collect information about 4 million Californians and then resolicit comments based upon the total cost expected to be imposed by Proposed Regulation 999.317(g).

B. Calculating the metrics required by Proposed Regulation 317(g) would violate principals of data minimization.

Many businesses honor “requests to know” or “requests to delete” from non-California residents.⁹³ Proposed Regulation 999.317(g) would require that a business report metrics concerning the percentage of requests to know, or requests to delete, received only from California residents, and that it calculate its acceptance/denial rate and median response time based only upon those California-resident requests. As most businesses do not, as a matter of course, demand that individuals who submit access or deletion requests identify their country or state of residency, in order to track the reportable data businesses would be required to begin collecting residency information from individuals that submit data requests.

Requiring the collection of residency information contradicts the spirit of the CCPA and negates the principle of data minimization which has been recognized by various federal and international privacy organizations.⁹⁴

C. Proposed Regulation 999.317(g) would not benefit the Attorney General or the public.

The Initial Statement of Reasons asserts that Proposed Regulation 999.317(g) is “necessary to inform the Attorney General, policymakers, academics, and members of the public about businesses’ compliance with the CCPA.”⁹⁵ It is doubtful, however, that Proposed Regulation 999.317(g) will help the Attorney General or other policymakers determine whether a company is in compliance with the Act.

For example, if a company reported a 100% denial rate for access requests, the Attorney General would have no indication whether the denials reflect non-compliance, or complete compliance, with the obligations conferred by the CCPA. For instance, Proposed Regulation

⁹³ Among other things, the European General Data Protection Regulation contains a similar right of access and a right of deletion. See GDPR, Articles 15 and 17.

⁹⁴ See, e.g., F.T.C., INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (Jan. 2015), ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf. Data minimization is not only a well-accepted privacy and security principle, it is a legal requirement within some jurisdictions. See GDPR, Article 5. Specifically, companies that are subject to the European GDPR are required to identify a lawful purpose for any information collection. Presumably the collection of residency information would need to be based under Article 6(1)(f) of the GDPR (i.e., the “legitimate interest” of the business). Under Article 6(1)(f), however, a business would need to balance its desire to comply with the Proposed Regulation with the rights and freedoms of data subjects not to submit information to a company about their residency in order to exercise their privacy rights.

⁹⁵ ISOR at 28,

999.313(c)(4) *requires* businesses to deny certain access requests by stating 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.”⁹⁶ Should both Proposed Regulation 999.317(g) and Proposed Regulation 999.313(c)(4) be adopted, a company that collects the above information would have to deny, at least in part, 100% of access requests for “specific pieces of information it has collected about that consumer.”⁹⁷ That denial rate would be a consequence of the business’s compliance with the Act.

A refusal to disclose sensitive categories of information is not the only basis for denying an access or deletion request consistent with the statute. Requests may be routinely denied if:

- A company is unable to authenticate the identity of consumers;⁹⁸
- Production or deletion of personal information would violate a federal law;⁹⁹
- Production or deletion of personal information would violate a state law;¹⁰⁰
- Production or deletion of personal information would violate the privacy rights of another individual;¹⁰¹ or
- Deletion of information would frustrate efforts to prevent malicious, fraudulent, or illegal activity.¹⁰²

As the denial of a request to know or a request for deletion is not in-and-of-itself probative of a company’s compliance with the Act, the publication of metrics stating the percentage of requests received, honored, and denied will not “inform the Attorney General, policymakers, academics, and members of the public about [a] businesses’ compliance with the CCPA.”¹⁰³

Not only do such metrics provide little useful information to the Attorney General or the public concerning compliance with the CCPA, they can inadvertently lead to consumer confusion and harm. For example, consider two companies that are in a similar industry and collect similar types of information. Company A reports that it complies with access requests 60% of the time; Company B reports that it complies with access requests 100% of the time. Consumers may look at the metrics and assume that company B has better privacy practices than Company A. In fact, the numbers could reflect that Company A declined access requests 40% of the time because it identified a phishing scheme and prevented numerous attempts at identify theft. Company B might have lacked the same sophistication to identify phishing

⁹⁶ Proposed Regulation § 999.313(c)(4).

⁹⁷ Cal. Civ. Code § 1798.110(a)(5).

⁹⁸ Cal. Civ. Code § 1798.100(c); Cal. Civ. Code § 1798.105(c); Proposed Regulation § 999.313(c)(1-2); Proposed Regulation § 999.313(d)(1).

⁹⁹ Cal. Civ. Code § 1798.145(a)(1); Proposed Regulation § 999.313(c)(5).

¹⁰⁰ Cal. Civ. Code § 1798.145(a)(1); Proposed Regulation § 999.313(c)(5).

¹⁰¹ Cal. Civ. Code § 1798.145(j).

¹⁰² Cal. Civ. Code § 1798.105(d)(2); Proposed Regulation § 999.313(c)(3).

¹⁰³ ISOR at 28,

schemes and inadvertently contributed to identity theft by honoring access requests submitted by bad actors.

As there is no record indicating that the information that would be disclosed under Proposed Regulation 999.317(g) is relevant to identifying companies that are not in compliance with the CCPA, the requirements of Proposed Regulation 999.317(g) amount to an arbitrary and capricious imposition on businesses. Unless, and until, a record is developed that demonstrates that the information required by Proposed Regulation 999.317(g) would benefit the Attorney General and the public, Proposed Regulation 999.317(g) should be abandoned.

D. Proposed Regulation 999.317(g) exceeds the authority of the Office of the Attorney General.

The Office of the Attorney General cited Section 1798.185 of the CCPA as the authority for the promulgation of Proposed Regulation 999.317(g).¹⁰⁴ Presumably the Office of the Attorney General is referring to the generic grant within Section 1798.185 of the ability to “adopt additional regulations as necessary to further the purposes of this title.”¹⁰⁵

In the preamble to Assembly Bill 375, which ultimately became the CCPA, the California Legislature identified five specific purposes of the Act. Proposed Regulation 999.317(g) is not related to – let alone necessary to further – any of the identified purposes:

1. “The right of Californians to know what personal information is being collected about them.”¹⁰⁶ Proposed Regulation 999.317(g) would only inform a consumer about how many other people requested access to their records. Proposed Regulation 999.317(g) would *not* inform a consumer about what personal information has been, or is being, collected about them.
2. “The right of Californians to know whether their personal information is sold or disclosed and to whom.”¹⁰⁷ Proposed Regulation 999.317(g) would only inform a consumer about how many people submitted a request to opt-out; it would *not* inform a consumer about whether their personal information has been, or will be, sold or disclosed to a third party.
3. “The right of Californians to say no to the sale of personal information.”¹⁰⁸ Proposed Regulation 999.317(g) would *not* give Californians a right to say no to the sale of personal information.
4. “The right of Californians to access their personal information.”¹⁰⁹ Proposed Regulation 317(g) would only inform a consumer about how many other people

¹⁰⁴ Proposed Regulation § 999.317 (Note).

¹⁰⁵ Cal. Civil Code § 1798.185(b).

¹⁰⁶ CAL. CONST. art. I §1; Assembly Bill No. 375 §2(i)(1).

¹⁰⁷ Assembly Bill No. 375 §2(i)(2).

¹⁰⁸ *Id.* at § 2(i)(3).

¹⁰⁹ *Id.* at § 2(i)(4).

requested access to their records. Proposed Regulation 999.317(g) would *not* give a consumer access to their own personal information.

5. "The right of Californians to equal service and price, even if they exercise their privacy rights."¹¹⁰ Proposed Regulation 999.317(g) does *not* speak to the right of Californians to obtain equal services and prices.


It is clear that the legislature's intent in enacting the CCPA was to give California residents control over *their own* personal information. Proposed Regulation 999.317(g)'s requirement that companies publish metrics regarding how the company handles *everybody's* personal information has no bearing on this legislative intent. Simply put, nothing within Section 1798.185 states, or implies, that companies must publish metrics concerning the quantity of access, deletion, or opt-out requests that they receive.

As Proposed Regulation 999.317(g) exceeds the Attorney General's authority under Section 1798.185, it should not be enacted.

VI. Conclusion

For the reasons discussed above we encourage the Attorney General to reconsider the advisability of the Proposed Regulations, and, at a minimum, revise the proposals to better align with the stated purpose of the CCPA and avoid creating further ambiguity and confusion in the business community.

Very truly yours,



David A. Zetoony
Partner and Co-Chair Global Data Privacy and Security Practice
Bryan Cave Leighton Paisner LLP

Christian Auty
Counsel
Bryan Cave Leighton Paisner, LLP

Andrea Maciejewski
Associate
Bryan Cave Leighton Paisner LLP

¹¹⁰ *Id.* at § 2(i)(5).

Message

From: Nora Colbert [REDACTED]
Sent: 12/6/2019 5:29:43 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comment Letter on proposed regs to implement the CCPA
Attachments: Comment Letter on proposed regs to implement the CCPA.pdf

Please see the attached comment letter submitted by Kathleen C. Ryan.

Thank you,

Nora

Nora Colbert
SAA, Regulatory Compliance & Policy
American Bankers Association
A certified [Great Place to Work®](#)

1120 Connecticut Avenue, NW, Washington, DC 20036
[REDACTED]

December 6, 2019

Submitted Electronically

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

Re: Proposed California Consumer Privacy Act Regulations

Dear Attorney General Becerra:

The American Bankers Association¹ appreciates the opportunity to comment on the proposed regulations to implement the California Consumer Privacy Act (CCPA). We welcome the Attorney General's issuance of the proposed regulations, which provide some helpful clarifications of the law. However, we urge the Attorney General to consider the following recommendations to assist financial institutions, including banks, insurers and insurance producers, to comply with the CCPA, while helping to ensure that consumers' rights are protected in the manner the legislature intended.

Summary of Comments

In response to the proposed regulations, we highlight the following observations and recommendations, which are explained further in the proceeding commentary:

- The proposed requirements for verifying consumer requests should be revised in order to help prevent fraud while ensuring consumers can obtain financial services.
- The CCPA is intended to protect consumers' privacy, not to infringe on the rights of others; the final regulation should ensure that the CCPA does not apply to a business's intellectual property or require a business to reveal information that would infringe on rights of others.
- Financial institutions transfer sensitive personal information (PI) to service providers to provide products and services for customers; these transfers are not sales as contemplated in the CCPA, and the final regulations should include clarifications regarding "service providers" that do not burden these transfers.
- The proposed regulations include several new, burdensome and unnecessary requirements related to accepting and responding to consumer requests; these unauthorized requirements should be eliminated in the final regulations.

¹ The American Bankers Association is the voice of the nation's \$18 trillion banking industry, which is composed of small, regional and large banks. Together, America's banks employ more than 2 million men and women, safeguard \$14 trillion in deposits and extend more than \$10 trillion in loans.

- The CCPA requires that a business notify a consumer if the business will use PI for purposes other than those disclosed before collection, however, the proposed regulations would transform the notice requirement into an explicit "opt-in" right for consumers; the final regulations should not include this unauthorized restriction on the use of PI.
- The proposed regulation does not adequately address concerns about the privacy of "household" PI and would permit a consumer to access the PI of others without consent or knowledge; the final regulation should delete "household" from the PI definition or provide procedures for a safe harbor for compliance.
- The final regulation should not include new and burdensome data collection and reporting requirements for businesses that handle PI of 4 million consumers annually.
- The Attorney General should issue model disclosure forms, the use of which is voluntary, that provide a safe harbor, to assist financial institutions in achieving compliance.
- The final regulations should provide guidance on a business's right to "cure" certain violations.
- The look back period for the right to know should be limited to the CCPA's January 1, 2020 effective date; a 12-month look back period should be imposed on requests to delete information, and should not be applied to PI collected before the CCPA's effective date.
- Businesses need adequate time to prepare for compliance with the regulations; the final regulations should establish an effective date of 18 months after issuance.
- Enforcement actions should be limited to acts or omissions occurring on or after the final regulations' effective date.

Discussion of Comments

I. Revise the Proposed Requirements for Verifying Requests in order to Help Prevent Fraud While Ensuring Consumers Can Obtain Financial Services

Financial institutions hold sensitive personal information (PI), making them a particularly attractive target for those who seek to perpetrate fraud and other malicious activities. The CCPA and the proposed regulations, if not clarified, could inadvertently facilitate unauthorized access to a consumer's PI. Therefore, we support the proposed regulation's prohibition on providing sensitive PI, including social security numbers, account numbers, and PINs, in response to a verified request for PI. The proposed regulations provide financial institutions with welcome flexibility to establish their own procedures for verifying consumer requests and to use established authentication procedures for requestors who have password protected accounts.

However, since financial institutions are often the focus of bad actors who seek access to the sensitive PI that financial institutions maintain to serve their customers, a financial institution must be able to decline a consumer request that it reasonably suspects is fraudulent, even if the financial institution can match the request to pieces of PI that it holds. Otherwise, financial institutions will face the dilemma of either enabling fraud and making unauthorized disclosures, or of violating the CCPA for refusing a "verifiable" consumer request. We urge the Attorney General to acknowledge in the final regulations that a financial institution needs to authenticate a requestor's identity (i.e., that they are who they say they are) in addition to matching information in the request with PI that the financial institution may have. We believe that a safe harbor from liability should be granted to businesses that satisfy the criteria for verification in the final regulations.

The final regulations also should clarify that financial institutions are not required to delete PI gathered to verify a request if that PI is necessary for legitimate business purposes. The proposed regulation would require a business to delete PI received to verify a request. However, if the requestor is a customer and the PI is necessary for underwriting a loan or providing other services to the customer, or for any other purpose as set forth in CCPA § 1798.105(d), the business would need to retain the information for that purpose. Moreover, the business may need to retain the PI to be able to establish that it complied with the requirement to verify a request. We request that the final regulation permit businesses to retain PI under these and similar circumstances where necessary.

II. Ensure that the CCPA Does Not Apply to a Business's Intellectual Property or Require a Business to Reveal Information That Would Infringe on Rights of Others

The CCPA grants the Attorney General authority to establish exceptions that are necessary to comply with state or federal law, including laws relating to trade secrets and intellectual property.² The CCPA is intended to protect consumers' privacy rights; infringing on intellectual property rights, trade secrets, and the rights of others clearly would be an unintended consequence of the Act and proposed regulation. The final regulation should specify that a business is not required to disclose trade secrets or infringe on the rights of others.³

III. Retain the Proposed Clarification Regarding Service Providers

Proposed § 999.314 provides that an entity that otherwise meets the definition of a service provider is a service provider even if it collects PI directly from consumers at the request of a business. The proposed regulation would further provide that a service provider that also meets the definition of a business must comply with the CCPA for any PI it collects or sells outside its role as a service provider. We support the proposed clarifications regarding service providers, and urge the Attorney General to consider further clarifications. Financial institutions frequently depend on service providers to deliver products and services to consumers efficiently. These clarifications are critical to ensure that a financial institution can transfer PI to a service provider to serve the financial institution's customers without the transfer being deemed a sale of PI under the CCPA.

IV. Eliminate New, Burdensome and Unnecessary Requirements Related to Accepting and Responding to Consumer Requests

Our members are concerned that the proposed regulations impose new procedures, notices and substantive rights not found in the CCPA. These new requirements exceed the Attorney General's authority, and would impose new burden on financial institutions without a clear and commensurate benefit to consumers. Our comments are summarized below.

² Cal. Civ. Code § 1798.185(a)(3) (West 2019).

³ We note that Californians for Consumer Privacy has agreed to such a provision in the recent draft of the new ballot initiative §§ 1798.100(f) and 1798.185, which would avoid unintended consequences by expressly stating that a business is not required to disclose trade secrets.

Methods for Receiving Requests to Know and to Delete

The CCPA requires a business to provide consumers with methods to exercise their rights to know information.⁴ In addition to providing at least two methods for receiving requests to delete and know information, proposed § 999.312(c) would additionally require that one method must 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." For banks, and especially small banks, that typically operate brick-and-mortar branches as well as websites, the proposed regulation will create an additional burden not expressly required in the statute. The proposed regulations also fail to address how a business may determine its primary interaction channel with consumers. We recommend that the proposed requirement be eliminated.

Acknowledgement of Requests to Know and to Delete

The CCPA provides consumers with the right to access their PI and to have their PI deleted, provided that such requests can be verified.⁵ Proposed § 999.313(a) provides that a business must confirm receipt of a request for access to or to delete PI within 10 days of receipt and describe the business's verification process and when a consumer can expect a response. These proposed requirements are not found in the CCPA, are overly burdensome, and should be eliminated in the final regulation. They add an unnecessary step to the process that will do little to help consumers but will increase costs.

The proposed regulations also require a financial institution to treat a request to know or to delete that is deficient, or that comes in through a non-authorized channel, as if it was properly submitted. In the alternative, the proposal would require a business to contact the consumer and inform them how to properly submit the request. *See* proposed § 999.312(f). The proposed rules would also impose a 10-day deadline to confirm requests. We are concerned that this 10-day deadline could be impossible to meet if the request is received through a non-designated channel or is deficient. While it is important to allow consumers flexibility, when consumers depart from the norm, the financial institution should have additional time to handle the request.

Requirements Related to Processing Requests to Delete

For verified requests to delete PI, the proposed regulations would require a two-step process in which the consumer can separately submit and confirm the request to delete their PI. In addition, proposed § 999.313 would require the business to disclose the manner in which PI was deleted. The CCPA mandates that a business must comply with a verified request to delete PI, subject to certain exceptions.⁶ However, the statute does not mandate a two-step process or the disclosure of how PI was deleted. These added requirements in the proposed regulation will create operational burden on financial institutions without providing a meaningful benefit to consumers and should be eliminated.

The proposed regulation also would impose new and burdensome procedures for declining to delete PI, and would create new consumer rights not found in the CCPA. For requests to delete

⁴ Cal. Civ. Code § 1798.130.

⁵ *Id.* §§ 1798.100, 105, 110, 115.

⁶ *Id.* § 1798.105.

that cannot be verified, proposed § 999.313(d)(1) would authorize a business to decline the request, but the business would be required to notify the requestor that it cannot verify the request *and must treat the request as a request to opt out of sale*. The proposed regulations exceed statutory authority because the CCPA does not require businesses to notify consumers in such cases, and more importantly, the CCPA does not direct businesses to treat unverified deletion requests as requests to opt out of sales. In addition, the proposed regulations will require financial institutions that do not sell personal information—and for that reason do not offer a “Do Not Sell” button—to develop unnecessarily processes regarding opt-out requests. Therefore, these elements added in the proposal should be deleted from the final regulation.

Proposed § 999.313(d)(6) further provides that a business that declines a request to delete PI—presumably a verified request—must notify the requestor of the reason for the denial, including any statutory or regulatory exception. These proposed requirements are not found in the CCPA and would impose burdens on businesses that do not appear to be warranted.

The final regulation should clarify that a business is not required to delete PI, even if a request is verified, if one or more of the exemptions found in the CCPA applies. We recommend that § 999.313(d)(1) be revised as follows:

"For requests to delete, the business may deny the request if the business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, and/or if another exception or exemption applies, including but not limited to the purposes in Civil Code § 1798.105(d)."

Requirements Related to Requests to Opt Out of Sale of PI

The CCPA authorizes a consumer to opt out of the sale of PI.⁷ Proposed § 999.315(e) would require a business to act on a consumer's request to opt out of the sale of their PI within 15 days. While verification of an opt out request is not required, proposed § 999.315(h) permits a business to decline an opt out request if the business has a reasonable and documented belief that the opt out request is fraudulent. However, under the proposed regulations, the business must notify the requestor of the denial and the reason why it believes the request is fraudulent.

We support the proposed regulation's authorization for businesses to decline opt out requests believed to be fraudulent. However, the CCPA does not require a response to an opt out request within 15 days, nor does it require a business to notify a consumer of a denial and the reasons for a denial. It would be extremely challenging to respond to an opt out request within 15 days of receipt, and if suspected fraud is involved, explaining the reason for denial could arm bad actors with information they could use to avoid detection in the future. We urge the Attorney General to eliminate these proposed requirements.

In addition, our members have expressed significant concerns with the proposed requirement in § 999.315(c) that businesses collecting PI online treat the use of privacy controls, such as browser plug-ins, as signaling a consumer's request to opt out of the sale of their PI. This will require businesses to detect “do not track” signals in addition to opt-outs initiated from a web page. It will be impossible in most, if not all cases, to associate the do not track signals with an individual consumer. These proposed regulations create requirements that go well beyond what the CCPA

⁷ *Id.* §1798.120.

mandates. Browser plug-ins and the like are not aligned with the Act's complex and extremely broad definitions of "sale"⁸ and "personal information."⁹ The CCPA emphasizes consumer choice and specifically defines the "Do Not Sell" button as a mechanism for opt-out. It is neither consistent with the statute to create this additional mechanism nor clear that consumers who use plug-ins intend to opt out of CCPA-defined sales. Since these proposed requirements impose assumptions on consumers, and will be costly and unnecessarily difficult to administer, they should be eliminated from the final regulation.

The proposed regulations would also require a business to: (1) 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 opt-out, (2) instruct them not to further sell the information, and (3) notify the consumer when this has been completed. These proposed requirements exceed the statutory rights provided in the CCPA and should be deleted.

V. Remove the Unauthorized Restriction on Use of PI

The CCPA requires a business to notify consumers of the purpose for data collection, at or before the time of collection, and to notify a consumer if the business will use the PI for a purpose other than the purposes initially disclosed to the consumer.¹⁰ Proposed § 999.305(a)(3) would change this to an opt-in mandate and require businesses to obtain "explicit consent" from consumers to use data for purposes not described in the initial collection notice. The CCPA, however, does not authorize the Attorney General to include an opt-in requirement for the use of data. If the final regulations include the explicit consent requirement, businesses will be motivated to provide very broad explanations for why data is being collected, weakening the effectiveness of the CCPA's notice requirements. We urge the Attorney General to eliminate the proposed requirement for explicit consent to use data for purposes other than those disclosed initially.

VI. Address Concerns About Unauthorized Access to or Deletion of Household PI

Proposed § 999.318 provides that a business receiving a verifiable request to access or delete household information, from an individual without a password protected account, may comply by providing aggregate household information. In addition, the proposed regulation indicates that a business that receives a joint request for access to specific pieces of PI for the household or for deletion of household PI must comply with the request if it can individually verify all members of the household.

While we support the clarification that a business may comply with an individual request for household PI by providing only aggregate PI, if the requestor does not have a password protected

⁸ "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration. *Id.* § 1798.140(t)(1).

⁹ "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household. *Id.* § 1798.140(o)(1).

¹⁰ *Id.* § 1798.100(b).

account, the proposed regulations still expose individuals to release or deletion of their PI without their knowledge and consent. Aggregation is helpful but is not sufficient to protect people if the household consists of only two or three people. Moreover, the proposed regulations do not address how the business should respond if the requestor has a password protected account. The implication is that if the requestor has a password protected account, the business must provide the household PI to the requestor, or delete household PI. Likewise, we believe it is virtually impossible for a financial institution to determine whether all members of a household jointly request access or deletion, without a level of investigation into a particular household that would be extraordinarily burdensome—if not impossible. Our members are concerned about the transient nature of households – spouses may separate, or adult children may return or leave the household – and there is no practical method for a financial institution to determine the makeup of the household when a request is received.

For these reasons, we urge the deletion of “household” from the definition of “personal information.” We believe the unauthorized disclosure or deletion of PI by one household member is an unintended consequence of the CCPA.^[1] If the final rule does not delete “household” from the definition of PI or otherwise exempt businesses from disclosing PI or deleting PI for a household, we respectfully request that the final rule create a safe harbor from liability if the business follows the procedures in the final regulation regarding verification of requests for access to or deletion of household PI.

VII. New and Burdensome Record-Keeping Requirements Should Be Removed

The proposed regulations expand record-keeping obligations, especially for businesses that buy or receive the PI of more than four million consumers annually. *See* proposed § 999.317(g). For businesses who surpass this threshold, the regulation would require releasing consumer request metrics in the business’s privacy policy. This mandate goes beyond the CCPA and does not benefit consumers.

VIII. Issue Model Disclosure Forms to Assist Financial Institutions in Achieving Compliance

The CCPA and proposed regulations would require new disclosures, including a disclosure at or before collection of PI; the notice of right to opt out of sale of PI; and the notice of financial incentive. For these required notices, and for a business's privacy policy, the proposed regulations impose certain standards. These standards include, for example, that the disclosures must be easy to read and understandable to an average consumer, use a format that draws a consumer's attention to the notice, and that is readable on smaller screens. These standards impose vague and subjective standards on businesses. To facilitate compliance by financial institutions and other businesses, the Attorney General should consider publishing model disclosure forms. As with other laws, particularly the privacy disclosures under the federal Gramm-Leach-Bliley Act (GLBA), use of the model forms should be completely voluntary and left to the discretion of each financial institution, but using the forms should provide that any financial institution that uses the model is deemed in compliance with the CCPA requirements.

^[1] Notably, § 1798.145(p) in Californians for Consumer Privacy's new ballot initiative would not require a business to comply with a request to know or a request to delete PI for a household.

IX. Provide Guidance on a Business's Right to "Cure" Certain Violations

The CCPA establishes, in part, that a “business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance.”¹¹ We urge the Attorney General to describe how a business may “cure” a violation and therefore avoid liability. Further, in circumstances where a cure cannot unwind the effects of a violation, guidance is needed as to other means by which the business could cure, or mitigate against, the violation through implementation of business practices designed to avoid (in the future) the conditions that led to previous violations. The goal should be to provide incentives to encourage policies and procedures that meet the purposes for which the CCPA was adopted, not to set a trap for the unwary.

X. Limit the Look Back Period for the Right to Know and the Right to Delete

The CCPA requires a business to provide information to a consumer for the 12-month period preceding the business’s receipt of a verifiable consumer request.¹² The CCPA takes effect on January 1, 2020.¹³ The final regulation should provide that the 12-month look back period applies from the CCPA’s effective date of January 1, 2020, precluding any retroactive application of the CCPA to PI collected or sold before January 1, 2020.

In addition, the CCPA requires a business to delete a consumer's PI without any time limits; thus, a financial institution could have to delete PI collected years before the CCPA's effective date. We request the final rules clarify that a business is not expected to delete PI that was collected before the CCPA's effective date.

XI. Establish an Effective Date for Final Rules That Allows Businesses Adequate Time to Prepare for Compliance

The CCPA’s deadline for the Attorney General’s rulemaking is July 1, 2020¹⁴, six months after the law's January 1 effective date. Under the CCPA, the Attorney General could begin enforcement of CCPA on July 1, 2020—the same day that final rules could be published—leaving businesses no time to comply with the final rules. Our members support the goal of consumer privacy protection; but the CCPA is complex and many aspects of compliance remain unclear. In fact, part of the rationale for the regulations is to provide that necessary clarity. Financial institutions need to know what the final regulations require before they can revise their internal procedures, review and potentially revise contracts, work with vendors, including vendors that provide privacy compliance solutions, and train staff. Therefore, compliance should be mandatory – and enforceable – only after an appropriate transition period following the issuance of final regulations.

Under California law, the Attorney General must set an effective date that is no earlier than on one of four quarterly dates, based on when the final regulations are filed with the Secretary of State: January 1, if filed between September 1 and November 30; April 1, if filed between December 1 and February 29; July 1, if filed between March 1 and May 31; and October 1, if filed between June 1 and August 31. Effective dates may vary, however, if a different effective date is provided for in a statute or other law, if the adopting agency requests a later effective date, or if the agency

¹¹ *Id.* § 1798.155(b).

¹² *Id.* § 1798.130.

¹³ *Id.* § 1798.198.

¹⁴ *Id.* § 1798.185(a).

demonstrates good cause for an earlier effective date.

We respectfully request that the Attorney General exercise discretionary authority to request a later effective date and make the rules effective 18 months after issuance. Allowing financial institutions sufficient time to come into full compliance will ensure that they implement the full privacy protections intended by the legislature, ultimately benefitting consumers.

XII. Enforcement Actions Should Be Limited to Acts or Omissions Occurring on or After the Final Rules' Effective Date.

The CCPA provides that the Attorney General shall not bring an enforcement action under the CCPA until the earlier of (i) six months after the publication of final CCPA rules, or (ii) July 1, 2020.¹⁵ The Attorney General should clarify that any enforcement action will only be based on acts or omissions occurring on or after the CCPA's effective date. For example, if the enforcement date is July 1, 2020, because that is earlier than the six-month anniversary of the final regulations, then the Attorney General should clarify that any enforcement will be based only on conduct occurring on or after July 1, 2020 (the CCPA effective date).

Thank you for the opportunity to provide comments on this rulemaking. We welcome any questions you may have regarding our comments.

Sincerely,



Kathleen C. Ryan
Vice President & Senior Counsel

¹⁵ *Id.* § 1798.185(c).

Message

From: Shapiro, Tracy [REDACTED]
Sent: 12/6/2019 11:14:39 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comment on California Consumer Privacy Act Regulations
Attachments: DLA Piper CCPA Comment (Tracy Shapiro) (12-6-19).pdf

Dear Attorney General Becerra and Staff:

Attached please find our comment on the California Consumer Privacy Act Regulations.

Respectfully,

Tracy Shapiro
Partner



DLA Piper LLP (US)
555 Mission Street
San Francisco, CA 94105
United States
www.dlapiper.com

The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use, disclosure, dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please reply to the sender and destroy all copies of the message. To contact us directly, send to postmaster@dlapiper.com. Thank you.



DLA Piper LLP (US)
555 Mission Street
Suite 2400
San Francisco, California 94105-2933
www.dlapiper.com

Tracy R. Shapiro

December 6, 2019

By Electronic Mail

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 Spring Street
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Re: Comment on CCPA Proposed Regulations

Dear Attorney General Becerra and Staff:

DLA Piper appreciates the opportunity to submit these comments on the Attorney General's proposed California Consumer Privacy Act (CCPA) Regulations. Our clients take compliance with the CCPA very seriously, and we submit these comments with the aim of encouraging changes to the draft that will protect the privacy of consumers in a manner that is both effective and practical.

1. Requirements for Responses to Right to Know Requests Should Be Aligned With the Language of the Statute

The California Attorney General's proposed regulations state that for businesses' responses to "right to know" requests for categories of personal information, categories of sources, and/or categories of third parties, the business shall provide an individualized response to the consumer. Section 919.313(c)(9). It is important for the Attorney General to understand that, in our experience, most businesses lack the technical capabilities and resources to comply with this requirement. Creating an automated response process, which very likely will be necessary to handle the volume of consumer requests, often necessitates retaining significant outside engineering and other resources, and even then solutions are not always achievable, depending on the manner in which businesses store data. This places an outsized compliance burden on smaller businesses that are subject to CCPA.

Section 999.313(c)(10)c-d of the proposed rules should be amended, consistent with the statutory language of § 1798.110(a)(3) and (4), to clarify that the "right to know" requirements to specify the purpose for collecting or selling information and the categories of third parties with whom the business shares personal information need not be individualized to the specific consumer. These latter two requirements would be very difficult to comply with in a customized way for each requester and the CCPA does not require this.

Section 1798.110(a) requires businesses that collect personal information about the consumer "to disclose to the consumer the following:

- (1) The categories of personal information it has collected about *that consumer*.
- (2) The categories of sources from which *the personal information* is collected.
- (3) The business or commercial purpose for collecting or selling *personal information*.
- (4) The categories of third parties with whom the business shares *personal information*.”

Id (emphasis added).

The statutory language is clear that the first two of these requirements are specific to the consumer. The second two apply to personal information *in general*.

By contrast, the proposed regulation is unclear because it adds the clause italicized below, which requires a disclosure for each category of personal information collected about the consumer. This clause should be stricken:

(10) In responding to a verified request to know categories of personal information, the business 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*.

The references to “the category of personal information” should be stricken from the final rules except as to personal information collected about the consumer.

2. The Requirement for Signed Attestations from Data Sources in § 999.305(d)(2)b Should Be Removed

We agree with the Cal Chamber comment that the signed attestation requirement in § 999.305(d)(2)b should be removed from the final rules. The CCPA nowhere mentions a requirement for signed attestations from data sources and this requirement should not be added to the final rules. Compliance is impractical because data buyers rarely obtain personal information from a consumer-facing entity. Rather, data buyers typically have no relationship with the consumer-facing entity, do not know the identity of the consumer-facing entity, and have no way to contact the consumer-facing entity to obtain such an attestation. It may be possible for a certification of some sort to be passed along from the source, but obtaining an attestation directly from the source is impracticable.

3. The 45 Day Time Period to Respond in § 999.313(b) Should Be Clarified As Not Beginning to Run Until a Full Request Is Received

This subsection should be amended to make clear that the 45 day presumptive deadline to respond to requests begins once a full, verified request is received. The phrase in § 999.313(b) “regardless of time required to verify the request” may be read to imply that partial requests that the submitters delay completing would toll the 45 day response period.

The draft regulations impose extensive verification requirements before businesses may respond to requests. It is entirely within the discretion of the submitter to submit a full or a partial request and to submit verification information. A receiving business cannot supply verification information; rather, the requester must do so. If the submitting requester chooses, for example, not to provide the required verification information for 44 or even 89 days, it can make it impossible for the business to comply within the time frame. For these reasons, the 45 and 90 day periods should start to run once the requester has submitted sufficient verification information.

4. The Personal Information Prohibited from Being Disclosed In Response to a Data Subject Request Should Expand As the Data Elements That Can Trigger Class Action Lawsuits under § 1798.150(a)(1) Expand

The proposed regulations make clear that businesses do not need to provide certain sensitive information to consumers in response to their requests for access to personal information. However, the proposed regulation does not include all data elements that would trigger class action exposure in the event of a data breach. For example, the legislature has added biometric data to the list of data elements whose breach can trigger class action lawsuits under § 1798.150(a)(1), yet there is no prohibition under draft regulation § 999.313(c)(4) against disclosing this information in response to an access request. Section 999.313(c)(4) should make clear that there is no requirement to disclose such data in response to a CCPA access request.

5. The Final Rules Should Defer Requiring a “Do Not Sell” Automated Signal Until After It Is Clear Whether the CPRA Initiative Is Approved By California Voters

The proposed “Do Not Sell” signal idea in § 999.315(c) is utterly foreign to the CCPA text and does not exist in practice today. The idea cannot be implemented with the final regulation.

Even more fundamentally, the approach in the proposed regulation is very different from the approach in the CPRA Initiative, and would be superseded by the Initiative, if it becomes law. In contrast to the proposed regulation, the Initiative would make recognition of the signal optional, would provide for site-by-site choice by California residents instead of the default “never sell” position in the draft rules, would defer the requirement until 2023, and would require two rulemakings by a different agency to define aspects of this rule. If the Initiative is approved by the voters, it would waste Attorney General’s Office resources to wade through

defining the signal and overseeing its implementation, only to see the AG's authority over the signal stripped and two new rulemakings conduct by a new privacy agency.

For all these reasons, the final rules should remove § 999.315(c) until after the outcome of the CPRA Initiative is known.

6. The Obligation to Notify of a Do Not Sell Request All 3rd Parties to Whom A Business Has Sold Personal Information in the Previous 90 Days Must Be Substantially Modified in the Online Advertising Context

The proposed requirement in § 999.315(f) may work in the context of data brokers, where CCPA “sale” relationships are clear. However, in the diffuse Internet advertising ecosystem, “sale” relationships are far less clear, with website publishers often not knowing which entity is receiving personal information in exchange for a thing of value. In this context, website publishers and other online services are able to communicate consumers’ opt outs to advertising providers at the time they request an advertisement or otherwise make personal information available to them, but identifying all sales that occurred retroactively and contacting the entities to which they sold data for the past 90 days is impractical.

7. The Standards for Valuing Consumer Data in the Context of Free or Reduced Price Services Should Be Further Broadened

Businesses would benefit from additional clarity regarding their ability to offer different levels of service depending on whether consumers have agreed to have their data sold. The proposed valuation methods in Section 999.337 are inapplicable to many business models. For example, the proposed valuation methods do not fit with added product features or consumer experiences for which a business sells personal information, but the sale does not produce trackable revenue for a business and a “reliable method of calculation”. *See* § 999.337(b)(8). This is often the case, due to the broad definition of “sale” included in the CCPA, which results in businesses technically “selling” data but not receiving any quantifiable value in return. Similarly, where businesses provide enhanced product features to consumers, but offering those features involves a sale of personal information, there is often no market value for the enhanced feature, and assigning a value would be arbitrary. The final rules should expressly account for situations where the specific, “reliable” valuation methods are not practical and allow reasonable, good faith estimates in these cases.

8. The Record-Keeping Requirements to Compile Metrics Regarding The Volume of Requests and Response Times for Each Type of Data Subject Request Should Be Removed from the Final Rules

The requirements in § 999.337(g)(1) & (2) are found nowhere in the statute and are not even proposed in the CPRA Initiative. Requiring that businesses post this information in their website privacy policy would lengthen privacy policies to include data that is of marginal, if any, interest to consumers. What is more, requiring business to post “[t]he median number of days

within which the business substantively responded to requests to know, requests to delete, and requests to opt-out” found in § 999.337(g)(1)d would create a perverse incentive for businesses to conduct verification more quickly, increasing the chance of errors. These subsections should be removed from the final rules.

Respectfully,

DLA Piper LLP (US)

A handwritten signature in black ink, reading "Tracy Shapiro". The signature is written in a cursive, flowing style with a long horizontal line extending from the end.

Tracy Shapiro

Message

From: Yelena Grant [REDACTED]
Sent: 12/6/2019 9:32:33 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: John Libby [REDACTED]
Subject: comment on CCPA

Dear Attorney General Becerra,

Thank you for taking the time to address public comments. We would like to request clarification about identifying a California "resident". Section 1798.140(g) reads "'Consumer' means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier." Section 17014 of Title 18 of the California Code of Regulations (CCR) explains that the term "resident" includes: "(1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. All other individuals are nonresidents." However, neither of these sections, nor anything else in the legislation, seems to assist us in identifying a resident as it applies to a mobile application user (ex. phone or tablet). From a mobile application, the best way to identify a California resident as defined here is to use an Internet Protocol (IP) address lookup. We would like to confirm that this is an acceptable method to do so; further, it would be beneficial if this could be an established safe harbor in the regulation for the temporary and transitory use of IP address to identify residency. In addition, please provide specific guidance on all methods that would be allowed to identify a California resident when someone is using a mobile application and if the alternatives you specify provide a safe harbor.

Best Regards,

MobilityWare LLC

Yelena Grant | Sr. Manager Legal Affairs
[REDACTED] | www.MobilityWare.com
440 Exchange, Suite 100 | Irvine | California | 92602



Message

From: Andrew Madden [REDACTED]
Sent: 12/6/2019 11:16:11 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comment on Proposed Regulation Concerning the CCPA
Attachments: Joint Comments by CAC and ACA.pdf

Attached please find joint comments from ACA International and the California Collectors Association regarding the Proposed CCPA Regulation.



December 6, 2019

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

Re: Proposed Regulations 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).

Dear Attorney General Becerra:

On behalf of the members of the California Association of Collectors (CAC) and ACA International (ACA), we submit these comments in response to the Attorney General's notice of rulemaking on the California Consumer Privacy Act (CCPA).

I. BACKGROUND ON THE CALIFORNIA COLLECTORS ASSOCIATION AND ACA INTERNATIONAL

CAC promotes lawful consumer debt collection for creditors and government entities in California. CAC serves its more than 165-member credit and collection companies in California by providing education and training; promoting ethical professional conduct; and acting as a voice in business, legal, regulatory and legislative matters. CAC members provide accounts receivable services for a wide array of industries, including small businesses, hospitals, government, banks, retail, non-profits, utilities and more.

ACA is the nation's leading trade association for credit and collection professionals. Founded in 1939 with offices in Washington, D.C. and Minneapolis, Minnesota, ACA

*California Association of Collectors
One Capital Mall, Suite 800
Sacramento, CA 95814
www.calcollectors.net*

*ACA International (Washington Office)
509 2ND Street, N.E.
Washington, DC 20002
www.ACAInternational.org*

represents approximately 2,500 members, including credit grantors, third-party collection agencies, asset buyers, attorneys, and vendor affiliates in an industry that employs more than 230,000 employees worldwide and over 20,000 in California. Given its longstanding history and broad membership, ACA is uniquely positioned to comment on the proposed regulations.

CAC and ACA members include the smallest of businesses that operate within a limited geographic range of a single state, and the largest of publicly held, multinational corporations that operate in every state. The majority of our member companies, however, are small businesses. According to a recent survey, 44 percent of ACA member organizations (831 companies) have fewer than nine employees. Additionally, 85 percent of members (1,624 companies) have 49 or fewer employees and 93 percent of members (1,784) have 99 or fewer employees. Even though a majority of our members are small businesses, it is unclear how many of them will be impacted by the thresholds set forth in the CCPA given the diverse clients they serve.

As part of the process of attempting to recover outstanding payments, our members are an extension of every community's businesses. Our members work with these businesses, large and small, to obtain payment for the goods and services already received by consumers. In years past, the combined effort of CAC and ACA members have resulted in the annual recovery of billions of dollars for the economy. This savings is returned to and reinvested by businesses. This allows small businesses and large employers to limit losses on the financial statements of those businesses. Without an effective collection process, the economic viability of these businesses and, by extension, the American and California economy is threatened. Recovering rightfully-owed consumer debt enables organizations to survive; helps prevent job losses; keeps credit, goods, and services available; and reduces the need for tax increases to cover governmental budget shortfalls.

Importantly, our members are committed to fair, reasonable, and respectful practices and take their obligations in collecting debt and protecting consumer privacy very seriously. As legitimate credit and collection professionals, our members play a key role in helping consumers fulfill their financial goals and responsibilities while facilitating broad access to the credit market.

II. COMMENTS OF THE CALIFORNIA COLLECTORS ASSOCIATION AND ACA INTERNATIONAL

We strongly support the goal of protecting the privacy of consumers and their data, and we are committed to vigorous compliance in furtherance of this pursuit.

The current landscape for compliance in the area of data privacy for the accounts receivable industry is robust, including complex state and federal regulations. There are multiple federal laws our members are already complying with in this area including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Fair Credit Reporting Act (FCRA), the Fair Debt Collection Practices Act (FDCPA), the Gramm Leach

Bliley Act, and the Family Educational Rights and Privacy Act of 1974. Notably, the industry is already very restricted in what information and how information can be communicated to consumers under the FDCPA.

The CCPA is a robust state law, which many members of the accounts receivables management industry have argued is overly complex and burdensome. Notably, it also touches many businesses outside of California if personal information of California consumers is collected, making its reach potentially much broader than California agencies. As the Attorney General moves forward in implementing the CCPA, it is critical to be diligent in ensuring legitimate businesses are not faced with insurmountable regulatory burdens surrounding data privacy laws, particularly if they stifle innovation or have a disproportional impact on small businesses. It is also critical to ensure legitimate businesses are provided crystal clear guidelines regarding compliance.

It is currently unclear how the CCPA will be harmonized with federal laws like HIPAA, the FCRA, the FDCPA, Gramm Leach Bliley Act, and the Family Educational Rights and Privacy Act of 1974. Furthermore, the General Data Protection Regulation went into effect in the European Union in May 2018 and impacts certain CAC and ACA members in the U.S., as well as international accounts receivable management agencies.

The accounts receivable industry does not collect consumers' information for any purposes other than those permitted by privacy and consumer financial protection laws. However, because of the breadth of the law and the lack of clarity surrounding exemptions certain practices of the accounts receivable management businesses could be swept under the law. Outlined below are several areas where the proposed regulations need additional clarification.

III. AREAS OF CONCERN

a. Confusion regarding consumer requests and statutory exemptions

The proposed requirement that a business respond to a consumer's request to know or a request to delete even when relying on a statutory or regulatory exception to the CCPA [999.313(c)(5), 999.313(d)(6(a), and the associated recordkeeping requirements in 999.317] undermines the statutory/regulatory exceptions of the statute.

The CCPA's statutory/regulatory exceptions apply to businesses that are already regulated and thus need not implement the CCPA to the extent it conflicts. However, to then require those same businesses to respond to a consumer request only to deny it based on a regulatory/statutory exception, forces those businesses to incur unnecessary costs and build infrastructure, which undercuts the purpose of the statutory exception. This aim could be accomplished instead by informing customers in the CCPA notice of the applicable statutory/regulatory exception.

b. **Regulation Section 999.308. Privacy Policy Conflict**

Regulation section 999.308(b)(1)(d) conflicts with Code of Civil Procedure (CCP) section 1798.110, which indicates information can be provided in a more general format. Regulation section 999.308(b)(1)(d) requires businesses for “each category of personal information collected” to 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 CCPA, however, does not require this information to be disclosed for “each category of personal information collected”, and thus this Regulation section 999.308 inappropriately extends the requirements of the statute.

c. **Regulation Section 999.305. Notice at Collection of Personal Information**

The proposed regulation is unclear as to how a third-party collection agency should handle consumer information that was involuntarily collected. Such situations could arise after a collection agency has received and complied with a cease-and-desist order from a consumer on an account but after time the consumer elects to make a payment. The consumer directly reaches out to the collection agency via phone or online to make a payment on the account without any interaction being initiated by the agency. The agency’s phone system records the incoming phone number and/or the agency’s online payment portal collects financial information relevant for the payment. The agency was not actively pursuing payment or trying to collect this information. The proposed regulations are unclear on how or if an agency would send a notice to a consumer about the intent to collect information, when the agency had no intent to do so.

d. **Regulation Section 999.313. Responding to Requests to Know and Requests to Delete**

Regulation section 999.313 requires clarification as to how third-party collection agencies handle requests for information when voice recordings are involved.

Section 999.313 sets forth requirements regarding requests to know information and requests to delete information. A consumer has the right to request all information a business has collected. CCPA section 1798.140 lists audio information and biometric information as two of the categories of personal information. Biometric information as defined by the section includes voice prints and recordings. The proposed regulations and the CCPA address covered “information,” but recordings are a tangible. It is unclear what the expectation is when handling a consumer’s request for information when an agency has recordings. Does the agency identify that it has recordings? Does the agency produce the actual recordings and in what form? Does the agency produce a transcription of the recordings?

e. **Effective Date**

The CCPA is broad in scope and complex. Many aspects of the CCPA and the proposed regulations are still unclear and will take time for businesses to gain clarity and properly

comply. We respectfully request that the Attorney General ask for a later effective date and make the rules effective 1 year after the date of issuance.

IV. CONCLUSION

In addition to our joint comments we encourage you to take into consideration the critical comments submitted by the California Chamber of Commerce which further detail the proposed regulations impact on the broader business community and the consumers they serve both inside and outside of the state of California.

CAC and ACA appreciate the opportunity to comment on the proposed regulation.

Submitted by:



Cindy Yaklin
Legislative Chair
California Association of Collectors



Andrew Madden
Vice President of Government and State Affairs
ACA International

Message

From: Maia Hamin [REDACTED]
Sent: 12/6/2019 11:57:20 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comment on Proposed Text of Regulations, CCPA
Attachments: CCPA Regulations Deletion Comment.docx; CCPA Regulations Deletion Comment.pdf

To the Privacy Regulations Coordinator, California Office of the Attorney General,

I'm a student in the Computer Science Department at Princeton University who would like to submit a comment to your office on some of the technical considerations relevant to the Request to Delete provision in the proposed regulations on the California Consumer Privacy Act. I've attached my comment as both a PDF and a Word document to this email --- let me know if there is any more information I can provide.

Thank you for taking my comments into consideration, and good luck with the future rule-making process!

Maia Hamin

Before the
California Office of the Attorney General
Los Angeles, CA

In the Matter of)
Title 11, Division 1, Chapter 20 of the CCR,) Notice File
Number Z2019-1001-05
concerning the California Consumer Privacy Act (CCPA).)

Comments by Maia Hamin, Student, Princeton University

Submitted December 6, 2019.

I am Maia Hamin, a student in the Computer Science Department of Princeton University. This is a response to the proposed text of a rulemaking action by the California Department of Justice, which

further outlines, among other elements of the California Consumer Privacy Act, the ways in which businesses must comply with consumer requests for the deletion of their personal data. In technical practice, “deletion” describes a range of degrees and methods of information erasure, and this comment attempts to lay out some of the possible technical interpretations of compliant deletion under the CCPA. The proposed text of the regulation expands the Act’s deletion provision by allowing businesses to respond to a deletion request by de-identifying or aggregating consumer data, and this comment further explores how de-identification in particular might become attractive for businesses aiming to achieve compliance with CCPA’s deletion request requirements, despite the fact that the properties and associated risks of de-identified data substantially differ from those of deleted data.

A central principle from the original text of the CCPA is the right of a consumer to request that a business delete any of their personal information it has collected. Previous data protection regulations have enshrined similar rights, but there has been widespread dispute about which technical implementations of deletion meet the compliance requirements (as an example, the GDPR’s “erasure” requirement has been interpreted to require everything from de-identification¹ to the incineration of physical storage devices²). In the proposed CCPA regulations, § 999.313(d) (“Responding to Requests to Delete”), specifies that a business can comply with a deletion request by “permanently and completely erasing the personal information on its existing systems with the exception of archived or back-up systems; de-identifying the personal information; or aggregating the personal information.”

In examining the guidance the current text provides on data erasure, it’s clear that the two distinguishing properties are permanence and completeness. Broadly, implementations of deletion can be grouped into two categories: “soft” deletion, in which the link between an access point and a data object is severed, and “hard” deletion (also called secure deletion), in which the physical memory that describes a data object is wiped, corrupted, or destroyed. For example, when someone deletes a file on a computer,

¹ Tolson, Is the Anonymization of Information the Same as Erasure? (2019). (<https://www.infogoto.com/is-the-anonymization-of-personal-data-the-same-as-data-erasure/>)

² Matthews, What You Need to Know About Data Destruction Post-GDPR (2019). (<https://it.toolbox.com/articles/what-you-need-to-know-about-data-destruction-post-gdpr>)

the file is soft deleted when its metadata is changed to indicate that it should no longer be visible to users. However, the bits representing the file's contents still exist somewhere in memory until they are overwritten by a new file, which means that someone with access to the physical device might still be able to reconstruct the file (which is, in fact, exactly how file recovery programs work). In order to guarantee that files are hard deleted, specialized software tools must overwrite or wipe free space (including the file's location, now presumed to be safe to overwrite) on the memory of the machines where the data is stored.³ Hard deletion, in which data is guaranteed to be irrecoverable, is the level of deletion referenced by those who espouse hardware destruction as a GDPR-compliant method of deletion. Without these hard delete guarantees, soft deletion methods cannot be guaranteed to be permanent nor complete, since the right tools might allow a user with access to the physical memory of a device to reconstruct data, and so soft deletion may fail to meet the regulation's standards for data erasure.

Adding to the complexity, businesses must execute deletion requests on data that exists not in single files but in multiple databases, which may be linked to or derive from each other, as well as higher-level systems which manipulate information from these databases. Soft deletion of a customer's information requires a business to locate all possible sources of personal information, follow the flow of data throughout its system to the different places where that information might have been added to new databases and systems, and break the link to the information at each one of these locations without breaking or corrupting any of the other data in the system.⁴ This is already a challenging task, which will require many businesses to conduct reviews of their entire data pipeline and develop tools for interacting with databases which might not have previously supported deletion functionality.

In addition, if the current legislation is interpreted to require hard deletion guarantees, then a business must also ensure that the memory on the physical machine corresponding to every broken link is securely wiped. Frequently, business data is split across many different machines, whether across multiple

³ For more information on secure deletion: Reardon et al, [SoK: Secure Data Deletion](https://oaklandsok.github.io/papers/reardon2013.pdf) (2016). (<https://oaklandsok.github.io/papers/reardon2013.pdf>)

⁴ For more information on the challenges of deletion in a business data environment: Wattamar, *GDPR and the Challenges of Digital Memory* (2018). (<http://sitn.hms.harvard.edu/flash/2018/gdpr-challenges-digital-memory/>)

servers in a business's data center or across thousands of different servers belonging to a third-party cloud computing provider. In order for these complex data-management systems to function, specifics of memory management are often abstracted away from the kind of high-level software applications a business operates. So, for an application or website to provide guarantees about hard deletion, the nature of its interaction with its data storage system might have to change significantly, which would require coordinated change from both the application and from its storage system provider. These alterations are certainly possible, and the aim of this explanation is merely to lay out the ways in which the two (broad) levels of deletion provide different guarantees and come with different levels of implementation burden.

Given the technical challenge of implementing a deletion system with permanence and completeness guarantees, it may be tempting for businesses to meet the CCPA's deletion request requirement by using one of the other two methods the statute lays out: de-identifying or aggregating the personal information. Of course, the process of aggregation, in which a customer's personal information is combined with other consumers' to generate descriptive data about a group of customers, does not itself delete a consumer's data record. Instead, the individual data record which holds the customer's personal or identifying data must be deleted once added to the aggregation in order to fulfill the spirit of the right to request deletion. Without additional specificity about how this individual-level data should be erased, it might be ambiguous whether the same standards of permanence and completeness apply, or whether addition to aggregation is a way to circumvent the more stringent technical requirements for processes which only involve data erasure.

In contrast to aggregation, de-identification involves modification of the individual data record pertaining to a customer, and might therefore be used in place of, rather than in addition to, erasure. To comply with the CCPA's definition of de-identified data, the data entries corresponding to a particular customer must be purged of any information which could "reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer." Finding and removing that information requires a systematized process for information discovery and erasure very similar to the one required for deletion. But, since the text does not specify that the removal of

identifying information must be permanent and complete, akin to data erasure, the erasure of this identifying information could be achieved with soft deletion (or even through other processes with less stringent guarantees). If, due to this lowered standard, businesses find it technically easy to implement compliant de-identification than deletion, this might become the solution of choice for businesses looking to achieve CCPA compliance in their responses to deletion requests.

The possibility that de-identification will become the standard remedy for deletion requests is potentially troublesome because de-identification can be less privacy-protective and secure than full erasure. A host of high-profile examples⁵ of successful re-identification of sensitive information have shown that de-identification is extremely challenging to implement successfully. Assumptions about what information can be safely included in a de-identified dataset are often proven disastrously wrong, and will continue to change as we develop increasingly powerful machine learning models for extracting patterns from data. For these reasons, the release, whether deliberate or as part of a breach or theft, of de-identified data can pose a security and privacy risk to a consumer. These risks are not present when data has been properly erased (and are seriously reduced even when data has been soft deleted, due to the significantly higher burden imposed on an attacker who must access the physical storage system). And, even outside of the specific risks posed by re-identification, there might be a host of reasons a consumer submitting a deletion request would prefer their information be expunged entirely from a system rather than just stripped of its identifiers. The question of when and where the customer's right to deletion can be satisfied by de-identification might benefit from further clarification, since there may be contexts in which de-identification provides all of the security and privacy benefits of deletion. But, given the increased risk posed by de-identified data, it might be undesirable to make de-identification the default response to deletion requests, which is at risk of happening unless the implementation standards and appropriate use cases for each are clarified.

⁵ *For an overview of several high-profile re-identification attacks:* Lubarsky, Re-Identification of “Anonymized” Data (2017). (<https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/>)

In short, adding specificity about the requirements of erasure in the text of the proposed regulations around the CCPA could encourage businesses to focus on the deletion properties that are most salient to customer privacy and data governance rights. It might prove useful for the regulation to differentiate between permanence and completeness requirements for application-level deletion, which might require that data be unlinked at its source and throughout its flows and transformations within the system, and storage-level deletion, where storage providers might be obliged to make available functionality for overwriting data in order to provide hard deletion guarantees.

Recommendations:

- Make erasure the default response to requests to delete, and require a legitimate reason that erasure is impractical when businesses wish to instead use deidentification to fulfil their obligation to such a request.
- In such cases, impose similar permanence and completeness requirements on de-identification. Since simple removal of identifying information is known to allow re-identification of data in many contexts, businesses should adhere to current best practices for de-identification to provide these guarantees.
- Clarify the meaning of “permanently and completely erased” by specifying that a business must make all non-exempt information about a requester permanently unretrievable throughout their data storage and processing systems.

Enshrining the answers to these questions in law will provide guidance for businesses as they implement their deletion request response systems, and help guarantee that standards for data deletion reflect the people’s judgement about the spirit and intention of the right to deletion laid out in the CCPA.

Before the
California Office of the Attorney General
Los Angeles, CA

In the Matter of)
Title 11, Division 1, Chapter 20 of the CCR,) Notice File Number Z2019–1001–05
concerning the California Consumer Privacy Act (CCPA).)

Comments by Maia Hamin, Student, Princeton University

Submitted December 6, 2019.

I am Maia Hamin, a student in the Computer Science Department of Princeton University. This is a response to the proposed text of a rulemaking action by the California Department of Justice, which further outlines, among other elements of the California Consumer Privacy Act, the ways in which businesses must comply with consumer requests for the deletion of their personal data. In technical practice, “deletion” describes a range of degrees and methods of information erasure, and this comment attempts to lay out some of the possible technical interpretations of compliant deletion under the CCPA. The proposed text of the regulation expands the Act’s deletion provision by allowing businesses to respond to a deletion request by de-identifying or aggregating consumer data, and this comment further explores how de-identification in particular might become attractive for businesses aiming to achieve compliance with CCPA’s deletion request requirements, despite the fact that the properties and associated risks of de-identified data substantially differ from those of deleted data.

A central principle from the original text of the CCPA is the right of a consumer to request that a business delete any of their personal information it has collected. Previous data protection regulations have enshrined similar rights, but there has been widespread dispute about which technical implementations of deletion meet the compliance requirements (as an example, the GDPR’s “erasure” requirement has been interpreted to require everything from de-identification¹ to the incineration of physical storage devices²). In the proposed CCPA regulations, § 999.313(d) (“Responding to Requests to Delete”), specifies that a business can comply with a deletion request by “permanently and completely erasing the personal information on its existing systems with the exception of archived or back-up systems; de-identifying the personal information; or aggregating the personal information.”

In examining the guidance the current text provides on data erasure, it’s clear that the two distinguishing properties are permanence and completeness. Broadly, implementations of deletion can be

¹ Tolson, Is the Anonymization of Information the Same as Erasure? (2019).
(<https://www.infogoto.com/is-the-anonymization-of-personal-data-the-same-as-data-erasure/>)

² Matthews, What You Need to Know About Data Destruction Post-GDPR (2019).
(<https://it.toolbox.com/articles/what-you-need-to-know-about-data-destruction-post-gdpr>)

grouped into two categories: “soft” deletion, in which the link between an access point and a data object is severed, and “hard” deletion (also called secure deletion), in which the physical memory that describes a data object is wiped, corrupted, or destroyed. For example, when someone deletes a file on a computer, the file is soft deleted when its metadata is changed to indicate that it should no longer be visible to users. However, the bits representing the file’s contents still exist somewhere in memory until they are overwritten by a new file, which means that someone with access to the physical device might still be able to reconstruct the file (which is, in fact, exactly how file recovery programs work). In order to guarantee that files are hard deleted, specialized software tools must overwrite or wipe free space (including the file’s location, now presumed to be safe to overwrite) on the memory of the machines where the data is stored.³ Hard deletion, in which data is guaranteed to be irrecoverable, is the level of deletion referenced by those who espouse hardware destruction as a GDPR-compliant method of deletion. Without these hard delete guarantees, soft deletion methods cannot be guaranteed to be permanent nor complete, since the right tools might allow a user with access to the physical memory of a device to reconstruct data, and so soft deletion may fail to meet the regulation’s standards for data erasure.

Adding to the complexity, businesses must execute deletion requests on data that exists not in single files but in multiple databases, which may be linked to or derive from each other, as well as higher-level systems which manipulate information from these databases. Soft deletion of a customer’s information requires a business to locate all possible sources of personal information, follow the flow of data throughout its system to the different places where that information might have been added to new databases and systems, and break the link to the information at each one of these locations without breaking or corrupting any of the other data in the system.⁴ This is already a challenging task, which will

³ For more information on secure deletion: Reardon et al, [SoK: Secure Data Deletion](https://oaklandsok.github.io/papers/reardon2013.pdf) (2016). (<https://oaklandsok.github.io/papers/reardon2013.pdf>)

⁴ For more information on the challenges of deletion in a business data environment: Wattamar, *GDPR and the Challenges of Digital Memory* (2018). (<http://sitn.hms.harvard.edu/flash/2018/gdpr-challenges-digital-memory/>)

require many businesses to conduct reviews of their entire data pipeline and develop tools for interacting with databases which might not have previously supported deletion functionality.

In addition, if the current legislation is interpreted to require hard deletion guarantees, then a business must also ensure that the memory on the physical machine corresponding to every broken link is securely wiped. Frequently, business data is split across many different machines, whether across multiple servers in a business's data center or across thousands of different servers belonging to a third-party cloud computing provider. In order for these complex data-management systems to function, specifics of memory management are often abstracted away from the kind of high-level software applications a business operates. So, for an application or website to provide guarantees about hard deletion, the nature of its interaction with its data storage system might have to change significantly, which would require coordinated change from both the application and from its storage system provider. These alterations are certainly possible, and the aim of this explanation is merely to lay out the ways in which the two (broad) levels of deletion provide different guarantees and come with different levels of implementation burden.

Given the technical challenge of implementing a deletion system with permanence and completeness guarantees, it may be tempting for businesses to meet the CCPA's deletion request requirement by using one of the other two methods the statute lays out: de-identifying or aggregating the personal information. Of course, the process of aggregation, in which a customer's personal information is combined with other consumers' to generate descriptive data about a group of customers, does not itself delete a consumer's data record. Instead, the individual data record which holds the customer's personal or identifying data must be deleted once added to the aggregation in order to fulfill the spirit of the right to request deletion. Without additional specificity about how this individual-level data should be erased, it might be ambiguous whether the same standards of permanence and completeness apply, or whether addition to aggregation is a way to circumvent the more stringent technical requirements for processes which only involve data erasure.

In contrast to aggregation, de-identification involves modification of the individual data record pertaining to a customer, and might therefore be used in place of, rather than in addition to, erasure. To comply with the CCPA's definition of de-identified data, the data entries corresponding to a particular customer must be purged of any information which could "reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer." Finding and removing that information requires a systematized process for information discovery and erasure very similar to the one required for deletion. But, since the text does not specify that the removal of identifying information must be permanent and complete, akin to data erasure, the erasure of this identifying information could be achieved with soft deletion (or even through other processes with less stringent guarantees). If, due to this lowered standard, businesses find it technically easy to implement compliant de-identification than deletion, this might become the solution of choice for businesses looking to achieve CCPA compliance in their responses to deletion requests.

The possibility that de-identification will become the standard remedy for deletion requests is potentially troublesome because de-identification can be less privacy-protective and secure than full erasure. A host of high-profile examples⁵ of successful re-identification of sensitive information have shown that de-identification is extremely challenging to implement successfully. Assumptions about what information can be safely included in a de-identified dataset are often proven disastrously wrong, and will continue to change as we develop increasingly powerful machine learning models for extracting patterns from data. For these reasons, the release, whether deliberate or as part of a breach or theft, of de-identified data can pose a security and privacy risk to a consumer. These risks are not present when data has been properly erased (and are seriously reduced even when data has been soft deleted, due to the significantly higher burden imposed on an attacker who must access the physical storage system). And, even outside of the specific risks posed by re-identification, there might be a host of reasons a consumer submitting a

⁵ For an overview of several high-profile re-identification attacks: Lubarsky, Re-Identification of "Anonymized" Data (2017). (<https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/>)

deletion request would prefer their information be expunged entirely from a system rather than just stripped of its identifiers. The question of when and where the customer's right to deletion can be satisfied by de-identification might benefit from further clarification, since there may be contexts in which de-identification provides all of the security and privacy benefits of deletion. But, given the increased risk posed by de-identified data, it might be undesirable to make de-identification the default response to deletion requests, which is at risk of happening unless the implementation standards and appropriate use cases for each are clarified.

In short, adding specificity about the requirements of erasure in the text of the proposed regulations around the CCPA could encourage businesses to focus on the deletion properties that are most salient to customer privacy and data governance rights. It might prove useful for the regulation to differentiate between permanence and completeness requirements for application-level deletion, which might require that data be unlinked at its source and throughout its flows and transformations within the system, and storage-level deletion, where storage providers might be obliged to make available functionality for overwriting data in order to provide hard deletion guarantees.

Recommendations:

- Make erasure the default response to requests to delete, and require a legitimate reason that erasure is impractical when businesses wish to instead use deidentification to fulfil their obligation to such a request.
- In such cases, impose similar permanence and completeness requirements on de-identification. Since simple removal of identifying information is known to allow re-identification of data in many contexts, businesses should adhere to current best practices for de-identification to provide these guarantees.

- Clarify the meaning of “permanently and completely erased” by specifying that a business must make all non-exempt information about a requester permanently unretrievable throughout their data storage and processing systems.

Enshrining the answers to these questions in law will provide guidance for businesses as they implement their deletion request response systems, and help guarantee that standards for data deletion reflect the people’s judgement about the spirit and intention of the right to deletion laid out in the CCPA.

Message

From: Jaime Walsh [REDACTED]
Sent: 12/6/2019 7:17:46 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comment Regarding Proposed CCPA Regulations
Attachments: 20191206 CCPA Comment_IG US Holdings, Inc.pdf

Dear Attorney General,

Please find attached comments regarding the proposed CCPA Regulations, submitted by IG US Holdings, Inc. on behalf of its US subsidiary entities.

Best regards,
Jaime Walsh

Jaime Walsh
Legal Counsel, North America

IG Group, 200 W Jackson Blvd, Chicago, IL 60606,
[REDACTED]

www.ig.com

45 YEARS OF TRADING
INDICES | SHARES | FOREX
COMMODITIES

Forex trading involves risk. Leveraged trading in foreign currency or off-exchange products on margin carries significant risk and may not be suitable for all investors. We advise you to carefully consider whether trading is appropriate for you based on your personal circumstances. You may lose more than you invest. We recommend that you seek independent advice and ensure you fully understand the risks involved before trading. This email is intended for the addressee(s) only and may contain information that is strictly confidential. If you are not the intended recipient, do not read, copy, or distribute this email or any attachments. If you have received this email in error, please notify the sender immediately and delete the email and attachments. Opinions or conclusions unrelated to the official business of this company shall be understood as neither given nor endorsed by it. IG is a trading name of IG US LLC (a company registered in Delaware under number 6570306). Business address at 200 West Jackson Boulevard, Suite 1450, Chicago, IL 60606, USA. IG US LLC is a registered RFED and IB with the CFTC and a member of the National Futures Association (NFA ID 0509630). All email sent to or from the IG corporate email system may be retained, monitored and/or reviewed by IG personnel. The contents hereof are not an offer, or a solicitation of an offer, to buy or sell any particular financial instrument provided by IG.



December 6, 2019

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

Via email to PrivacyRegulations@doj.ca.gov

RE: IG US Holdings, Inc. Comment regarding the proposed California Consumer Privacy Act Regulations

Dear Attorney General Bercerra,

IG US Holdings, Inc. ("IG") appreciates the opportunity to comment on the proposed regulations ("Regulations") implementing the California Consumer Privacy Act ("CCPA"), as well as the California Attorney General's efforts to protect its residents from improper or unknown uses of personal information. While the Regulations do provide some clarity as to the CCPA's requirements, it also opens more questions. Additionally, guidance has not been provided with respect to several provisions of the CCPA. We request the Attorney General's office to provide further clarity either in the final regulations or informally with written guidelines.

IG US Holdings, Inc.'s North American Subsidiaries

To provide some background, IG is a United States subsidiary of IG Group Holdings PLC, a London-based global financial services firm listed on the London Stock Exchange. IG is the direct parent of North American Derivatives Exchange, Inc. ("Nadex"), a Commodity Futures Trading Commission ("CFTC") registered designated contract market and derivatives clearing organization, IG US LLC ("IGUS"), a CFTC registered retail foreign exchange dealer, and FX Publications, Inc. (d/b/a "DailyFX"), a CFTC registered Guaranteed Introducing Broker which also provides market commentary and educational resources. All three entities are highly regulated and accept retail clients from all over the United States.¹

Nadex was originally known as "HedgeStreet, Inc.", and operated from 2004-2007 in San Mateo, California, before closing its doors in late 2007. HedgeStreet was acquired by IG Group in 2008 and relaunched as "Nadex" in 2009. Nadex is a derivatives exchange, not a brokerage. Accordingly, Nadex does not enter transactions opposite its clients, rather all traders transact against other exchange

¹ Nadex also accepts clients from a number of international countries. IG US LLC does not currently accept clients from Arizona or Ohio.

members and market participants. Clients apply on the Nadex website to become “members” of the exchange, where they will enjoy the security of trading fully collateralized derivative contracts based on underlying commodity, indices, and currency markets on a secure and regulated trading platform. All applicants are subject to an identification verification and background check. CFTC regulations require Nadex to maintain all account and trade data for a period of five years following closure of the member’s account.

IGUS is a new entity and opened for business in January 2019. IGUS offers forex trading on a margined and over-the-counter basis. Clients apply on the IGUS website and are subject to identification verification and background check. IGUS is required to maintain account information and trade data for a period of five years following closure of the client’s account.

Daily FX was previously a news outlet owned by FXCM and was later acquired by IG in 2016. Daily FX received its introducing broker registration in November 2018. Daily FX remains primarily a news and educational website, but also introduces prospective clients to IGUS, its guaranteed broker.

In order to open a live trading account with Nadex or IGUS, the entities collect personal identification information such as name, address, date of birth, social security number, phone, and email in order to verify the applicant. In all instances clients are informed of the identification verification and background checks, and are presented with the entities’ Privacy Policies which indicate information will be shared with affiliates and other entities that provide valuable services to the business. Nadex and IGUS also offer a demo account, which collects name, phone number, country and email address. A demo account owner does not provide their state of residence. Daily FX collects name, phone number, country and email address in exchange for educational material. The user’s state of residence is not provided. Nadex operates out of Chicago, Illinois and IGUS operates out of Chicago, Illinois, and London, England. Daily FX operates from New York, New York.

Proposed Regulations Implementing the California Consumer Privacy Act

Our concerns regarding the Regulations primarily arise from those sections which conflict with the internal policies and procedures of Nadex and IGUS, which are in place due to the highly regulated nature of these industries. For example, section 999.308(b)(5) requires a business’s Privacy Policy to include instructions on how a consumer can designate an authorized agent to make requests on behalf of the consumer.² Section 999.315(g) permits a consumer to use an authorized agent to submit a request to opt-out on the consumer’s behalf.³ Section 999.326(b) indicates that an authorized agent is not required to provide written authorization or identification if granted power of attorney.⁴ Neither Nadex nor IGUS permit anyone other than the account owner to make any kind of request with regard to the personal information associated with the account. Furthermore, Nadex does not permit its members to utilize powers of attorney in any event. These policies are in place to protect the sensitive and private information of the account holder. While the Regulations would require the business to acquire sufficient verification from the requestor before complying with any request, Nadex and IGUS take this a step

² Cal. Code. Regs. tit. 11 §999.308 (2019) (proposed).

³ Cal. Code. Regs. tit. 11 §999.315 (2019) (proposed).

⁴ Cal. Code. Regs. tit. 11 §999.326 (2019) (proposed).

further to provide enhanced security to its clients and to comply with their regulatory obligations. The Regulations appear to give consumers a right which they do not have when choosing to engage in online trading with Nadex and IGUS. As our policies provide additional protection beyond those of which the Regulations and CCPA provide, and because deviation from these policies could negatively impact our federal regulatory requirements, we would like confirmation that the current practice of communicating only with account owners will not be deemed in violation of the Regulations or the CCPA.

Section 999.305(a)(3) of the Regulations states that “[a] business shall not use a consumer’s personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer’s personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.”⁵ We object to the requirement that the business obtain “explicit” consent and suggest passive consent, which is widely used in the United States, with an opportunity to opt-out is sufficient. Requiring explicit consent has great potential to overburden the business in terms of monitoring and tracking all consents and managing those accounts for which consent was not received. Alternatively, explicit consent should be waived for those purposes which would constitute a “business purpose” as defined by the CCPA.⁶

Section 999.308 of the Regulations sets forth information that must be included in a business’s Privacy Policy.⁷ We note that as public notices are required to include more and more information, the longer notice has less significance to the user. The longer the Privacy Policy, the less likely an individual will actually read the policy in its entirety, hindering the very intent of the legislation.

⁵ Cal. Code. Regs. tit. 11 §999.305 (2019) (proposed).

⁶ *The California Consumer Privacy Act of 2018*. Cal. Civ. Code §1798.140(d). “Business purpose” means the use of personal information for the business’ or a service provider’s operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are: (1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards. (2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity. (3) Debugging to identify and repair errors that impair existing intended functionality. (4) Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer’s experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction. (5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider. (6) Undertaking internal research for technological development and demonstration. (7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

⁷ Cal. Code. Regs. tit. 11 §999.308 (2019) (proposed).

Questions Remaining Regarding the California Consumer Privacy Act

With respect to unanswered questions arising from the CCPA itself, we request clarification as to the qualifications which would subject a business to the requirements of the CCPA.

Firstly, section 1798.140(c) requires a business to do business in the State of California, yet little guidance is provided as to what constitutes doing business in California.⁸ Nadex, IGUS, and Daily FX are all online businesses in the financial industry, and accordingly have clients from all over the United States. As previously stated, Nadex operates in Chicago, IGUS operates in Chicago and London, and Daily FX operates in New York. The servers which enable trading to occur on Nadex and IGUS are located in Illinois and the United Kingdom, respectively. No products are shipped to California, nor are services provided in California, rather all services take place online. We request the Attorney General clarify whether the mere fact that the entities have clients who reside in California without additional contacts with the state would qualify as “doing business in California”.

Nadex, IGUS, and Daily FX are all relatively new and fairly small businesses. Nadex and IGUS collect the personal information (as defined in Section 1798.140(n) of the CCPA) of California residents who open a live trading account, however, it appears they both fall below the threshold⁹ levels which would subject them to the CCPA. The first threshold would subject a business to the CCPA if it has a gross annual revenue of at least \$25 million. It is unclear whether the gross annual revenue threshold of \$25 million applies to the business’ total revenue from all of its clients regardless of their residency, or if the threshold applies to revenue generated solely from California residents. It seems more reasonable that the threshold should only apply to revenue generated from California residents, namely because the revenue the business generates from non-California residents has no connection to the privacy or personal information collected from California residents. Additionally, the threshold levels under subsections (B) and (C) of 1798.140(c)(1) reference the personal information of “consumers” which the CCPA defines as “a natural person who is a California resident”¹⁰. As (B) and (C) directly tie the threshold levels to California residents, it is most sensible that the \$25 million threshold identified in subsection (A) would relate to California residents only as well, making all three thresholds directly applicable to very individuals the CCPA seeks to protect. We therefore request clarification as to from which clients the \$25 million was intended to generate.

⁸ Cal. Civ. Code §1798.140(c).

⁹ *Ibid.* “Business” means: (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers’ personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information, that does business in the State of California, and that satisfies one or more of the following thresholds: (A) Has annual gross revenues in excess of twenty-five million dollars (\$25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185. (B) Alone or in combination, annually buys, receives for the business’ commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices. (C) Derives 50 percent or more of its annual revenues from selling consumers’ personal information.

¹⁰ Cal. Civ. Code §1798.140(g).

Also with respect to the first threshold level, we request guidance as to when a business must become compliant with the CCPA after achieving \$25 million in revenue. It is presumed revenue would be based on the most recent tax year. We would like confirmation that for purposes of meeting the threshold, the revenue would be based on the most recent fiscal tax year (for example, June 1, 2019 - May 31, 2020), and that the business will have a period of time following the final fiscal year revenue calculation to come into compliance with the CCPA, as compliance the day after (or the day of) learning of the final revenue number is unreasonable and unrealistic.

The second threshold level under subsection (B) of 1798.140(c)(1) would subject a business to the CCPA if it “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.” We object to the inclusion of devices in this threshold level. The language appears to require a business to multiply records of personal information each time a user logs into his account from a new device, despite that no new personal information is provided by the user. For example, if a client logs into his account from his personal computer, then later from his phone and still later from his tablet, the CCPA would consider each a separate record despite that the client is logging into the same trading account containing his same personal information and trade data. This requirement does not benefit the client as no additional personal information is collected from the client, and the only information gained is that the client logged in from three devices on the particular day. This does not necessarily even indicate to the business that the client owns three devices, as there are numerous opportunities to use public terminals or devices belonging to friends or family. Moreover, the requirement would be burdensome to businesses who would need to tally devices within an account requiring significant development work in order to produce more granular reporting.

Another problem arises with respect to the second threshold because the definition of personal information includes internet protocol addresses and geolocation data¹¹. As you will be aware, Google Analytics and Adobe Analytics are web analytics tools that enable businesses to analyze website traffic, which is essential for effective marketing and business strategy planning. These analytics tools collect bits of information about website visitors and provide customized reports to provide information such as which geographical location visits the website most. One such data point collected is the visitor’s IP address. Individuals visiting a business website that uses analytics tools will have certain data points collected, despite that they are not necessarily current consumers, and may never become consumers, but are rather merely passive visitors to a website. The number of visitors to a website from a particular state can easily exceed 50,000 in a matter of days or weeks. Because an IP address is associated with a particular device, it appears such a use would fall under this subsection (B) and subject nearly any business using these analytics tools, of which there are millions, to the CCPA (assuming the business also has California consumer clients). It is unlikely this was the Attorney General’s intent. Additionally, while an IP address is associated with a particular device, without further information it is highly unlikely the IP address could be used to positively identify a California resident. Many IP addresses are dynamic, but there is no way for a business to differentiate between a static and a dynamic IP address. Moreover, an IP address may be associated with a device in a public location, such as a library or coffee house, and accessible to many users. Likewise, an IP address associated with a device in a household shared by

¹¹ Cal. Civ. Code §1798.140(o)(1)(A) and (G).

multiple individuals could not identify one particular individual. We ask the Attorney General to clarify whether the threshold level of 50,000 annually was meant to include visitors to a website. We also request the Attorney General to declare that an IP address (or other similar identifier) alone without other identifying information could not reasonably be used to identify an individual, and thus is considered “deidentified”, as defined in section 1798.140(h), and not to be factored into the 50,000 threshold.¹²

For certain services, Nadex, IGUS, and Daily FX all collect only limited information including name, phone number and email. As these records are not associated with a state of residence, the businesses are unaware of how many – if any - records belong to California consumers. Accordingly, at present these records cannot be taken into account when determining whether the businesses receive 50,000 consumer records or more annually. The three businesses would like to collect the least amount of personal information necessary in order to provide the services a client desires, indeed a practice encouraged by the Regulations in section 999.323(c), and therefore we do not plan to request state of residence in instances where the services can be provided sufficiently and securely without. Adding another data point for the sole purpose of determining which individuals reside in California unnecessarily subjects these individuals to further collection of personal information, in opposition to the government’s efforts to restrict collection of unnecessary personal information. We request guidance as to how we should proceed with these records of unknown origin in order to comply with the CCPA without subjecting our clients to additional data collection.

The third threshold level under Section 1798.140(c)(1) would subject a business derives 50 percent or more of its annual revenues from selling consumers’ personal information to the CCPA. Section 1798.140(t)(1) defines “sell” as “selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.”¹³ This definition is overly broad as a business would most certainly receive valuable consideration for virtually any purpose for which it may share personal information. Valuable consideration could be assurance that an individual is who they purport to be after the business shares personal information with a third-party verification service to perform an identification and background check. Or the business may gain confidence that the individual has sufficient funds in their bank account to pay for their transactions after running a debit card check with a service linked to the individual’s bank account. Without verification of the identity of its clients, or the assurance that clients have sufficient funds to pay for their transactions, neither Nadex nor IGUS would be able to provide services to the individuals at all. Because sharing personal information of its clients with verification services would fall under the definition of “sell”, and Nadex and IGUS could not operate their businesses, and hence generate revenue, without such verification, technically 100% of its revenue could be said to have resulted

¹² Cal. Civ. Code §1798.140(h). “Deidentified” means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information: (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain. (2) Has implemented business processes that specifically prohibit reidentification of the information. (3) Has implemented business processes to prevent inadvertent release of deidentified information. (4) Makes no attempt to reidentify the information.

¹³ Cal. Civ. Code §1798.140(t).

indirectly from “selling” their clients’ personal information. Because of the snowball effect and vagueness of the term “valuable consideration”, we request that the definition of “sell” be limited to only monetary consideration and that the “50 percent of revenue” required of the threshold be derived *directly* from the sale of personal information.

Related to the second and third thresholds, section 1798.140(t)(2)(C) of the CCPA states that a business does not sell personal information if “[t]he business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purposes if both of the following conditions are met: services that the service provider performs on the business’ behalf, provided that the service provider also does not sell the personal information. (i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135. (ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.”¹⁴ As written, this provision appears to actually have three requirements, rather than two as indicated by the first sentence. First, the service provider must provide the services on the business’ behalf. Second, the service provider must not sell the personal information. Third, the business must provide notice that the information is being used or shared in its terms and conditions. Subsection (ii) contradicts the first sentence of the section, which requires the service provider not sell the personal information, whereas (ii) prohibits the service provider from further “collect[ing], sell[ing], or us[ing] the personal information of the consumer *except as necessary to perform the business purpose*.”¹⁵ Thus, it appears (ii) provides some latitude with respect to whom the service provider may share the personal information with so long it is to perform the business purpose on behalf of the business. Under the Regulations, section 999.314(b) states that (b) “[t]o 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),¹⁶ that person or entity shall be deemed a service provider for purposes of the CCPA and these regulations.”¹⁷ According to this section, Google and Adobe Analytics would be considered service providers for the purpose of the CCPA, and the sharing of personal information (IP addresses and geolocation data) would not be considered a sale of personal information under 1798.140(t)(2)(C). Therefore, those data points would be excluded from the second threshold level identification of 50,000 annual consumer records. We request confirmation that this interpretation is correct.

¹⁴ *Ibid.*

¹⁵ *Ibid.* (emphasis added).

¹⁶ Cal. Civ. Code §1798.140(v). “Service provider” means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

¹⁷ Cal. Code. Regs. tit. 11 §999.314 (2019) (proposed).

Section 1798.140(d) of the CCPA defines "Business purpose" and sets out seven instances in which collecting and sharing of personal information would be considered a business purpose.¹⁸ As written, it appears the list is exhaustive and no other activities would be considered a business purpose under the definition. It is suggested that the seven instances be reclassified as mere examples, as the Attorney General is not aware of all the legitimate purposes for which a business may require personal information. Additionally, the seven purposes do not account for additional uses in the future as the result of advancing technology.

Finally, we suggest that the compliance date be amended from the earlier of July 1, 2020 or 6 months following adoption of the final regulations, to the *later* of July 1, 2020 or 6 months following adoption of the final regulations. This would enable businesses to amend their policies and procedures to comply with the CCPA requirements with the benefit of final Regulations and guidance from the Attorney General.

Thank you for consideration of these remarks, and please do not hesitate to contact us should you have any questions in this regard.

Sincerely,



Jaime Walsh
Legal Counsel

¹⁸ Cal. Civ. Code §1798.140(d). "Business purpose" means the use of personal information for the business' or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are: (1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards. (2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity. (3) Debugging to identify and repair errors that impair existing intended functionality. (4) Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction. (5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider. (6) Undertaking internal research for technological development and demonstration. (7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

Message

From: Tatsuki Tomita [REDACTED]
Sent: 12/6/2019 4:37:10 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comment to CCPA

Dear Attorney General,

I appreciate the work being done so far in drafting the California Consumer Protection Act. Privacy is a basic human right yet it has been left unregulated for too long. But it is time to fix many of the societal problems we are seeing today as a result of this inaction.

Since I represent a company that develops a web browser software for millions of users worldwide, including some in the state of California, my comment is focused on online privacy.

Although CCPA is certainly an important step forward in the direction of protecting consumer privacy, we believe that there are several fundamental areas that need to be changed.

As we all know, managing one's privacy online has become very difficult for most consumers; user profiling and the data being collected from numerous data points about our online behavior is alarming.

In addition, the sophisticated mechanisms of online advertising and the real-time bidding system for behaviorally targeted advertisements are beyond most people's comprehension.

We have seen numerous societal impacts caused by online manipulation including teen depression, disinformation, political and electoral interference to name a few.

CCPA requires businesses to disclose personal information collected and further provides an option for consumers to opt-out of the sale of their data.

However, this approach is impractical and does not accomplish the objectives of the regulation.

Consumers visit many websites on a regular and non-regular basis. Asking each one of them to opt-out from every single website requires too much effort and puts the burden on the consumer. It is an impossible task.

Businesses should not be allowed to sell personal information to third parties in the first place. In addition, companies should be prohibited from using personal information for targeted advertising. Personal information should *only* be used to provide the service consumers signed up for.

Putting these provisions in place would make CCPA a real robust privacy regulation. Today, the state of California has a great opportunity to set the course for others to follow.

Thank you.

Tatsuki Tomita
Palo Alto
Vivaldi Technologies

Message

From: Noordyke, Mitchell S. [REDACTED]
Sent: 12/7/2019 12:27:49 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comment to the Proposed Regulations for the California Consumer Privacy Act
Attachments: FaegreBD_CCPA_Comment to California Attorney General_2019-12-06.pdf

Dear Colleague,

Please find attached a letter from Faegre Baker Daniels LLP offered as formal comment to the Attorney General's proposed regulations for the California Consumer Privacy Act.

Thank you,

Mitchell S. Noordyke, CIPP/US/E, CIPM
Associate

 [Download vCard](#)

Faegre Baker Daniels LLP

2200 Wells Fargo Center | 90 South Seventh Street | Minneapolis, MN 55402-3901, USA

Brian B. Schnell
Partner

Faegre Baker Daniels LLP
2200 Wells Fargo Center • 90 South Seventh Street
Minneapolis • Minnesota 55402-3901

December 6, 2019

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

Re: Comment Seeking Clarification of \$25 Million Threshold for Franchise Relationships

Attorney General Becerra:

Faegre Baker Daniels LLP is a full-service law firm handling complex transactions, litigation and regulatory work for businesses that range from multinational companies to emerging startups. Our franchise practice helps market-leading franchisors launch, grow, protect and evolve successful systems across multiple industries. Our privacy and cybersecurity practice helps clients build strong, adaptive privacy and cybersecurity operations in an increasingly regulated and high-stakes field. We submit this comment as experienced practitioners in franchise and privacy law who have concerns that the California Consumer Privacy Act (“CCPA”) lacks clarity regarding when it applies to franchisors and franchisees.

Franchising is a regulated industry in California under the California Franchise Investment Law, Cal. Corp. Code § 31000, *et seq.*, and the California Franchise Relations Act, Cal. Bus. & Prof. Code § 20000, *et seq.* California recognizes that franchising is a thriving business model based on a franchise agreement between the franchisor and franchisee. *Patterson v. Domino's Pizza, LLC*, 60 Cal. 4th 474 (2014). In *Patterson*, the California Supreme Court explained that franchising is where “the franchisor sells the right to use its trademark and comprehensive business plan,” while the franchisee “independently owns, runs, and staffs the retail outlet that sells goods [and/or services] under the franchisor's name.” *Id.* at 477. “In the typical arrangement, the franchisee decides who will work as his employees, and controls day-to-day operations in his store.” *Id.* at 490 (internal citations omitted). Thus, while the franchisor often “imposes comprehensive and meticulous standards for marketing its trademarked brand and operating its franchises in a uniform way,” the “franchisee retains autonomy as a manager and employer.” *Id.* at 478. It is the franchisee who implements the operational standards on a day-to-day basis, hires and fires store employees, and regulates workplace behavior. *Id.* It is common in franchise relationships that the franchisee pays a monthly license or royalty fee to the franchisor for the rights granted under franchise agreement, but the two do not share profits or losses. *See id.* at 481.

We are submitting this public comment to highlight that the CCPA lacks clarity as it applies to franchisors and franchisees. Specifically, Cal. Civ. Code § 1798.140(c)(1)(A) provides that the CCPA applies when, among other things, an entity “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.” This \$25 million “threshold” raises several unanswered questions for franchisors, including:

- Does a franchisor count all of its royalty revenue toward the \$25 million threshold or only royalty revenue it receives from California franchisees?
- If a franchisee owns locations inside and outside of California, does a franchisor count all the royalty revenue it receives from that franchisee or only royalty revenue it receives from that franchisee’s California locations?
- If a franchisor’s affiliate has corporate-owned locations (i.e., locations owned and operated by the franchisor’s affiliate), does the revenue of those corporate-owned locations count toward whether the franchisor itself meets the \$25 million threshold?

In addition, we are concerned that Cal. Civ. Code § 1798.140(c)(2) lacks sufficient clarity for the franchise industry because it defines a covered business to also include “any entity that controls or is controlled by a business as defined in paragraph (1) and that shares common branding with the business.” As you know, “control” or “controlled” is defined to include, among other things, “the power to exercise a controlling influence over the management of a company.” This definition could be read to suggest that a franchisee outside of California, even a franchisee with single location on the east coast, potentially has CCPA compliance obligations, provided its franchisor is a business as defined in paragraph (1) and the state of California claims its franchisor has the power to exercise a controlling influence of the management of the out-of-state franchisee. We doubt the California legislature intended such a result.

While the franchise relationship involves a marketing plan or system prescribed by the franchisor, Cal. Corp. Code § 31005(a)(1), the franchisor typically does not have the power to exercise a controlling influence over the management of a franchisee. We suggest that the rulemaking process clarify that a franchisor does not have “the power to exercise a controlling influence over the management of a company” merely for prescribing a marketing plan or system pursuant to Cal. Corp. Code § 31005(a)(1) and as summarized in *Patterson v. Domino’s Pizza, LLC*, 60 Cal. 4th 474, 477 (2014).

Thank you for your consideration of this comment.

Very truly yours,

Brian B. Schnell
Partner

Message

From: Carlos Enriquez [REDACTED]
Sent: 12/7/2019 12:45:47 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Commentary on the proposed CCPA Rule

Farmers Insurance Federal Credit Union is a federally chartered institution regulated by the National Credit Union Administration, maintaining very healthy financials as represented by our high capital ratios and a net worth of approximately 12%, growing membership of approximately 52,000 members primarily serving the Farmers Insurance Group with a heavy concentration of members in California.

While there are myriad of concerns regarding the CCPA, I would like to address a primary apprehension in overlapping of rules, regulations and laws especially in the confusion regarding the exemption for personal information as addressed in the Gramm-Leach-Bliley Act (GLBA) along with the California Financial Information Privacy Act (CFIPA). CCPA references "personal information" as defined in Calif. Civil Code 1798.145(o). The GLBA and CFIPA both use the terms "nonpublic personal information" and define that term to mean "personally identifiable financial information." The CFIPA definitions aligns with the Gramm Leach Bliley Act, as such maintains consistency. The challenge is with the CCPA's broad definition of "personal information" which appears to overreach that of other laws' use of "nonpublic personal information." The GLBA pertains to "personally identifiable financial information" collected in the course of a transaction or providing a financial product or service, etc. The CCPA pertains to personal information collected in basically **"any manner"**, including when there is no transaction. For example: As a financial institution we deposit/post, checks as a negotiable instruments for our members, under CCPA it "could" appear that the we have now received "personal information" on that maker, yet we would note that we would not have what we currently define as "nonpublic private information". The exemption is unclear and can be interpreted in different ways.

I do see the value in the instance where an institution sells nonpublic personal information requiring additional regulation. It is my opinion that current regulations, primarily under GLBA and CFIPA, meet the requirements of protecting consumer privacy while we and fellow financial institutions service our members banking needs. As such would recommend that financial institutions who do not share nonpublic information be exempted from applications of CCPA.

Thank you for your time and attention,

Carlos Enriquez, Jr.
Compliance Officer



Thank you for being a member of our Credit Union family.

Message

From: Tony Ficarrotta [REDACTED]
Sent: 12/6/2019 9:41:00 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Leigh Freund [REDACTED] David LeDuc [REDACTED]
Subject: Comments from the Network Advertising Initiative (NAI)
Attachments: NAI Comment Letter - Proposed CCPA Regulations (Dec. 6, 2019) .pdf

Thank you for the opportunity to submit comments regarding the Office of the Attorney General's request for comments regarding proposed regulations for the California Consumer Privacy Protection Act of 2018 (CCPA). Please find attached comments from the NAI. Please feel free to reach out with questions or to discuss these comments in greater detail.

Thank you,

Tony Ficarrotta
Counsel, Compliance & Policy
Network Advertising Initiative
[REDACTED]



Network Advertising Initiative
409 7th Street NW, Suite 250
Washington, DC 20004

December 6, 2019

VIA ELECTRONIC MAIL: PrivacyRegulations@doj.ca.gov

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

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

Dear Mr. Becerra:

The Network Advertising Initiative (“NAI”) is pleased to submit these comments regarding the regulations proposed for adoption¹ under the California Consumer Privacy Act of 2018 (the “CCPA”).²

The NAI applauds the efforts the Office of the Attorney General has undertaken to interpret and implement the complex requirements of the CCPA while considering detailed comments from dozens of organizations and individuals in the first phase of this rulemaking process.

The NAI’s aim in providing these comments on the proposed regulations (the “Regulations”) is twofold. First, to identify parts of the Regulations that could be amended to further explain or clarify the proposed requirements. Such amendments would benefit consumers and businesses by promoting compliance with the Regulations. Second, to identify provisions in the Regulations that may conflict with the purpose or intent of the CCPA, and suggest amendments that would bring the Regulations into closer alignment with the CCPA and therefore further the CCPA’s purposes.

¹ CAL. CODE REGS. tit. 11, §§ 999.300-341 (proposed Oct. 11, 2019).

² CAL. CIV. CODE §§ 1798.100 *et seq.*

Overview of the NAI

Founded in 2000, the NAI is the leading self-regulatory organization representing third-party digital advertising companies. As a non-profit organization, the NAI promotes the health of the online ecosystem by maintaining and enforcing strong privacy standards for the collection and use of data for digital advertising in multiple media, including web, mobile, and TV.

All NAI members are required to adhere to the NAI's FIPPs-based,³ privacy-protective Code of Conduct (the "NAI Code"), which has undergone a major revision for 2020 to keep pace with changing business practices and consumer expectations of privacy.⁴ Member compliance with the NAI Code is promoted by a strong accountability program, which includes a comprehensive annual review by the NAI staff of each member company's adherence to the NAI Code, and penalties for material violations, including potential referral to the FTC. Annual reviews cover member companies' business models, privacy policies and practices, and consumer-choice mechanisms.

Several key features of the NAI Code align closely with the underlying goals and principles of the CCPA. For example, the NAI Code requires members to provide consumers with an easy-to-use mechanism to opt out of different kinds of Tailored Advertising,⁵ and requires members to disclose to consumers the kinds of information they collect for Tailored Advertising, and how such information is used.⁶ The NAI Code's privacy protections also go further than the CCPA in some respects. For example, the NAI Code includes outright prohibitions against the secondary use of information collected for Tailored Advertising for certain eligibility purposes, such as credit or insurance eligibility, regardless of whether such information is ever sold, and even when a consumer has not opted out of Tailored Advertising.⁷

The NAI also educates consumers and empowers them to make meaningful choices about their experience with digital advertising through an easy-to-use, industry-wide opt-out mechanism.⁸

³ See, e.g., FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf>.

⁴ See NETWORK ADVERTISING INITIATIVE, 2020 NAI CODE OF CONDUCT (2020) [hereinafter NAI CODE OF CONDUCT], https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf.

⁵ See, e.g., *id.* § II.C.1.a. The NAI Code of Conduct defines Tailored Advertising as "the use of previously collected data about an individual, browser, or device to tailor advertising across unaffiliated web domains or applications, or on devices, based on attributes, preferences, interests, or intent linked to or inferred about, that user, browser, or device. Tailored Advertising includes Interest-Based Advertising, Cross-App Advertising, Audience-Matched Advertising, Viewed Content Advertising, and Retargeting. Tailored Advertising does not include Ad Delivery and Reporting, including frequency capping or sequencing of advertising creatives." *Id.* § I.Q. Capitalized terms used but not defined herein have the meanings assigned to them by the NAI Code of Conduct. See generally *id.* § I.

⁶ See *id.* § II.B.

⁷ See *id.* § II.D.2.

⁸ For more information on how to opt out of Tailored Advertising, please visit <http://optout.networkadvertising.org>.

Part I: Definitions**A. The Regulations should be amended to add a definition for the term “webform.”**

The Regulations use the term “webform” in several places in connection with the submission of consumer requests through a business’s website or mobile application.⁹ In common usage, the term “webform” may be used to denote an online mechanism through which a user may submit information like a name, email address, phone number, and/or demographic information over the Internet.¹⁰ However, because the Regulations contemplate consumers making requests to businesses that may involve only personal information that is not associated with a named actual person,¹¹ such as a cookie ID, mobile advertising ID, or IP address that the consumer does not know or have easy access to, the common usage of the term “webform” is too limited to allow for consumers to make effective requests in connection with those pseudonymous identifiers.

To avoid confusion and ensure that businesses provide consumers with request mechanisms that are appropriate for the kind of personal information involved in a consumer request, the Regulations should be amended to add a definition for “webform” that allows for flexible and sensible implementations by businesses.

Recommended Amendments to Proposed Regulatory Language:***Section 999.304(w):***

“Webform” means any reasonable and easily accessible method made available by a business to consumers for the submission of consumer requests through the business’s website, mobile application, or other internet-connected device. This may include, but is not limited to, interactive buttons, links, tick-boxes, fields for entering personal information, or other reasonable methods that a consumer may use to submit a request to a business.

B. The proposed definition of “categories of third parties” should be amended to clarify that the enumerated categories of companies may be third parties under the Regulations in some contexts, but not others.

As noted in the Initial Statement of Reasons (“ISOR”) accompanying the Regulations, the CCPA requires businesses to disclose to consumers the “categories of third parties with whom the

⁹ See CAL. CODE REGS. tit. 11, §§ 999.306(c)(2); 999.312(a); 999.312(c)(2); 999.315(a) (proposed Oct. 11, 2019).

¹⁰ See, e.g., *Form (HTML)*, WIKIPEDIA, [https://en.wikipedia.org/wiki/Form_\(HTML\)](https://en.wikipedia.org/wiki/Form_(HTML)). (last visited Dec. 5, 2019).

¹¹ See CAL. CODE REGS. tit. 11, § 999.325(e)(2) (proposed Oct. 11, 2019).

business shares personal information,” but does not define the term “categories of third parties.”¹²

The ISOR also highlights the fact that the proposed definition of “categories of third parties” was drawn from a code of conduct for mobile apps developed in 2013 through the National Telecommunications and Information Administration in the U.S. Department of Commerce.¹³ For the mobile app context, the enumerated list of categories of third parties in the proposed definition is illustrative of the kinds of companies that may be third parties where the app itself is the first party.¹⁴

For example, the user of a mobile app might not understand that the mobile operating system running the app may also collect information about how the user interacts with the app. In that context, because the intent of the user may be to interact directly only with the mobile app, and not with the mobile operating system, it is appropriate to classify the mobile app as a first party and the mobile operating system as a third party. However, as soon as that user exits the mobile app and begins to interact directly with the operating system by scrolling or swiping through other apps the user has installed, the mobile operating system is no longer a third party. Instead, the same mobile app the user has just closed could become a third party if the app continues to collect information about the user’s activity on the mobile device after it has been closed, while the operating system is the first party.

The way users interact with the websites, mobile apps, and other internet-connected services and devices generally involves context shifts similar to the kind described above, so the Regulations should further clarify that the kinds of businesses that should be included as a “category of third party” may change depending on the context in which personal information is collected.

Recommended Amendments to Proposed Regulatory Language:

Section 999.301(e):

“Categories of third parties” means types of entities that do not collect personal information directly from consumers. Depending on the context in which an entity collects personal information, the types of entities that do not collect personal information directly from consumers including may include, but is not limited to

¹² CAL. DEP’T OF JUSTICE, OFFICE OF THE ATTORNEY GEN., INITIAL STATEMENT OF REASONS (ISOR), PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS 4 (2019) [hereinafter ISOR], <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf>.

¹³ *Id.*

¹⁴ See CAL. CODE REGS. tit. 11, §§ 999.301(e) (proposed Oct. 11, 2019) (enumerating advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers).

advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers.

Part II: Consumer Exercises of CCPA Rights and Business Responses

A. The provisions in the Regulations regarding methods for submitting requests to know should be amended for clarity and to harmonize with the CCPA.

The Regulations, as currently drafted, would require all businesses to provide a toll-free telephone number as one method through which consumers may make a request to know.¹⁵ However, the CCPA was amended on October 11, 2019 by Assembly Bill No. 1564.¹⁶ As amended, the CCPA does not require a business to provide a toll-free telephone number to accept certain consumer requests to know if the business: (1) operates exclusively online; and (2) has a direct relationship with a consumer from whom it collects personal information.¹⁷ Because the Regulations conflict with the CCPA on this point, the Regulations should be amended to harmonize with the CCPA.

Recommended Amendments to Proposed Regulatory Language:

Section 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, ~~this shall include, at a minimum,~~ an interactive webform accessible through the business's website or mobile application. ~~If the business does not operate exclusively online, or does not have a direct relationship with a consumer from whom it collects personal information, this shall include, at a minimum, a toll-free telephone number.~~ 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.

B. Certain requirements in the Regulations regarding business responses to consumer requests to know or delete should be amended for clarity and to harmonize with the CCPA.

1. Provisions in the Regulations regarding the timing of a business's response to a request to know or delete should be amended to harmonize with the CCPA.

¹⁵ *Id.* § 999.312(a).

¹⁶ See A.B. 1564, 2019-2020 Leg. Sess., Reg. Sess. (Ca. 2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1564.

¹⁷ CAL. CIV. CODE § 1798.130(a)(1).

The ISOR asserts that the CCPA contains two conflicting provisions regarding the maximum time allowed for businesses to respond to a consumer request to know or delete because section 1798.130(a)(2) of the CCPA allows for an extension of the initial 45-day response period by an additional 45 days, while section 1798.145(g) allows for an extension of the initial 45-day response period by an additional 90 days.¹⁸ The ISOR states that by adopting the 45-day standard from section 1798.130(a)(2) of the CCPA exclusively, the Regulations have clarified the application of conflicting requirements in the statute.¹⁹

The NAI does not agree with the characterization in the ISOR of the differing 45-day and 90-day extension provisions in the CCPA as “conflicting.” That is because the 45-day extension period from section 1798.130(a)(2) is available to businesses when “reasonably necessary,” while the availability of the 90-day extension provision in section 1798.145(g) is limited to only when “necessary.” This difference makes it clear that the longer 90-day extension is available to businesses only under a stricter standard of necessity – where the longer extension is “necessary” for a business to process the request. This is in contrast to the 45-day extension period, which is available to businesses under the more flexible standard of “reasonably necessary.”

The language in the Regulations elides this distinction because it uses the 45-day extension period from Section 1798.130(a)(2), while using the “necessary” standard for taking that extension from Section 1798.145(g) (“If **necessary**, businesses may take up to an additional **45 days** to respond to the consumer’s request.”).²⁰ This approach appears to conflict with the CCPA, which applies two different standards (“reasonably necessary” vs. “necessary”) for two different extension periods (45 days vs. 90 days). The Regulations should be amended to restore the distinction adopted by the legislature.

In addition, the Regulations should be amended to allow for the initial 45-day period to begin running at the time a business verifies a consumer request. Verifying consumer requests may involve communicating with consumers over time, and businesses cannot control how long it may take consumers to provide information necessary to verify a request.

Recommended Amendments to Proposed Regulatory Language:

Section 999.313(b):

Businesses shall respond to requests to know and requests to delete within 45 days of verifying those requests. The 45 day period will begin on the day that the business receives verifies the request, ~~regardless of time required to verify the request.~~ If reasonably necessary, businesses may take up to an additional 45 days to respond to the

¹⁸ See ISOR, *supra* note 12, at 17.

¹⁹ *Id.*

²⁰ See CAL. CODE REGS. tit. 11, §§ 999.313(b) (proposed Oct. 11, 2019).

consumer's request, for a maximum total of 90 days from the day the request is ~~received~~, verified. If strictly necessary, businesses may take up to an additional 90 days to respond to the consumer's request, for a maximum total of 135 days from the day the day the request is verified. In either case, ~~provided that~~ the business must 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.

2. The Regulations should be amended to remove provisions that would require businesses to respond to consumer requests in a way that differs from what consumers have actually requested.

The Regulations introduce the novel concept that consumer requests to know or delete made to a business that cannot adequately verify those requests should be assigned a different meaning by the business – for example, by requiring a business to re-interpret a consumer request to delete as a request to opt-out.²¹ This concept is disconnected from the requirements of the CCPA and at odds with the intent of the consumers making those requests.

The CCPA is grounded in the fundamental principles of notice and choice for consumers. It has extensive transparency and disclosure requirements for businesses and provides consumers with an array of rights that they may exercise with businesses, which are informed by business transparency. Indeed, businesses subject to the CCPA must disclose to consumers all of the rights they may exercise – including requests to know,²² requests to delete,²³ and requests to opt out of “sales” of personal information.²⁴ With that information, consumers are empowered to decide which rights to exercise – including a decision to exercise all of them, some of them, or none of them. Forcing companies to impute a different intent to consumers is unnecessary and burdensome for companies with no corresponding consumer benefit. That’s because consumers already have the benefit of being informed about and able to exercise any of the rights granted under the CCPA that they wish with businesses subject to the CCPA.

Further, forcing businesses to re-interpret consumer requests when they cannot adequately verify a consumer’s identity creates new risks for consumer harm. For example, suppose that a consumer has read and understood the privacy policy of a retail website, and understands that the retailer may collect and “sell” the consumer’s personal information in order to offer coupons or discounts on certain goods offered on the website. The consumer accepts the benefit of this bargain and decides not to opt out of “sales” of personal information by the retailer. However, that consumer might eventually find that the discounts and offers she is receiving from the retailer (which may be based on personal information previously collected through the website) are no longer relevant or interesting to her, and decides to make a

²¹ See *id.* §§ 999.313(c)(1)-(2); 999.313(d)(1).

²² See CAL. CIV. CODE § 1798.110(c).

²³ See *id.* § 1798.105(b).

²⁴ See *id.* § 1798.120(b).

request to the retailer to delete her personal information to start with a clean slate, and hopefully receive different discounts and offers based on the use and transfer of personal information collected by the retailer after the deletion request. However, if the retailer is unable to verify the consumer's request to a reasonable degree of certainty based on the limited personal information it has collected, then under the Regulations, it would have to opt the consumer out of "sale" of personal information. This would thwart the consumer's intent in this case, as she would stop receiving discounts and offers she wanted to receive when the retailer is forced to treat her request for deletion as a request to opt out of sales.²⁵

Amending the Regulations to remove the requirements for businesses to re-interpret consumer requests would help businesses operationalize their processes for honoring consumer requests without resulting in any downside for consumers, who will still be able to make any request they are entitled to under the CCPA.

Recommended Amendments to Proposed Regulatory Language:

Section 999.313(c)(1):

For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the consumer that it cannot verify their identity. If the request is denied in whole or in part, the business shall provide or direct the consumer to its general business practices regarding the collection, maintenance, and sale of personal information set forth in its privacy policy. ~~If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (c)(2).~~

Section 999.313(d)(1):

For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified and shall instead provide or direct the consumer to its general business practices regarding the collection, maintenance, and sale of personal information set forth in its privacy policy. ~~treat the request as a request to opt out of sale.~~

²⁵ See CAL. CODE REGS. tit. 11, § 999.313(d) (proposed Oct. 11, 2019).

3. The Regulations should be amended to remove the requirement that a business provide a consumer with the specific basis for denying a request to delete.

A business that receives a consumer's request to delete may have various legally valid reasons for denying that request, in whole or in part. Those reasons may include an inability to adequately verify the identity of the consumer making the request,²⁶ or one or more of nine distinct statutory grounds for denying a request to delete, in whole or in part.²⁷ In cases where a business does deny a request to delete, the Regulations as currently drafted would require the business to inform users about "the basis for the denial, including any statutory and regulatory exception therefor."²⁸

While providing information about the basis for a denial of a request to delete would promote the consumer's interest in transparency regarding business retention of personal information subject to a request for deletion,²⁹ that interest should be weighed against the potential burden placed on businesses who may be required to provide customized, detailed responses when denying requests for deletion. Clarifying that a business may provide accurate, general information about why the business may have denied a request to delete would strike an appropriate balance between a consumer's interest in transparency and the operational burdens imposed on businesses.

Recommended Amendments to Proposed Regulatory Language:

Section 999.313(d)(6)(a):

(6) In cases where a business denies a consumer's request to delete the business shall do all of the following:

*a. Inform the consumer that it will not comply with the consumer's request and describe the **general** basis for the denial, including any statutory and regulatory exceptions **the business may have relied up when denying the request** ~~therefore~~ [.]*

- C. Certain requirements in the Regulations regarding requests to opt-out should be amended to harmonize with the statutory language established by the CCPA, to establish greater clarity, and to ensure that consumer choices are honored.**

1. The Regulations should be amended to clarify that a business may verify that an individual making a request to opt-out is a "consumer" entitled to make such a request in accordance with the CCPA.

²⁶ See *id.* § 999.313(d)(1).

²⁷ See CAL. CIV. CODE § 1798.105(d)(1)-(9).

²⁸ See CAL. CODE REGS. tit. 11, § 999.313(d)(6)(a) (proposed Oct. 11, 2019).

²⁹ See ISOR, *supra* note 12, at 20.

Although requests to opt out are treated differently from verifiable consumer requests under the CCPA³⁰ and under the Regulations,³¹ businesses should still be permitted to take reasonable steps to ensure that an individual making a request to opt out is a "consumer" under the CCPA entitled to make the request at all (i.e., that the user is a California resident).³² While some businesses will choose to extend the CCPA's requirements more broadly and, for instance, comply with an opt out request from a New York resident, businesses are not required to do so under the CCPA. The Regulations should be amended to clarify that fact.

Recommended Amendments to Proposed Regulatory Language:

Section 999.315(h):

A request to opt-out need not be a verifiable consumer request. However, a business may take reasonable steps to verify that an individual making a request to opt-out is a "consumer" entitled to make that request, as defined by Civil Code section 1798.140(g). In addition, if a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, or not within the scope of the CCPA, the business may deny the request. The business shall inform the requesting party that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent or outside the scope of the CCPA.

2. The Regulations should be amended to ensure that user-enabled privacy controls result in businesses honoring consumer choices, not choices made by technology companies seeking to determine the will of consumers.

Under the Regulations, businesses that collect personal information from consumers online would be required to treat "user-enabled privacy controls," whether in the form of a "browser plugin or privacy setting or other mechanism," as a valid request to opt out of sales if it communicates or signals the consumer's choice to opt-out of the sale of their personal information.³³ While the Regulations place appropriate emphasis on the need for controls to be "user enabled," which is a critical element for signals that purport to express a user's choice, multiple challenges remain with respect to the effective implementation of user-enabled signals that should be addressed in final regulations.

³⁰ Compare, e.g., CAL. CIV. CODE § 1798.100(c) (requiring a business to comply with a consumer request for the categories and specific pieces of information the business has collected about the consumer only upon receipt of a "verifiable consumer request") with CAL. CIV. CODE § 1798.135(a)(4) (requiring a business to honor a consumer's request to opt out of the sale of personal information without reference to a verifiable consumer request).

³¹ See CAL. CODE REGS. tit. 11, § 999.315(h) (proposed Oct. 11, 2019).

³² CAL. CIV. CODE § 1798.140(g).

³³ CAL. CODE REGS. tit. 11, § 999.315(a) (proposed Oct. 11, 2019).

The marketplace for web browsers and extensions currently includes a diverse set of browser-based controls. Some of them are user-enabled, and others operate by default. Most importantly, these various controls seek to accomplish a wide range of objectives, and they do so through different, and evolving, technological approaches. For instance, some consumers install ad-blocking browser extensions because they don't want to see any ads while browsing the web. Other consumers use browser plug-ins such as Ghostery³⁴ to gain greater insights into third-party data gathering. Meanwhile, several browser-makers have embraced technology that automatically, by default, prevents third-party technologies, such as cookies, from operating the way that websites—and users—intend and expect.

Importantly, privacy settings and signaling mechanisms for web browsers and other internet-connected devices (such as mobile devices, connected TVs, and other IoT devices) are diverse and constantly evolving, and help consumers determine how they share personal information used to customize their experiences, deliver specialized content, and deliver tailored advertising. These Regulations are being developed with the benefit of only a snapshot of what technology signals may be developed in coming years. While many are focusing their attention on the world wide web, this is only one medium consumers may use to engage with businesses, share personal data, and exercise their rights under the CCPA.

Given this reality, it is imperative that regulations to implement the CCPA achieve two key objectives: (1) ensure that user-enabled privacy controls represent a clear, informed consumer choice to opt out of “sales” under the CCPA; and (2) remain technology-neutral by prohibiting businesses from using technologies that may inhibit or conflict with signals that express consumer choices to opt out of sales under the CCPA.

First, the final regulations should further clarify that user-enabled privacy controls that businesses are required to treat as valid requests to opt out of sales of personal information must clearly and unambiguously express the meaning of the signals sent by those controls. For example, some consumers choose to install ad-blocking extensions for their web browsers, which may prevent digital ads from loading on web pages that the browser visits. The fact that such a browser extension is installed and activated does not *ipso facto* communicate a consumer's intent to opt out of sales of personal information, and businesses should not be required to treat them as such. Similarly, a “do not track” signal currently available in some web browsers was never designed for or marketed to users as a tool to for opting out of sales under the CCPA. For that reason, “do not track” signals cannot be expected to communicate to businesses a consumer's intent to opt out of sales of personal information, and businesses should not be required to treat them as such.

Second, the final regulations should include a provision that prohibits businesses from interfering with or obstructing the function of such user-enabled privacy controls. For example,

³⁴ GHOSTERY, <https://www.ghostery.com> (last visited Dec. 6, 2019).

existing user-enabled privacy controls for opting out of Interest-Based Advertising in some cases rely on the use of third-party cookies to store user-enabled opt-out choices. Similar mechanisms will be also be available for users to express a choice to opt out of sales under the CCPA. However, certain web browsers such as Safari may automatically delete third-party cookies without differentiating between cookies that store user privacy preferences and those that serve other functions, like analytics or ad customization.³⁵ Web browsers should not be permitted to interfere with a consumer's CCPA opt-out choices simply because those choices are expressed using third-party cookies.

Recommended Amendments to Proposed Regulatory Language:

Section 999.315(a)

*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 **clearly and unambiguously** 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. **A business is prohibited from interfering with or stopping the propagation of user-enabled privacy controls that so signal the consumer's choice to opt-out of the sale of their personal information.***

3. The Regulations should be amended to clarify how businesses are required to "act upon" a request to opt out.

As currently drafted, the Regulations would require a business in receipt of a request to opt out to "act upon the request as soon as feasibly possible, but no later than 15 days from the date the business receives the request."³⁶ The Regulations should be amended to clarify that acknowledging receipt of a request to opt out is sufficient to satisfy the requirement.

Recommended Amendments to Proposed Regulatory Language:

Section 999.315(e):

*Upon receiving a request to opt-out, a business shall act upon the request **by, at a minimum, acknowledging receipt of the request** as soon as feasibly possible, but not later than 15 days from the date the business receives the request.*

³⁵ See, e.g., John Wilander, *Intelligent Tracking Prevention*, WEBKIT: BLOG (June 5, 2017), <https://webkit.org/blog/7675/intelligent-tracking-prevention/>.

³⁶ CAL. CODE REGS. tit. 11, § 999.315(e) (proposed Oct. 11, 2019).

4. The Regulations should be amended to remove the requirement for businesses to notify third parties to whom they have sold personal information of a consumer's opt-out request.

As discussed in other comments above, the core principles of the CCPA are notice and choice. Under the law, consumers are entitled to detailed notice about the ways a business collects and uses personal information, which in turn allows consumers to make informed choices about, e.g., whether to opt out of that business's sale of personal information, or to request that the business delete the consumer's personal information. This set of corresponding consumer rights and business obligations is also directional – a consumer has the right to notice and choice from each covered business under the CCPA, and each covered business owes notice and choice to each California consumer. However, the CCPA clearly does not create a general right for consumers to be free from all sales of their personal information from all businesses by default, or obligate businesses to stop selling personal information in the absence of a consumer's request to opt out.

However, as currently drafted, the Regulations depart from these core CCPA principles when they require each business that receives a request to opt out to notify each third party to whom the business has sold personal information within 90 days of receiving the request to opt out.³⁷ In turn, each third party that is so notified must opt the consumer out of its sales of personal information,³⁸ even though the consumer may have never expressed an opt-out choice to those third parties. The ISOR explains that this new requirement in the Regulations is intended in part to address the concern that “consumers may not know the identity of the companies to whom businesses have sold their information in order to make an independent request.”³⁹ This is a meaningful concern – however, it is mitigated by two important factors that the ISOR does not address.

First, California's Data Broker Registration bill (AB 1202) became law on October 11, 2019.⁴⁰ The express intention of the legislature in drafting this bill included addressing the fact that “consumers are generally not aware that data brokers possess their personal information, how to exercise their right to opt out, and whether they can have their information deleted, as provided by California law,” and that “it is the intent of the Legislature to further Californians' right to privacy by giving consumers an additional tool to help control the collection and sale of their personal information by requiring data brokers to register annually with the Attorney General and provide information about how consumers may opt out of the sale of their personal information.”⁴¹ The way the bill defines “data broker” covers precisely the kind of

³⁷ *Id.* § 999.315(f).

³⁸ *Id.*

³⁹ ISOR, *supra* note 12, at 25.

⁴⁰ See A.B. 1202, 2019-2020 Leg. Sess., Reg. Sess. (Ca. 2019), http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1202.

⁴¹ *Id.*

scenario the Regulations address in section 999.315(f), *i.e.*, a third party that has obtained personal information from a business, and that may re-sell that information to others.⁴² The California legislature was aware of the issue identified in the ISOR, and determined that the appropriate way to promote consumer awareness and exercise of choice was to require “data brokers” to participate in a central registry where consumers may learn about them and subsequently exercise their right to opt out of sales when they decide to do so. Put another way, AB 1202 works in conjunction with the CCPA’s core principles of notice and choice in a way the Regulations do not, because AB 1202 gives consumers a way to know about and opt out of third-party resales of personal information, while the Regulations take that choice out of the hands of consumers, contrary to the spirit of the CCPA. Instead, the Regulations should be amended to require businesses to direct consumers to the new data broker registry (where applicable), which would appropriately address the concerns raised in the ISOR and harmonize with the intent of the legislature without requiring a new set of impractical and extra-legal requirements.

Second, the Regulations would prevent businesses from selling personal information even though a consumer has never expressed a choice to opt out of sales to those businesses. This result is antithetical to the principles of notice and choice. Further, it may upset consumer expectations if it results in an opt out of sales from a business with which the consumer is already familiar and has made an informed choice *not* to opt out of sales. Directing consumers to the new data broker registry instead will enhance transparency for consumers and provide an effective mechanism for them to learn about third parties and exercise their CCPA rights with those third parties.

In addition, it will be difficult or impossible for businesses to operationalize the requirement to look back 90 days to notify businesses they have sold personal information to and instruct them to stop selling that information.

Finally, the proposed requirement for a business to notify the consumer after notifying third parties to opt that consumer out of sales (although the consumer has made no such request) is burdensome and unnecessary. It does not provide actionable information for consumers and should be removed.

Recommended Amendments to Proposed Regulatory Language:

Section 999.315(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*~~

⁴² “Data broker” means a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.” *Id.*

~~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.~~ If a business knowingly sells a consumer's personal information to third parties who may further sell such information, the business must provide explicit notice of that fact in its privacy policy and provide a link to the internet web page created by the Attorney General pursuant to Civil Code Section 1798.99.84, and explain that consumers may navigate to that page to learn more about how to exercise their CCPA rights with those third parties.

D. The Regulations should be amended to further clarify how businesses may inform consumers about the method used to comply with requests to delete.

The Regulations, as currently drafted, would require a business to respond to a consumer after honoring their request to delete and "specify the manner in which it has deleted the personal information."⁴³ The Regulations should be amended to clarify that businesses should meet this requirement by referring to the deletion methods specified in proposed regulation 999.313(d)(2) (i.e., that the business has either permanently erased, de-identified, or aggregated the personal information), and not by providing consumers with excessive or confusing technical information about, e.g., specific de-identification or aggregation methods the business may have used.

Recommended Amendments to Proposed Regulatory Language:

Section 999.313(d)(5):

In its response to a consumer's request to delete that the business has verified and completed, the business shall indicate which deletion method it used to delete the personal information pursuant to section 999.313(d)(2). ~~specify the manner in which it has deleted the personal information.~~

E. The Regulations should be amended to further clarify how the standards for verifying consumer requests apply to businesses that maintain pseudonymous personal information.

The Regulations include detailed provisions pertaining to the verification by a business of consumer requests to know and delete, which have conveyed needed clarity about how businesses may provide (or delete) personal information to consumers who are entitled to it, while maintaining strong security measures and preventing the unauthorized disclosure of personal information.

⁴³ CAL. CODE REGS. tit. 11, § 999.313(d)(5) (proposed Oct. 11, 2019).

However, the Regulations lack sufficient clarity with respect to requirements for businesses to verify requests from consumers in cases where the business maintains only pseudonymous personal information. Therefore, the Regulations should be amended to further clarify how businesses may verify the identity of the consumer making a request, either to a “reasonable degree of certainty”⁴⁴ or a “reasonably high degree of certainty,”⁴⁵ as applicable. As currently drafted, the Regulations state that a business *may* match two data points provided by the consumer with data points maintained by a business to achieve a “reasonable degree of certainty,” and three data points to achieve a “reasonably high degree of certainty.”

Amendments to the Regulations should clarify that, in both cases, a business is not required to match a minimum number of data points to achieve the requisite degree of certainty, and further that the ability of a business to match such data points does not *per se* constitute the requisite degree of certainty. Making those amendments will provide businesses with helpful guidelines for reaching the requisite degree of certainty while clarifying that businesses remain responsible for actually achieving those standards, and may not simply rely on a prescriptive number of match points as a proxy for them. This is particularly relevant and important for businesses that do not collect and store multiple pieces of personal information about a consumer, or have a means to correlate previously collected personal information with new personal information supplied in a request. It is also relevant for businesses that only store pseudonymous personal information, and have explicit policies prohibiting the collection and use of personally identifiable information, such as names or email addresses, which may be used to directly identify an individual.

Further, the Regulations should be amended to clarify that the different “certainty” standards apply equally to businesses who maintain pseudonymous personal information about consumers, even though the “matching” process may occur through a fact-based verification procedure instead of matching data points known by the consumer and maintained by the business.

Recommended Amendments to Proposed Regulatory Language:

Section 999.325(b):

A business’s compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may, but is not required to include matching at least two data points provided by the consumer with data points maintained by the business, which the business has determined to be reliable for the purpose of verifying the consumer. Businesses that cannot verify the identity of the consumer making the request to a reasonable degree of certainty after matching two such data points may, but are not required to take further steps to verify the consumer’s

⁴⁴ *Id.* § 999.325(b).

⁴⁵ *Id.* § 999.325(c).

identity, including matching additional data points provided by the consumer, conducting a fact-based verification process, and considering the factors set forth in section 999.323(b)(3).

Section 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, but is not required to 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 that cannot verify the identity of the consumer making the request to a reasonably high degree of certainty after matching three such data points may, but are not required to take further steps to verify the consumer's identity, including matching additional data points provided by the consumer, conducting a fact-based verification process, and considering the factors set forth in section 999.323(b)(3). Businesses shall maintain all signed declarations as part of their record-keeping obligations.

Section 999.325(e)(2):

(e)

Illustrative scenarios follow:

(2)

If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the non-name identifying information. This may require the business to conduct a fact-based verification process that considers the factors set forth in section 999.323(b)(3). When conducting such a fact-based verification procedure, the business still must achieve the degree of certainty required for consumer requests set forth in sections 999.325(b)-(d), as applicable, which may, but is not required to include matching non-name identifying information provided by the consumer with non-name identifying information maintained by the business as set forth in sections 999.325(b)-(d).

Part III: Disclosure Obligations

- A. The Regulations should be amended to clarify that businesses required to provide consumers with a “notice at collection” may always provide such notice at or before the time that business collects personal information.**

Under the CCPA and the Regulations, a consumer is entitled to receive from a business that collects the consumer’s personal information notice about the categories and purposes of such collection “at or before” the point of collection.⁴⁶ This standard allows businesses to provide the required notice either before any collection of personal information, or at the same time that it collects personal information.

However, the Regulations contain one provision that appears to suggest businesses must satisfy this requirement by providing certain notice before the point of collection.⁴⁷ This provision disagrees with the standard articulated in the statute and elsewhere in the Regulations. The Regulations should be amended to harmonize all requirements for notice at collection to the “at or before” standard.

Recommended Amendments to Proposed Regulatory Language:

Section 999.305(a)(2)(e):

The notice at collection shall be designed and presented to the consumer in a way that is easy to read and understandable to an average consumer. The notice shall:

*Be visible or accessible where consumers will see it **at or before the time** any personal information is collected. For example, when a business collects consumers’ personal information online, it may conspicuously post a link to the notice on the business’s website homepage or the mobile application’s download page, or on all webpages where personal information is collected. When a business collects consumers’ personal information offline, it may, for example, include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to the web address where the notice can be found.*

- B. The requirements in the Regulations for businesses that are not required to provide a “notice at collection” should provide more flexibility to promote compliance.**

The regulations proposed to implement section 1978.115(d) of the CCPA would create detailed, prescriptive requirements that dictate how a business that does not collect personal

⁴⁶ See *id.* §§ 999.301(i), 999.305(a)(1), 999.305(a)(5); CAL. CIV. CODE § 100(b).

⁴⁷ CAL. CODE REGS. tit. 11, § 999.305(a)(2)(e) (proposed Oct. 11, 2019).

information directly from consumers must ensure those consumers receive explicit notice and an opportunity to opt out of sales by that business. For example, such a business would be required under the Regulations to contact the source of the personal information to “obtain signed attestations from the source describing how the source gave the notice at collection and including an example of the notice.”⁴⁸

The NAI Code already requires technology companies in its membership that do not interact directly with consumers to take steps to require that the publisher partners they work with, and who *do* interact directly with consumers, provide notice and choice to those consumers about the collection and use of information about them for Tailored Advertising.⁴⁹ In the NAI’s experience, this is often accomplished through contractual agreements. To harmonize with existing and proven industry practices for pass-on notice and choice requirements, the Regulations should clarify that a contractual agreement satisfies the requirement for a “written attestation.”

In addition, there is strong precedent for the use of model notices as a way to promote uniformity and quality of privacy disclosures.⁵⁰ This is valuable not only for business efficiency, but also for more consistency for consumers. The Regulations should be amended to clarify that when a business that does not collect information directly from consumers contractually requires the use of model notices, the maintenance of a model notice by that business will satisfy the requirement to keep an example of the notice.

Recommended Amendments to Proposed Regulatory Language:

Section 999.305(d)

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

(1)

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

(2)

Contact the source of the personal information to:

a.

⁴⁸ *Id.* § 999.305(d)(2)(b).

⁴⁹ See NAI CODE OF CONDUCT, *supra* note 4, at § II.B.4.

⁵⁰ See, e.g., 17 C.F.R. § 248.2 (allowing the use of model privacy forms for compliance with Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information); 17 C.F.R. § 248 (Appendix A to Subpart A of Part 248 – Forms), <https://www.govinfo.gov/content/pkg/CFR-2019-title17-vol4/pdf/CFR-2019-title17-vol4-part248-subpartA-appA.pdf>.

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

b.

Obtain signed attestations from the source, which may include contractual assurances, describing how the source gave the notice at collection and including an example of the notice, which may include model notices when such notices are the method used by the source to provide the required notice at collection. Attestations shall be retained by the business for at least two years and made available to the consumer upon request.

C. The requirement to disclose whether a business sells the personal information of minors under 16 years of age without affirmative authorization should be amended to include a knowledge condition.

The provisions in the Regulations regarding privacy policy disclosures include a requirement that a business disclose whether or not it sells the personal information of minors under 16 years of age without affirmative authorization.⁵¹ This provision should be amended to harmonize with the “actual knowledge” condition found in the CCPA’s provisions regarding the sale of the personal information of consumers under 16 years of age.⁵² Making this change would prevent businesses from being required to make such statements in their privacy policies when they do not have actual knowledge of the statement’s truth or falsity.

Recommended Amendments to Proposed Regulatory Language:

Section 999.305(b)(1)(e)(3):

State whether or not the business sells the personal information of ~~minors~~ consumers the business has actual knowledge are under 16 years of age without affirmative authorization.

D. The Regulations should be amended to remove the new requirement for businesses to post statistics regarding consumer requests.

The Regulations, as currently drafted, create a new requirement not found in the CCPA that would compel certain businesses to provide annual statistics in their privacy policies regarding the number of consumer requests received, complied with, and denied by those businesses.⁵³ Although the ISOR cites potential benefits to the Attorney General, policymakers, academics, and members of the public that could result from this novel requirement,⁵⁴ those benefits are speculative and in any case disproportionate to the burden that would be placed on businesses

⁵¹ CAL. CODE REGS. tit. 11, § 999.305(b)(1)(e)(3) (proposed Oct. 11, 2019).

⁵² See CAL. CIV. CODE § 1798.120(c).

⁵³ See CAL. CODE REGS. tit. 11, § 999.305(g) (proposed Oct. 11, 2019).

⁵⁴ See ISOR, *supra* note 12, at 28.

required to compile and provide such statistics. For that reason, the Regulations should be amended to remove this new requirement.

Recommended Amendments to Proposed Regulatory Language:

~~Section 999.305(g):~~

~~(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.~~

However, if the above disclosure requirements are not removed from the Regulations, the Regulations should still be amended to clarify that a business intending to honor requests to know, delete, or opt-out for individuals other than California “consumers” (e.g., residents of other states) may report statistics based on all requests received by the business, and need not report California “consumer” statistics separately. As a practical matter, many businesses lack the ability to differentiate between California “consumers” and residents of other states, so in many cases businesses will seek to extend the rights granted to “consumers” under the CCPA more broadly to residents of other states. This is a positive outcome for consumers in general. However, given this reality, it is not practical for many businesses to report data for California residents separately.

Recommended Amendments to Proposed Regulatory Language:

~~Section 999.305(g):~~

~~(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) If a business has received additional requests from individuals other than "consumers" as that term is defined by Civil Code section 1798.140(g), the business is not required to compile or disclose statistics for those requests separately, but may include them in compilations required by subsection (g)(1) and the disclosures required by subsection (g)(2).

Part IV: Other issues

A. The proposed requirement for consumers to provide opt-in consent for a business use of personal information in some circumstances should be removed to harmonize with the CCPA.

The CCPA, as noted elsewhere above, is fundamentally a notice and choice law. The legislature circumscribed the choice that must be provided to consumers to cover the sale by businesses of consumers' personal information, and set opting out as the standard for the choice required.⁵⁵ In general, the Regulations are consistent with those principles, but they depart from them significantly with a new opt-in consent requirement that is not based in the statute, and is inconsistent with its general structure.

As currently drafted, the Regulations would require a business to provide notice to consumers and obtain "explicit consent" if the business intends to use the consumers' personal information for any purpose other than the purposes disclosed in the notice at collection.⁵⁶ This new requirement conflicts with the general structure of the CCPA in at least two ways. First, while the legislature circumscribed the choice that must be provided to consumers to cover the **sale** by businesses of consumers' personal information, the new requirement would create a different consumer choice based on new **uses** of personal information by a business, even if that new use does not involve any other business or third party, much less a sale. Second, while the legislature set opting out as the default standard for the choice required by

⁵⁵ Except where the sale involves the personal information of consumers younger than 16 years old. See CAL. CIV. CODE § 1798.120(c).

⁵⁶ CAL. CODE REGS. tit. 11, § 999.305(a)(3) (proposed Oct. 11, 2019).

the CCPA, the new requirement would set a higher standard of “explicit consent” for certain activities that are not subject to consumer choice at all under the statute.

While the intent of the Regulations to allow consumers to rely on the information provided in the notice at collection⁵⁷ is a worthy one that the NAI fully supports, the requirements set forth in the Regulations go far afield of the CCPA. The CCPA already allows consumers to rely on the disclosures made by businesses in the notice at collection because, under the statute, a business may not use personal information for new purposes before providing consumer with a new and updated notice at collection.⁵⁸ In addition, a long-established principle under Section 5 of the FTC Act already prevents businesses from applying changes to their privacy policies retroactively, because doing so would be an unfair act or practice.⁵⁹ Consumer reliance on previous versions of a notice at collection is already strongly protected.

Further, the likely effect of the proposed “explicit consent” requirement will be to incentivize businesses to massively over-disclose the purposes for which they might at some point use personal information in order to avoid the requirement of obtaining “explicit consent” for any changes, even if they have no current intention of using personal information for those purposes. This would be a net detriment to consumers, who would otherwise have more relevant information about the purposes for which a business currently collects their personal information on which to base a choice about whether to opt out of that business’s sale of personal information.

For these reasons, the Regulations should be amended to remove the requirement for businesses to obtain explicit consent from users before using personal information for new purposes. Even without an “explicit consent” requirement, consumers would still be entitled to notice of any changes, the right to opt out of sales based on any changes, and the ability to rely on business adherence to past notices at collection for previously collected personal information.

Recommended Amendments to Proposed Regulatory Language:

Section 999.305(a)(3):

A business shall not use a consumer’s personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer’s

⁵⁷ See ISOR, *supra* note 12, at 47-48.

⁵⁸ “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.” CAL. CIV. CODE § 1798.100(b).

⁵⁹ See, e.g., *In re Gateway Learning Corp.*, FTC Docket No. C-4120 at ¶ 14 (F.T.C. 2004) (complaint) (stating that applying material changes to a privacy policy retroactively is an unfair act or practice), <https://www.ftc.gov/sites/default/files/documents/cases/2004/12/041228ltr0423047.pdf>.

personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use through an updated notice at collection ~~and obtain explicit consent from the consumer to use it for this new purpose.~~

B. The Regulations should be amended to harmonize requirements for service providers with the requirements in the CCPA.

The CCPA permits businesses to share personal information with “service providers”⁶⁰ in a way that does not constitute a sale of personal information subject a consumer’s opt-out choice.⁶¹ However, the CCPA restricts the purposes for which a business may share personal information with service providers to “business purposes.”⁶²

In order for service providers to carry out contracted-for business purposes, it is necessary in some circumstances for them to collect and disclose personal information with other entities, because doing so is integral to the business purpose the service provider was contracted to carry out for the business. The Regulations recognize this fact when they state that a service provider may combine personal information received from one or more entities to which it is a service provider to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity,⁶³ which is explicitly recognized as a business purpose under the statute.⁶⁴

However, the Regulations as currently drafted do not allow for the combination of personal information to perform the other business purposes that service providers are explicitly permitted to carry out under the statute. Further, the ISOR states without argument that combining personal information to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity is the only activity where the combination of personal information may be “reasonably necessary and proportionate to achieve the operational purposes” a service provider has collected personal information to carry out.⁶⁵ This broad pronouncement is unjustified, because what data processing activities are “reasonably necessary and proportionate to achieve an operational purpose” is a fact-specific inquiry that may vary by business purpose and by the type of business carrying out the activity.

For these reasons, the Regulations should be amended to allow personal information to be combined for any statutory business purposes, so long as the conditions for remaining a service provider are otherwise satisfied.

⁶⁰ CAL. CIV. CODE § 1798.140(v).

⁶¹ *Id.* § 1798.140(t)(2)(C).

⁶² *See id.* § 1798.140(v).

⁶³ CAL. CODE REGS. tit. 11, § 999.314(c) (proposed Oct. 11, 2019).

⁶⁴ CAL. CIV. CODE § 1798.140(d)(2).

⁶⁵ ISOR, *supra* note 12, at 22.

Recommended Amendments to Proposed Regulatory Language:*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, to the extent necessary to ~~detect data security incidents, or protect against fraudulent or illegal activity~~ carry out a business purpose as that term is defined by Civil Code section 1798.140(v), pursuant to its service provider contracts.

C. The Regulations should be amended to remove the requirement that a business disclose the value of a consumer's personal information when a financial incentive is provided.

It is challenging for any business to assign value to a single consumer's data, and data often gains value when it is aggregated. Consequently, financial incentive programs will more likely be based on a complex calculation of costs to the business and market comparisons. Any number that a business ultimately discloses will not be meaningful to consumers. Further, businesses deploy a wide range of business models that, in many cases, are proprietary. Therefore, requiring a business to disclose its methods and calculations could require disclosure of competitively-sensitive information. The Regulations should therefore be amended to clarify that a business is not required to disclose proprietary or competitively-sensitive information.

Recommended Amendments to Proposed Regulatory Language:*Section 999.307(b)(5):*

(b) A business shall include the following in its notice of financial incentive:

(5) An 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 consumer's data.

(6) Nothing in this section requires a business to include information in its notice of financial incentive that is proprietary or competitively sensitive.

D. The Regulations should be amended to allow information kept for record-keeping purposes to be used for security and anti-fraud purposes.

The Regulations, as currently drafted, prohibit businesses from using information maintained for record-keeping purposes for any other purpose.⁶⁶ Limiting the purposes for which a business may use record-keeping information is an important consumer protection. However, the Regulations should clarify that the scope of this requirement is limited to personal information a business maintains for recordkeeping purposes. In addition, personal information businesses obtain for recordkeeping purposes may also be useful for security and anti-fraud purposes. Allowing a security and anti-fraud exception to this requirement could serve a narrow and legitimate business need and pose no discernable risk of consumer harm from secondary uses of the information.

Recommended Amendments to Proposed Regulatory Language:

Personal information maintained by a business for record-keeping purposes pursuant to section 999.317 shall not be used for any other purpose, except for security and anti-fraud purposes.

Conclusion:

The NAI is grateful for the opportunity to comment on the Regulations for the CCPA. If we can provide any additional information, or otherwise assist your office as it engages in the rulemaking process, please do not hesitate to contact Leigh Freund, President & CEO [REDACTED] or David LeDuc, Vice President, Public Policy [REDACTED].

Respectfully Submitted,

The Network Advertising Initiative

BY: Leigh Freund
President & CEO

⁶⁶ CAL. CODE REGS. tit. 11, § 999.317(e) (proposed Oct. 11, 2019).

Message

From: Young, Stephanie [REDACTED]
Sent: 12/6/2019 8:13:04 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Dolqueist, Lori Anne [REDACTED]; Hon, Willis [REDACTED]
Subject: Comments of California Water Association on Proposed Regulations Concerning the California Consumer Privacy Act
Attachments: CWA Comments on Regulations re CCPA.pdf

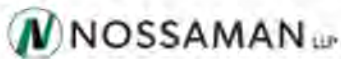
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Dear Privacy Regulations Coordinator:

On behalf of Lori Anne Dolqueist, please find attached a letter providing the Comments of California Water Association on Proposed Regulations Concerning the California Consumer Privacy Act. Please me know if you have any trouble accessing the letter. A courtesy copy is being sent today via U.S. mail.

Sincerely,
Stephanie Young
Stephanie Young
Legal Secretary
NOSSAMAN LLP
50 California Street, 34th Floor
San Francisco, CA 94111

[REDACTED]



SUBSCRIBE TO E-ALERTS
nossaman.com

PLEASE NOTE: The information in this e-mail message is confidential. It may also be attorney-client privileged and/or protected from disclosure as attorney work product. If you have received this e-mail message in error or are not the intended recipient, you may not use, copy, nor disclose to anyone this message or any information contained in it. Please notify the sender by reply e-mail and delete the message. Thank you.



ATTORNEYS AT LAW

50 California Street
34th Floor
San Francisco, CA 94111

[REDACTED]
Lori Anne Dolqueist
[REDACTED]
[REDACTED]

December 6, 2019

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
PrivacyRegulations@doj.ca.gov

**Re: Comments of California Water Association on Proposed Regulations
Concerning the California Consumer Privacy Act**

Dear Attorney General Becerra:

On behalf of California Water Association (“CWA”), we provide these comments on the proposed regulations concerning the California Consumer Privacy Act (“CCPA”). CWA is the statewide association representing the interests of water utilities subject to the jurisdiction of the California Public Utilities Commission (“CPUC”). CWA’s members provide safe, reliable, high-quality drinking water to approximately six million Californians. CWA appreciates the opportunity to comment on the proposed regulations and assist in providing greater clarity to businesses and consumers with respect to CCPA implementation.

The CCPA establishes consumer rights relating to the access to, deletion of, and sharing of personal information that is collected by businesses. The Attorney General has determined that the CCPA and the proposed regulations may have a significant adverse impact on California businesses.¹ The Notice of Proposed Rulemaking invites submissions suggesting differing compliance requirements that take into account the resources available to businesses and proposals for full or partial exemptions from the regulatory requirements for certain businesses. As discussed in more detail below, CWA recommends that the proposed regulations be modified to (1) provide greater clarity with respect to the interplay between the CCPA and obligations imposed by state agencies such as the CPUC, (2) exempt certain regulated utility-specific practices that promote efficiency and further state policies, and (3) recognize the challenges associated with deletion of historical data.

¹ California Department of Justice, Notice of Proposed Rulemaking Action, Title 11. Law, Division 1. Attorney General, October 11, 2019, p. 11.

Preservation of CPUC Regulatory Oversight

All CPUC-regulated water utilities must collect and retain-customer specific data to provide safe and reliable service, to further state policy goals regarding conservation and affordability, and to comply with CPUC requirements. CPUC-regulated water utilities may provide this information to the CPUC as part of the CPUC's regulatory oversight and may share this information with other utilities, government agencies and municipalities, or other entities, but only as directed and authorized by the CPUC. In order to safeguard customer privacy, the CPUC has established rules and requirements regarding the collection, retention, use and sharing of customer data by the utilities it regulates.

As the CPUC notes in its own comments on the proposed regulations, which CWA supports, the CPUC's oversight of the utilities it regulates must be maintained, and the obligations imposed by the CCPA cannot undermine the CPUC's ability to protect utility customers and promote State policies with respect to conservation and affordability.

Under the CCPA, the obligations imposed on businesses shall not restrict a business's ability to "Comply with federal, state, or local laws."² Furthermore, a business is not required to comply with a consumer's request to delete personal information if the information is necessary to comply with a legal obligation.³ As the CPUC explains in its comments on the proposed regulations, it utilizes a variety of methods to regulate the collection, retention, use and sharing of customer data, including decisions, general orders, resolutions, rules, tariff approvals, letters, and other communications.

CWA interprets the CCPA provisions regarding compliance with laws and legal obligations to include compliance with all CPUC requirements and directives. Therefore, to the extent that certain obligations set forth in the CCPA and proposed regulations would restrict a water utility's ability to comply with CPUC requirements and directives, the water utility would be exempt from those CCPA obligations. Similarly, if a consumer's request to delete personal information would conflict with statutory obligations or legal obligations imposed and approved by the CPUC, a water utility would not have to comply with that request.

Nonetheless, in order to ensure that CPUC-regulated entities are exempt from certain obligations if they would prevent compliance with CPUC requirements and directives, CWA suggests that the language below be incorporated into the final regulations:

§ 999.301. Definitions

"Comply with federal, state, or local laws," as set forth in Civil Code section 1798.145(a)(1) includes compliance with all

² Cal. Civ. Code §1798.145(a)(1).

³ Cal. Civ. Code §1798.105(d)(8).

requirements and directives imposed by state agencies through formal and informal regulatory activities.

A “legal obligation” as set forth in Civil Code section 1798.105(d)(8) includes compliance with all requirements and directives imposed by state agencies through formal and informal regulatory activities.

Sharing of Customer Information for a Public Purpose

The CPUC has authorized water utilities to release customer-specific information to local governments, wholesale water agencies, and other entities for the purpose of calculating local taxes, managing wastewater systems, collecting miscellaneous fees, and implementation and enforcement of conservation programs and measures. The transfer of this customer-specific information thus serves important public policy interests. The CPUC has established safeguards that ensure that the customer information that is shared is kept private and only used for the purpose for which it is intended.

Although some water utilities may collect a nominal fee related to the transfer of data to a neighboring municipality or wastewater utility, they do not “sell” data in the manner for which the CCPA was designed to provide protection. The fees collected by the water utilities simply place the financial burden and costs of accumulating and transferring the data onto the party requiring the information rather than the utility’s customers. The opt-out provisions in the CCPA and the proposed regulations should not apply to this type of data collection and sharing by water utilities since the information is not being used for commercial purposes by the water utilities, but instead to serve the public good. CWA recommends that the following language be incorporated into the final regulations to allow these beneficial practices to continue:

§ 999.301. Definitions

“Sell,” “selling,” “sale,” or “sold” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration as set forth in Civil Code section 1798.125(b) and specified in these regulations. The transfer of a consumer’s personal information by a regulated public utility to a state or local government, utility or other entity, as authorized by the California Public Utilities Commission, is not a “sale” under Civil Code section 1798.140(v), notwithstanding an exchange of monetary compensation for the consumer’s personal information.

Deletion of Historical Data

CPUC General Order 103-A established minimum standards for design, construction, location, maintenance, and operations of the facilities of water and wastewater utilities operating under the jurisdiction of the CPUC. General Order 103-A also sets forth requirements for record retention. Pursuant to General Order 103-A, certain records, which include records containing personal customer information, must be retained for at least ten years, and longer in certain circumstances.

In order to comply with General Order 103-A, water utilities are not in a position to grant customer requests under the CCPA to delete customer-specific information unless the information was no longer required to be retained by the CPUC. At this point, these records may have been moved to offsite storage or may be in difficult to manage formats, such as tape logs. The burden of locating and deleting these records would far outweigh any public benefit. CWA therefore requests that historical water utility records more than ten years old be exempt from deletion request obligations. CWA suggests the following language be incorporated into the final regulations:

§ 999.313(d)(3). Responding to Requests to Delete

If a business stores any personal information on archived or backup systems **or at an offsite storage location**, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system **or at an offsite storage location**, until the archived or backup system **or offsite storage location** is next accessed or used. **Personal information located on archived or backup systems or in an offsite storage location that is more than 10 years old at the time of the request shall be exempt from the CCPA's deletion requirement as set forth in Civil Code section 1798.105.**

Alternatively, since the proposed regulations already contemplate delaying compliance with consumer requests to delete information on archived or backup systems, CWA requests that they be modified to account for the difficulties associated with accessing historical water utility records that may contain personal information. CWA suggests the following alternative language be incorporated into the final regulations:

§ 999.313(d)(3). Responding to Requests to Delete (alternative proposed language)

If a business stores any personal information on archived or backup systems **or at an offsite storage location**, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system **or at an offsite**

storage location, until the archived or backup system or offsite storage location is next accessed or used. If a business does not access its archived or backup systems or its offsite storage location within six (6) months of a consumer's request to delete, the deletion request shall expire. Businesses shall provide notice to consumers of the possibility of expiration of requests for deletion of personal information on archived or backup systems or at an offsite storage location.

CWA recognizes the challenge of balancing consumer privacy interests against the CPUC's mandate to ensure safe, reliable and affordable utility service, and the obligation of regulated water utilities to comply with CPUC requirements and directives. CWA appreciates the opportunity to submit these comments.

Respectfully submitted,



Lori Anne Dolqueist, Nossaman LLP
Attorneys for California Water Association

Message

From: Dileep Srihari [REDACTED]
Sent: 12/6/2019 4:28:27 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Alexi Madon [REDACTED]
Subject: Comments of CompTIA on CCPA Draft Regulations
Attachments: CompTIA CCPA Regulation Comments 12-6-19.pdf

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

Please find attached the comments of CompTIA on the draft CCPA regulations.

Dileep Srihari

Before the
CALIFORNIA DEPARTMENT OF JUSTICE
Los Angeles, CA 90013

In the Matter of)	
)	
California Consumer Privacy Act)	Notice File No. Z2019-1001-05
Implementing Regulations)	

**COMMENTS OF
THE COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION**

Dileep Srihari
Vice President and Senior Policy Counsel

Alexi Madon
Vice President, State Government Affairs

COMPUTING TECHNOLOGY INDUSTRY
ASSOCIATION
515 2nd Street NE
Washington, DC 20002

December 6, 2019

TABLE OF CONTENTS

INTRODUCTION	1
I. § 999.305. Explicit Consent Cannot Be Required for Each New Business Purpose.....	2
II. § 999.306. Businesses Exempt from Opt-Out Notification Should Not Be Penalized if They Later Choose to Sell Information.....	3
III. § 999.307. Mandated Data Valuation and Methodology Disclosure is Unworkable.	4
IV. § 999.314. Service Provider Regulations Must Account for Provisions in CCPA That Explicitly Contemplate the Use of Data for Provider Operations.	5
V. § 999.315. Opt-Out Mechanisms Should Guard Against Self-Serving Browser Implementations and be Prospective Only.....	6
VI. § 999.317. Record-Keeping Requirements that are Inconsistent with CCPA Should Be Eliminated or Clarified.....	8
CONCLUSION.....	9

Before the
CALIFORNIA DEPARTMENT OF JUSTICE
Los Angeles, CA 90013

In the Matter of)	
)	
California Consumer Privacy Act)	Notice File No. Z2019-1001-05
Implementing Regulations)	

**COMMENTS OF
THE COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION**

The Computing Technology Industry Association (CompTIA),¹ the leading association for the global information technology (IT) industry, respectfully submits these comments in response to the above-captioned Notice of Proposed Rulemaking Action (NOPA) regarding the California Consumer Privacy Act (CCPA). CompTIA's member companies encompass a wide cross-section of the IT sector, including software, technology services, telecommunications services, and device and infrastructure companies. Our members are committed to ensuring the privacy and security of customer data through well-crafted protections that achieve meaningful benefits, while avoiding unnecessary restrictions that would limit innovation and/or impose significant costs that would ultimately harm competition and consumers.

INTRODUCTION

In these comments, we focus on selected provisions of the proposed NOPA that should be revised prior to adoption of the final regulations. As a general matter, it bears mentioning that several draft provisions discussed below would significantly expand upon requirements

¹ CompTIA supports policies that enable the information technology industry to thrive in the global marketplace. We work to promote investment and innovation, market access, robust cybersecurity solutions, commonsense privacy policies, streamlined procurement, and a skilled IT workforce. Visit www.comptia.org to learn more.

established in the text of the CCPA, in some cases in a manner that conflicts with the purpose of the relevant statutory provision. The CCPA is already a remarkably detailed statute in many respects, and where the Legislature has provided significant detail, the implementing regulations cannot simply add more requirements that are surplus to, or in some cases even replace, the statutory scheme. Doing so would be inconsistent with the Department's authority under law, and those provisions must be modified or eliminated in the final regulations.

The specific provisions addressed in these comments, and the edits proposed below, are not necessarily the only areas for potential improvement in the draft regulations. We look forward to reviewing the other comments submitted and engaging further with the Department as the CCPA rulemaking process proceeds further.

DISCUSSION

I. § 999.305. Explicit Consent Cannot Be Required for Each New Business Purpose.

Proposed Edit:

§ 999.305(a)(3). A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use ~~and obtain explicit consent from the consumer to use it for this new purpose.~~

As currently drafted, Section 999.305(a)(3) would require that the notice provided at the time of collection disclose the purposes for which personal information will be used, while adding a new requirement that *explicit consent* be obtained for every new purpose. Requiring a business to obtain explicit consent for every new purpose significantly and impermissibly

extends the statutory language, which clearly only requires that notice of such additional purposes be provided.²

In addition, adding an explicit consent provision would significantly undermine the purpose of the statutory provision, which is to ensure that customers understand how their personal information is being used. If the draft regulation is adopted in its current form, businesses would be incentivized to provide more far-reaching and/or generalized notices upfront in order to avoid the “explicit consent” requirement. This would undermine the statutory objective of ensuring that consumers understand more specifically how their personal information will be used. Instead, consumers would be better served if businesses are incentivized to provide more specific notice when a new purpose is implemented, at which time the consumers can opt-out or remove their information if desired.

II. § 999.306. Businesses Exempt from Opt-Out Notification Should Not Be Penalized if They Later Choose to Sell Information.

Proposed Edit:

§ 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.~~

The CCPA is not intended to prevent a business’s future potential to sell personal information, and mandating such forward-looking restrictions will prevent businesses from

² Compare § 999.305(a)(3) (adding an explicit consent requirement) with CCPA § 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.”)

evolving their business plans. Treating all personal information collected during a non-sell period as a “deemed opt-out” imposes a higher burden on the business – potentially even higher than if the information had been appropriately collected after selling commenced, since the draft regulations require businesses to keep a record of the opt-outs they receive. This is in tension with other parts of the statutory text, which contemplate that businesses should be able to use information for additional purposes if notice is provided (*see also* section II above). Moreover, as currently drafted, the provision above creates uncertainty for businesses that may not have been selling personal information at the time of collection, but later choose to do so.

III. § 999.307. Mandated Data Valuation and Methodology Disclosure is Unworkable.

Proposed Edit:

§ 999.307(b). A business shall include the following in its notice of financial incentive: ***

(5) An 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 consumer’s data.~~

The draft regulation above goes significantly beyond the text of the CCPA by requiring businesses to disclose the value and methodology of the financial incentive. Such a requirement would be difficult to administer, particularly since different types of commercial relationships can make it difficult for a company to precisely value consumer data. At some level, the regulation seems to misapprehend the nature of “value” in data, for data itself is difficult to value in the abstract, with the services provided surrounding such data playing a greater role in “value” than the information itself. Indeed, academics have created wildly divergent methods for valuing

consumer data. The requirement also serves little consumer benefit, particularly since at least one metric of “value” – the value of the difference in price or services obtained by the consumer by granting consent – should be readily apparent to the consumer.

In addition, forcing businesses to disclose information how they might choose to value their own data – even if only to comply with a regulatory requirement – would be forcing the release of potentially very commercially sensitive information. Methodology information could provide competitors with insights about how a business operates, or the nature of its relationships with other entities. Mandating release of such proprietary information would inhibit a business’s ability to operate, eventually limit competition, and ultimately backfire on consumers.

IV. § 999.314. Service Provider Regulations Must Account for Provisions in CCPA That Explicitly Contemplate the Use of Data for Provider Operations.

Proposed edit:

§ 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, without the agreement of such person, entity, or consumer, for the purpose of providing services ~~to another person or entity that result in the sale of a consumer’s personal information to a third party.~~ 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.

§ 999.314(d). 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.~~

CCPA explicitly permits disclosures to “service providers” for a broad list of business purposes, and further defines “business purpose” to include both a business’ or a service

provider's operational purposes.³ The statute also permits service providers to use personal information received from one business for the business purposes of the service provider where the use is authorized as part of the contracted-for "services" provided to that business.⁴ In contrast, the draft regulation focuses solely on the business purpose of the business itself and ignores the use of information by the service provider for its operational purposes or other notified purposes, defeating the design of the statute. This would prevent several of the activities that are explicitly included on the list of permissible business purposes from taking place. The proposed edits to subsections 314(c) and (d) above offer one potential path for fixing these problems.

V. § 999.315. Opt-Out Mechanisms Should Guard Against Self-Serving Browser Implementations and be Prospective Only.

Proposed edits:

§ 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. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information. User-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall not automatically opt-out consumers. Consumers must take an affirmative action to opt-out. ***

§ 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

³ CCPA § 1798.140(d).

⁴ CCPA § 1798.140(t)(2)(C).

information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer, provided that the consumer undertakes an affirmative action to opt out of the sale of their information. Default opt-outs shall not constitute an affirmative step to opt out.

~~§ 999.315(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.~~

Codifying browser-based signals in regulations would potentially allow browser software developers to unilaterally turn on “do not sell,” or even do it selectively for certain companies. This represents a very significant transfer of power, and the regulations must therefore take care to avoid the potential for self-serving implementations in browser software. The first two edits above – to subsections 315(a) and (c) – would address this possibility by requiring users to take affirmative steps to enable any browser-based opt-out features.

Meanwhile, subsection (f) proposed to require businesses to reach back 90 days *prior* to an opt-out request and instruct third parties not to further sell information. This requirement is not found in the text of CCPA and does not create any meaningful protections for consumers since businesses would not necessarily have control over how third parties have treated data that was transferred without being subject to any opt-out restrictions. Therefore, the only effects of this provision would be to create needless administrative burdens (at best), and a false sense of privacy (at worst) to consumers that any pre-opt-out information is somehow within the power of the collecting business to scrub from all third parties. The better approach is to give consumers information and empower them to take action, and then to make businesses responsible for implementing those actions on a prospective basis only.

VI. § 999.317. Record-Keeping Requirements that are Inconsistent with CCPA Should Be Eliminated or Clarified.

Proposed edit:

~~§ 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 requests to opt out that the business received, complied with in whole or in part, and denied; and~~

~~d. The median or average 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.~~

The record-keeping envisioned by subsection 317 goes beyond what is required by the text of the CCPA, and the Department therefore lacks the necessary authority to create this new requirement. Moreover, the proposed language in subsection 317(g) is substantively problematic. For example, it is unclear what constitutes a request that is “complied with” or has been “denied,” since certain requests may fit into different buckets depending on contact. If a consumer could not be verified, how would that be characterized? What if the request was subject to a statutory exception? The lack of specificity on these issues will make implementation very challenging. At a minimum, subsection (g) should be deleted, or at the least significantly clarified to provide greater certainty to businesses on these matters.

If the provision is nevertheless retained, subsection (g)(1)(d) should provide an option for the *average* number of days to respond, rather than *median*-only, since many businesses already maintain various response-time statistics on an average basis rather than a median basis. For those businesses, having an average reporting option would therefore potentially avoid requiring the unnecessary expense of collecting or reporting of additional data.

CONCLUSION

CompTIA and our member companies continue to take consumer privacy issues very seriously, and well-crafted privacy protections must achieve meaningful benefits while avoiding unnecessary restrictions that would harm innovation, hurt competition, drive up costs, or violate the statutory scheme established by the Legislature. We urge the Department to adopt the changes described above, and we look forward to reviewing feedback from others on the draft regulations.

Sincerely,

/s/ Dileep Srihari

Dileep Srihari
Vice President and Senior Policy Counsel

Alexi Madon
Vice President, State Government Affairs

COMPUTING TECHNOLOGY INDUSTRY
ASSOCIATION
515 2nd Street NE
Washington, DC 20002

December 6, 2019

Message

From: Alan Thiemann [REDACTED]
Sent: 12/6/2019 9:31:18 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: William Harris [REDACTED]; Lauren Scheib [REDACTED]; John Weiner [REDACTED]; John Kleeman [REDACTED]
Subject: Comments of the Association of Test Publishers
Attachments: Final Comments 12062019.pdf

Please find attached the comments filed on behalf of the Association of Test Publishers (ATP). We appreciate the opportunity to provide this input and we hope our views will provide constructive recommendations for modifying the Proposed Regulations. We are available for follow up questions or a face-to-face meeting should the Office feel it would be helpful.

Please let me know if a call or meeting is requested.

Thank you for your attention to this matter.

Alan Thiemann
General Counsel

--

Alan J. Thiemann
Law Office of Alan J. Thiemann
700 12th Street, NW
Suite 700
Washington, DC 20005
[REDACTED]

BEFORE THE CALIFORNIA DEPARTMENT OF JUSTICE

California Code of Regulations, Chapter 20, Title II, Div. 1 (sections §§ 999.300 - 999.341)

Comments of the Association of Test Publishers

The Association of Test Publishers (“ATP”) submits these comments to address the serious concerns of the testing industry about the Proposed Regulations for implementing the California Consumer Privacy Act (“Proposed Regulations”), as published on October 11, 2019. This submission is being made by the required date of December 6, 2019.

The ATP is the international trade association for the testing industry. The ATP is comprised of hundreds of publishers, test sponsors (i.e., owners of test content, such as certification bodies), and vendors that deliver tests used in various settings, including healthcare, employment (e.g., employee selection and other HR functions), education (e.g., academic admissions), clinical diagnostic assessment, and certification/ licensure (e.g., licensure/ recertification of various professionals), and credentialing, as well as businesses that provide testing services (e.g., test security, scoring) or administering test programs (“Members”). Since its inception in 1987, the Association has advocated for the use of fair, reliable, and valid assessments, including ensuring the security of test content and test results. Our activities have included providing expertise to and lobbying the US Congress and state legislatures on proposals affecting the use of testing in employment and education, as well as representing the industry on regulatory matters and litigation surrounding the use of testing. We developed and currently publish compliance guidelines on the EU General Data Protection Regulation (“GDPR”) and are currently publishing a series of educational bulletins entitled, “Privacy in Practice” that focus on compliance with both US and international privacy laws and regulations.¹

The ATP respects the goals of the Proposed Regulations to ensure comprehensive implementation of the California Consumer Privacy Act (“CCPA”) and to provide guidance to businesses that must comply. However, we strongly believe that specific circumstances common in the testing industry, along with the many smaller/medium-sized businesses in the industry, justify modification of the Proposed Regulations when balanced against the rights of individual test takers as consumers. Thus, the ATP urges the Attorney General to take these specific comments into account in adopting final regulations.

¹ The ATP is preparing to publish a bulletin on compliance with the CCPA yet this month. Another pending bulletin focuses on the use of international standards by testing organizations to achieve data security and privacy objectives (i.e., ISO 27001, ISO 27701), as well as the use of third-party audits that are performed under AICPA (American Institute of CPAs) standards for Systems and Operational Controls (SOC) Reports. *See* discussion of “reasonable security measures,” *infra.* at p. 18.

Many testing events occur which greatly benefit and protect the general public, along with those who rely on test results, especially individual test takers. California consumers are no exception to the vast – and growing – population of users of assessments whose purpose is to advance themselves personally and/or professionally.²

Individuals voluntarily submit to being tested for many reasons. Among them is to obtain a driver's license, to identify ways to improve their lives, to understand their academic strengths and weaknesses, to gain admittance to an institution of higher learning or other academic/adult educational program, to seek employment or to gain a promotion once employed, to become licensed/certified in a profession, to become certified in sport/recreation (e.g., flying, scuba) or professionally (e.g., IT certifications in literally thousands of technical skills), and even to understand their own health (e.g., diagnostic tests) or how to provide lifesaving procedures on others (e.g., CPR). In a majority of these instances, assessments are pivotal to a public interest and/or consumer protection motive (e.g., medical, legal, accounting, airline pilot, police, EMT).

Many of these situations are examples of “high stakes” secure testing, i.e., where the outcome of a test carries a significant consequence for the test taker (such as a securing a job, getting admitted to a school, or being issued a license or certificate). In these cases, the test items are kept secure (even by the U.S. Copyright Office, which has separate copyright registration procedures for secure tests) to ensure that future test takers cannot obtain advance knowledge of them – which would have the effect of invalidating the test results. In fact, if some test takers are able to obtain favorable results on a test by cheating then the value of the testing program is completely undermined for everyone. Testing has become part of our daily lives; individuals generally well understand that testing provides them with benefits, directly or indirectly, by assisting to serve the public health, safety, and welfare of the community or society as a whole.

Thus, it is vitally important that every high stakes testing program is able to ensure that its online registration process can be conducted in accordance with the CCPA and that all test administrations, whether conducted in person or online, are fair to all test takers. In so doing, a testing organization must be able to ensure that an individual who takes a test is in fact the same individual who is registered to take the test (with or without establishing that s/he is eligible to take the test). Furthermore, testing organizations must monitor testing events to ensure that

² The ATP's comments are not intended to apply to educational testing in K-12 classrooms. However, the ATP is aware that some school admissions testing of children is done by computer, as well as career-oriented K-12 educational and vocational education programs for children. In any situation involving the testing of minors, including for medical/diagnostic purposes, the ATP expects that the controlling business would require a test taker agreement to be signed by the parent, inasmuch as minors do not have legal status to enter into such an agreement. Thus, regardless of age of the minor child, the ATP requests that the final regulations (§999.330-332) be modified to be consistent with this legal requirement. We submit that if there is an effective “affirmative authorization” by a parent or guardian in the first instance, there is no need for any separate opt-out notice to the child or a separate opt-in process.

administration irregularities which may have an adverse impact on every test taker are detected and handled in an appropriate manner.³ Equally important, testing organizations seek to ensure that all personal information collected from test takers (i.e., “consumers”) is protected from unauthorized access and/or acquisition, and that all privacy-related requests from consumers are handled appropriately under the terms of the relevant laws. For all of these reasons, the ATP submits that every high-stakes testing organization has the following legitimate purposes associated with the need for collecting and using the personal information of test takers: (1) to ensure fairness in testing; (2) to prevent fraud (i.e., cheating) by individuals taking a secure test; and (3) to protect proprietary (and often copyrighted) secure “high stakes” test items from being stolen by test takers and illegally distributed to future test takers.

Consistent with the above objectives, the ATP notes that many high stakes testing programs are national in scope, drawing test takers from every state.⁴ For ease of business operations, ATP Members often adopt a uniform Privacy Policy to meet the needs of all test takers across the United States. Given the upcoming effective date of the CCPA, we understand that many testing organizations have already modified their privacy policies to meet the CCPA requirements. Thus, it is very important to ATP Members to be able to manage their operations to address all aspects of the CCPA while complying with other applicable state privacy laws. Through its comments, the ATP has addressed testing-specific issues to highlight interpretations and recommended ways to modify the Proposed Regulations.

General Background – Roles and Responsibilities in Testing

At the outset, we need to make the Attorney General aware that a majority of the high stakes testing programs do NOT rely on a traditional two-party business relationship, where a

³ It is important to recognize that in most high stakes tests, the test-taker is expected to answer questions on his/her own, without having advance access to test questions, receiving any assistance from another person, by using reference materials or notes, or having unauthorized access to the Internet. Obviously, these high stakes tests are unique to the specific individual taking the test – the results/scores are only intended for and relevant to the specific individual who has registered for the test and then verified to take the test. Consequently, every testing organization pays significant attention to the security of test content and test taker information, to ensure that cheating on tests is prevented so that every test taker has an equally fair opportunity to succeed.

⁴ Indeed, many ATP Members operate international testing programs, meaning that those organizations register and administer tests to foreign test takers. Thus, they must operate in accordance with foreign privacy laws, especially the General Data Protection Regulation (“GDPR”). In those situations, many ATP Members have attempted to establish a uniform privacy policy that harmonizes the GDPR with the CCPA. It is unrealistic to expect an entity doing business internationally to adopt completely separate and distinct privacy policies for each country in which it operates (or for each state in the United States).

consumer has a direct relationship to the business that is selling goods or services (e.g., going into a store or online to make a purchase directly from a seller). To accomplish smoothly functioning and efficient operations to serve their customers, many testing organizations have segmented their operations into two or more diverse roles in the provision of testing services: one entity that owns the test (that may have developed the test or contracted for its development) and makes all of the decisions about how to use any personal information obtained from an individual test taker; and one or more secondary entities that actually handle the delivery, administration and scoring of the testing services. It is such a secondary entity that in many instances is the one that actually has the direct contact with the test taker/consumer.⁵ In addition, there often are other parties who provide supporting services to either or both of the two principal businesses (i.e., function as a “service provider” under the CCPA). The final regulations must recognize that any business that functions as a “service provider” does not control the collection and use of consumers’ personal information.⁶

Another unique factor of the high stakes testing industry is that “consumers” of tests and testing services may be individuals, but in many instances, the rights to use tests and/or testing services are “sold” to businesses (i.e., employers) or professionals (e.g., doctors, psychologists), who then have the responsibility to arrange for the administration of the tests to the actual test takers, either by themselves or by a test delivery vendor. In this context, then, it is equally important to note that, especially for “secure tests” (i.e., those tests whose items must not be made available to test takers in advance of a test administration), the tests themselves are not “sold” in the commercial sense, but are provided for use by the customer of the testing services — ownership of the tests is not conveyed in a commercial “sale.”⁷

⁵ Under the GDPR, these parties are labeled as the “controller” and the “processor.” The ATP encourages the Attorney General to adopt these terms or at least provide equivalent definitions by making use of similar parallel terms, both for the sake of clarity and to enable consistent treatment of personal information by entities that must comply with both the CCPA and the GDPR. Without clarification in the final regulations, the ATP fears that the CCPA could be interpreted as placing a higher regulatory burden on the processor/service provider than it does on the controller.

⁶ Thus, the ATP generally endorses the Proposed Regulations regarding “service providers” (see §999.313), although we have recommended clarification of these regulations, as addressed in Section 7 (*see infra* at pp. 21-23).

⁷ Secure tests are granted special copyright protection in the United States under the 1976 Copyright Act. The regulations implementing the Act define (in part) a “secure test” as “a nonmarketed test...” “For these purposes, a test is not marketed if copies are not sold but it is distributed and used in such a manner that ownership and control of copies remain with the test sponsor or publisher.” 37 CFR 202.20(b)(4). [FOOTNOTE CONTINUED ON NEXT PAGE]

Perhaps because of the complexities inherent in the provision of testing services, the standard practice for most testing organizations is the use of a formal test taker form/agreement to spell out to each individual test taker both his/her rights and responsibilities related to the testing services (e.g., rights to challenge or appeal, retest rules, prohibitions on copying/sharing test items), as well as the information about the business's privacy policy, which the consumer must acknowledge or accept.⁸ Among the uses of personal information that may be enumerated in such agreements are specific steps taken to ensure that cheating does not occur (e.g., monitoring test administration either physically or electronically). Many testing organizations require the test taker to sign this agreement first when registering online for the test and then again at the test administration before the test taker begins the testing session, which provides evidence that the test taker was given the required notice twice.

Because of the well-documented division of responsibilities among different entities participating in a testing event, the most critical issue in a privacy context is which entity has the responsibility for collecting personal information from test takers and for determining what use(s) are to be made of that information, which usually is the test owner. While the high stakes test owner may obtain test taker information from one or more of its service providers in the performance of the testing services, the responsibility for compliance with the CCPA must fall squarely on the test owner, the entity that makes all of the relevant decisions about what personal information should be collected and what uses it makes of that personal information.⁹

Equally pertinent to this issue is the key distinction between test takers' personal information (e.g., name, address, email address) and the outcome of testing services purchased by the test takers – the test results or scores. Although it may be appropriate in some situations to recognize that the answers to test items given by a test taker are “personal” to that individual,

See 42 Fed. Reg. 59,302, 59,304 & n.1 (Nov. 16, 1977). The ATP contends that the final regulations must include guidance on an exception addressing the recognition of a business's IP rights under federal law.

⁸ The ATP believes that, to the extent that a test taker form/agreement is used by a testing organization as a “point-of-collection notice,” it must meet the requirements of §999.305(a). Nevertheless, no matter how much a business tries to use “plain language” and “avoid legal jargon,” someone can always assert that a document fails to conform. The final regulations should be modified to include language that a notice shall be “reasonably written to achieve the goals” to ensure that a balanced approach is used to evaluate all such documents.

⁹ Of course, some of those responsibilities may be delegated by contract to one or more service providers, who often times have the direct relationship with the test takers, such as handling registration of test takers, administering the actual testing services, scoring tests, and/or managing the security of the testing event. *See discussion of “data broker” infra.* at p. 23.

test results/scores are not “collected” information.¹⁰ Test results/scores are the product of the test services procured by the consumer; they are not information collected from test takers, but are derived outcomes produced by the testing organization using proprietary scoring rubrics.¹¹

Moreover, the uses of test results/scores are co-extensive with the need of each test taker for the testing services. In other words, if an individual is seeking a license/certificate documenting a particular skill (e.g., in law, medicine, technology), the issuer of that license/certificate is the owner of the test and the outcome is based on the individual’s test results/score; similarly, if an individual is seeking a job or a promotion, that decision is made by the employer, based upon various factors, including the individual’s test results/scores. Application of overly-prescriptive privacy requirements on the sharing of an individual’s test results/scores defeats the very purpose the individual had in taking the test in the first place.¹²

Another issue related to test results/scores is raised by the CCPA definition of “personal information” to include “inferences” drawn from any of the information identified to create a profile about a consumer; specifically, the law addresses inferences about a consumer’s: preferences; characteristics; psychological trends; predispositions; behavior; attitudes; intelligence; abilities; or aptitudes. *See* Cal. Civ. Code §1798.140(o)(1)(K). The ATP submits

¹⁰ Even “raw” data provided by a test taker is not always considered to be “personal information” or treated as personal information. In circumstances where the test taker is an employee, where the testing organization’s IP rights must take priority over a person’s test answers, and where other exemptions may exist that supports a denial of a request for access to, or deletion of, information collected from the test taker, such test answers are effectively not personal information. These situations are covered in the test taker agreement (*see infra*, fn 10).

¹¹ Significantly, this type of derived information is largely unique in the testing industry. Test results/scores are distinguished from consumers’ input on social media services, where an individual’s postings to the platform are then shared in the same manner and context in which they were inputted. Nor are testing results/scores remotely similar to derived personal information that is generated in a marketing context, where a person’s buying patterns/behaviors are tracked and used to create a profile that is sold to other marketers. Indeed, the Proposed Regulations (at §999.305(d)), make it clear that such results cannot be “personal information at the time of collection” – obviously, test results/scores do not even exist at the time of collection of the consumer’s personal information related to the testing services. An individual acquires (or obtains) testing service where test scores are the contracted for outcome or product. What a testing organization does with those scores is governed by and disclosed to the test takers in the test taker agreement.

¹² This is true regardless of whether the individual paid for the test; in some instances (e.g., employment, training) the employer may have paid for the test. Even when an individual pays for the test, s/he authorizes the test owner to share the results/scores with certain designated recipients (e.g., schools to which the individual is applying, jobs for which the individual is applying, certification bodies from which the individual is seeking a license or certificate). Either way, the need for a decision-maker, or multiple decision-makers, to obtain the test results/scores is precisely the reason why the individual registered for and took that test.

that if the CCPA is implemented with extreme interpretations, it would effectively ban all of the testing services we have discussed. Rather, we believe that the CCPA is focused on regulating the sale of consumer marketing profiles to other marketers, not preventing consumers from obtaining testing services they themselves consider valuable. Read in this light, then, the final regulations should articulate this distinction and establish the clear focus on the uses of personal information for consumer marketing activities, not the prevention of legitimate business service outcomes.

Another reason for our concern about the treatment of test results/scores stems from the definition of the term “sale” under the CCPA. The CCPA defines the “selling” of personal information broadly to mean a business 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 to another business or a third party for monetary or other valuable consideration. Unfortunately, neither the CCPA nor the Proposed Regulations defines what qualifies as “other valuable consideration.” It is absolutely crucial that the Attorney General establish a proper definition in the final regulations, clarifying what is “valuable consideration” in specific contexts. Without such clarity, a testing organization that shares a “common interest” in scoring and reporting test scores of test takers with its affiliates, subsidiaries, service providers, contractors, or other business partners (“vendors”) (i.e., the controlling business must share personal information in order to fulfill its contractual obligations to provide testing services – especially the test results/scores on a test), inappropriately may be deemed to be violating the CCPA. The ATP contends that such “common interest” sharing does not constitute “valuable consideration” inasmuch as test takers’ results/scores are only shared to further the underlying testing service contract and they do NOT result in any commercial value related to any marketing of personal information to these other businesses.¹³

In advancing these positions regarding privacy notices, the ATP affirmatively agrees that a testing organization that uses test takers’ personal information, including any test results/scores, for advertising/marketing purposes, or shares such information with a vendor in a way that permits the vendor to commercially use that information, must comply with the CCPA requirements as related to such purposes.¹⁴ Therefore, when a testing organization wants to communicate with previous test takers to promote or market its products or services (e.g., new

¹³ In most situations, the testing organization’s contract with a vendor specifically restricts the use of any personal information shared pursuant to the contract to the services required. In other words, the vendor is not allowed to use that personal information for its own business purposes outside of the services being provided under the contract with the controlling business. It is that third-party commercial marketing that the CCPA intends to regulate, not the ability of vendors to provide legitimate services in the fulfillment of an underlying contract.

¹⁴ By comparison, it should be abundantly clear that communicating with a consumer about his/her current contract for testing services (e.g., providing details about which test and the test location or date), is expected as part of a current contractual relationship and does not constitute marketing.

testing products or companion testing opportunities not already involved in a services contract), those communications constitute marketing and the business must comply with the CCPA.

This background information on the roles and responsibilities as found in the testing industry relate to specific Proposed Regulations, as addressed in the following comments.

Comments on the Proposed Regulations

1. Issues in determining if a testing organization is covered.

Two fundamental issues confront a testing organization in determining if it is covered under the CCPA: (1) whether it has more than \$25 million in gross revenues; and (2) whether it collects personal information on more than 50,000 California consumers. Moreover, parent companies and subsidiaries using the same branding are covered in the definition of "business," even if they themselves do not exceed the applicable thresholds – the ATP objects to this determination on the grounds that if the parent/subsidiary is itself a separate legal entity, it is lawfully entitled to be treated as a separate business. The final regulations should rectify this mistaken legal position.

Despite extensive debate since passage of the CCPA as to whether the appropriate revenue threshold is "California revenues" or total revenues of the organization for all of its operations, the Proposed Regulations are silent in resolving that question. Because a testing organization may have total gross revenues that exceed the \$25 million threshold on a national or even international basis, but generate less than that amount from selling testing services to California consumers, resolving that question is extremely important for the testing industry. In other words, a business may engage in test development and other consulting services completely outside of California that do not involve the collection of personal information of California consumers or any commercial marketing of their personal information collected by others. We submit it would be unfair to hold a business liable to comply based on revenues that are not related to the legitimate consumer privacy purposes of the CCPA. In those situations, the ATP submits that the business is not subject to the CCPA.¹⁵ We request that the final regulations address both of these possibilities to clarify the appropriate scope of the CCPA.

Turning to issues over the threshold involving the number of consumers, many testing organizations, whether they are controllers or processors (service providers) of test takers' personal information, may have no way to determine if they have records on more than 50,000

¹⁵ Thus, any interpretation of this threshold test that interferes with and/or creates a burden on interstate commerce is invalid under the Commerce Clause of the United States Constitution. (Article I, Section 8, Clause 3), which gives to Congress the exclusive power to regulate commerce "between the several States." This is true regardless of whether the entity is located in California or outside of the state.

California consumers. The ATP has already heard from some of its members that, especially when functioning as a service provider (e.g., providing test delivery and/or scoring services), test takers' physical addresses are not always used, which therefore makes it impossible to determine the consumers' state of residence, and consequently, whether the testing organization meets the threshold.¹⁶ This lack of physical address is also likely if the testing organization uses only a coded (or tokenized) identifier. Accordingly, the ATP requests that the final regulations acknowledge that the inability to determine (either physically or electronically) the number of California consumers in a database will not in itself be interpreted as a violation of the CCPA – or will not result in an automatic assumption that the business is covered.

2. Issues concerning “point-of-collection” notices.

As noted above, a testing organization that acts as a controller may not actually collect test takers' personal information, rather it is most often collected by one or more service providers (e.g., website operator, payment gateway, testing services vendor). That practical reality leads to concerns about how Privacy Notices are to be handled under the Proposed Regulations.

While §999.305(a)(1) sets forth the “general principle” that such notice “is to inform consumers at or before the time of collection of a consumer’s personal information of the categories of personal information to be collected from them and the purposes for which the categories of personal information will be used[.]” nowhere in this regulation, nor in the CCPA itself, is there a requirement as to who has to provide the notice. As such, the ATP submits that a valid “point-of-collection” notice should be able to be provided to a specific consumer by either the controlling business or by its service provider(s) under contract. We urge the Attorney General not to lose sight of the crucial general principle – as long as the appropriate notice is given to consumers (here test takers) prior to the collection of personal information, it should not matter whether that specific notice is given by the owner/sponsor of the test/test program, who makes the decisions about the purposes and uses of the collected information, or by a service provider working under contract to the test owner that may actually have the direct contact with the consumers.¹⁷

¹⁶ Many organizations operate national or international online testing programs, where typically test takers are only identified by full name and email address, but since there is no need the physical address, it is not captured. This is particularly the case when an entity follows privacy minimization guidelines. Moreover, a single testing organization may have multiple customer contracts and thus not know—or have any ability to ascertain—how many California consumer records it has (e.g., 50,000 or 4 million).

¹⁷ The Proposed Regulations state that, “If a business does not give the notice at collection to the consumer at or before the collection of their personal information, the business shall not collect personal information from the consumer.” §999.305(d). The ATP recommends that this sentence should be modified to acknowledge [FOOTNOTE CONTINUED ON NEXT PAGE]

Similarly, the Proposed Regulations (§999.306(d)) also state that a business is not required to provide a “point-of-collection” notice when it collects personal information from a third party and not the individuals themselves. But in such situations, the Proposed Regulations require that the controlling business cannot “sell” such personal information unless it goes through another step to ensure that the appropriate notice was in fact provided by the third party. As we noted earlier, the controlling testing organization is NOT selling or making any commercial use of personal information, but is using/sharing it with its vendors to fulfill an ongoing test services contract with the consumer directly or through another entity that has a contractual relationship with the consumer (e.g., an employer, a certification body from whom the consumer is seeking to earn a certificate, credential, or license) – and equally important, to notify the consumer about the test results.¹⁸ Forcing the controlling test owner/sponsoring program to perform one or more extra compliance steps beyond the underlying contractual obligations of the parties is onerous, time consuming, and therefore represents an unnecessary cost to all of the businesses involved – plus, it provides no additional benefits or rights to the consumers/test takers. The approach seemingly mandated by the Proposed Regulations elevates form over substance – the rights of the consumer under both the CCPA and §999.305(a)(1) are met when any one of the businesses with a legal obligation, as agreed to between them, gives the notice.

An important inconsistency in the Proposed Regulations arises when the initial point of contact is online. This problem is significant for testing organizations, where the great percentage of consumer registrations for testing services occurs online. The Proposed Regulations (§999.306(d)) state that a “consumer whose personal information is collected while a notice of right to opt-out notice (sic) is not posted shall be deemed to have validly submitted a request to opt-out.” First, such an assumption is unwarranted – just because a business collects personal information does not mean it is selling that information. Moreover, that assumption expressly conflicts with the statement immediately following, that a business does not have to post an opt-out notice if it is not selling personal information. In contrast, though, §999.315(c)

that any business involved in the “common interest” use of the consumer’s personal information should be permitted to give notice. If the consumer does not opt out in response to such a notice, s/he has opted-in to the collection and use of personal information – this is an “affirmative authorization” as defined in §999.301(a).

¹⁸ Sharing or “selling” personal information in an employment testing situation is often a total misnomer. When the employer is paying for the test, with the employee’s obvious knowledge, the testing organization is under contract with the employer and the test taker’s personal information is shared directly from the employer with the testing organization. If the test results for specific employees were not allowed to be shared as part of the contract, no testing services could be provided. The ATP submits that the Proposed Regulations should not be interpreted in such a manner as to prevent specific business contracts from being entered into and performed – and the final regulations need to make this point clearly.

of the Proposed Regulations requires that if a business collects consumers' personal information online, it "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 ["do not sell"] request ... for that browser or device, or, if known, for the consumer."¹⁹

As related to the testing industry, neither requirement makes sense. A test taker who registers for a test online is not likely to opt-out of the collection of his/her personal information, without which the testing services cannot be delivered, including the delivery of the test results/scores. If a test taker were to opt-out of the service, the testing organization would be unable to share the test taker's information with its "common interest vendors" and the testing services would not be able to be fulfilled. Similarly, a test taker who needs his/her test results shared to apply for a job/promotion (i.e., shared with an employer) or to obtain a desired certificate, credential or license (i.e., shared with a certification board or state licensing board) is not likely to tell the controlling testing organization not to share the test results -- that is the whole point of taking the test.²⁰ On this point, users of test results/scores are not going to take the word of the test taker as to his/her scores; that information must come from the issuer of the results/scores to be assumed valid.

Additionally, in the conduct of its testing services, it is vitally important that the testing program is able to collect specific video or biometric information (e.g., photo IDs, fingerprints), to ensure that an individual who appears for a test session is in fact the same individual who is registered to take the test (with or without establishing that s/he is eligible to take the test), and furthermore, that its testing events are adequately monitored and controlled at the testing location (e.g., secure test center) or at home, and that testing irregularities which may have an adverse impact on every test taker are detected and handled in an appropriate manner.

¹⁹ Even if a testing organization wanted to comply with either of these requirements, it is practically impossible given conflicts in the Proposed Regulations. In §999.305(b)(3)) the business is required to provide the consumer with a link to access "an interactive webform" where consumers can exercise their rights, while §999.305(c) requires the link to redirect individuals to the relevant portion of the business's privacy policy. This inconsistency needs to be rectified in the final regulations.

²⁰ The timing of a consumer's decision to opt-out also plays a significant role in a testing organization's handling of the matter. On a procedural level, it is impractical to opt-out after the test taker has already taken the test because it would result in inappropriate and dangerous outcomes for a testing organization to permit a consumer to opt out after a test has been taken or scored. Either outcome would be tantamount to allowing the test taker to delete his/her test results because the score was too low or cheating by retaking the test after seeing the items and then "deleting" the first score -- a test taker using either "opt-out" could not receive a valid score or would be engaged in an attempt to cheat on a future test.

Finally, the Proposed Regulations fail to take account of the recent amendments to the CCPA in regards to the respective one-year exemptions in the treatment of employees' personal information and business contacts' personal information. As explained below, it is important to members of the testing industry that appropriate guidance regarding those changes be included in the final regulations.

a) Need for guidance on handling employee personal information.

The Legislature passed an amendment providing a one-year moratorium on the treatment of employee personal information, which is not reflected in the Proposed Regulations. The ATP strongly encourages the Attorney General to address this situation in the final regulations by setting forth specific guidance as to how a business should handle relevant employee personal information during the moratorium, especially with regard to the notice of collection that it provides to its employees and other affected individuals.²¹ Of course, testing organizations are themselves employers that must keep and utilize employee information in the course of meeting state laws, insurance requirements, and the like. As such information retained by the business is NOT consumer related, and should not be regulated by CCPA.

More than testing organizations as employers, we note that to the extent testing organizations provide testing services, a business employer customer is often the controlling entity in determining what personal information is collected from its employees and how it is used in regards to a particular test used for internal HR decisions. Since this delay applies to all businesses that may otherwise be covered, it is critical that this guidance be made available as quickly as possible.

In the context of privacy notices for employees, job candidates and contractors some requirements in the Proposed Regulations ("do not sell" and website privacy links) appear to be inapplicable at this time; the final regulations should reflect the exemptions, or explain how the moratorium should be implemented for 2020.

b) Need for guidance on handling business contact information.

The September amendments also contained a one-year moratorium on the treatment of business contact information. That amendment is of importance to the testing industry because in many situations, a testing organization is selling tests/testing services not to individual test takers, but to employers and/or others (e.g., doctors, counselors) who in turn administer the test to their customers (i.e., the individual test takers). Thus, the testing organization, who is the owner of the test, is not the controlling entity that makes the decisions about the collection and use of the personal information of its customers/clients/consumers. In these instances, the testing organization becomes a processor/service provider (e.g., for test scoring, for record-keeping) to

²¹ The language of AB 25, amending the CCPA, also applies to job applicants, as well as candidates for officer and board positions. The ATP submits that the final regulations must cover all affected individuals.

the entity that actually controls the privacy decisions²² — and whose privacy policy governs the notices to consumers. Consequently, a testing organization will have contact information on a number of representatives of controlling business entities, which are outside of the scope of the CCPA at least for 2020. The ATP strongly encourages the Attorney General to include guidance on how a business should handle this information in the final regulations. When a business deals with another business, and a representative of the second business provides his or her contact information, for 2020 at least, that collection is not treated as the collection of personal information, but is “business information.” For example, when such a business contact provides a business address, telephone number, and a business email address, the representative is acting on behalf of his or her employer — the person is not the “consumer” and the business is not “a natural person” as defined Section 17014 of Title 18 of the California Code of Regulations. *See* Cal. Civ. Code §1798.140(g).

In addressing this issue in the final regulations (and beyond 2020), the ATP submits that the Attorney General should consider the interpretation of similar language adopted by the Office of the Privacy Commissioner of Canada under the Personal Information Protection and Electronic Documents Act (“PIPEDA”), *Bulletin on Personal Information* (2013). Essentially, that bulletin holds that PIPEDA does not apply to an organization in respect of the business contact information of an individual that the organization collects, uses or discloses solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession. Even so, the bulletin does note that some contact information (e.g., personal cell phone number) may still be considered personal. Indeed, the ATP notes that the Ontario bulletin improperly fails to recognize that a self-employed individual is sometimes a business and at other times, the person will provide personal information — in our opinion, a business should be allowed to make this distinction when it has sufficient evidence to determine that an individual has provided business contact information as part of a business relationship.

In the context of privacy notices for customers (e.g., of testing organizations) the requirements in the Proposed Regulations (“do not sell” and website privacy links) would be inapplicable at this time; the final regulations should reflect the exemptions or explain how the moratorium should be implemented for 2020.

3. Issues related to privacy policies.

As a general rule, a testing organization will use its privacy policy to provide the information required to meet applicable privacy laws and regulations. As the ATP discussed earlier, that fact makes it particularly important for the final regulations to recognize that, when

²² Because the testing organization is providing processing services as a service provider, it may end up with test takers’ personal information shared with it by the controlling entity. As discussed in Section 7 (*infra.* at pp. 18-20), in the role as a service provider, the testing organization must adhere to the contractual obligations to protect the privacy rights of those customers’ end users. *See also* General Overview – Roles and Responsibilities (*supra.*, pp. 3-4).

an entity documents that it is doing business in multiple states (or countries), the Attorney General should be required to take that fact into account in making any legal evaluation of the business's privacy policy.

In general, a business's privacy policy is intended to set forth a clear statement about what personal information is collected and how it will be used, as well as to set forth in a transparent manner what rights a consumer has with respect to that information and how the consumer may go about exercising those rights. In order to comply with the Proposed Regulations, privacy policies must be expanded to cover other matters, including handling requests from consumers, dealing with collection of personal information of minors, and adding information related to "Do Not Sell" and opt-out opportunities. Accordingly, the ATP recommends that the final regulations clarify that a business shall be allowed to provide information about, and access to, the "Do Not Sell" link and/or the opportunity for the consumer to opt out of the collection and use of personal information, in its privacy policy.

Despite the statement in the Proposed Regulations that, "The privacy policy shall not contain specific pieces of personal information about individual consumers and need not be personalized for each consumer[.]" (§308(a)(1)), the Proposed Regulations apparently contemplate that a business will be required to make significant changes to its privacy policy regarding the "look back" period, to address: (1) the categories of personal information collected within the preceding 12 months (and categories of sources); (2) whether the business has sold/disclosed certain personal information within the preceding 12 months to third parties for a business or commercial purpose; (3) the categories of personal information covered; and (4) if the business sells personal information of minors under age 16 without parental authorization. *See* §999.313(1)(E). The ATP believes that such "backwards-looking" information will be unique for different consumers and for different situations; thus a privacy policy should be written to notify consumers about its "future" intentions, as opposed to what may have taken place in the past twelve months. This approach seems especially appropriate given the changes that are likely to occur in the way future privacy policies are structured and the details they contain. Quite clearly, the "look back" feature of the CCPA is most appropriate in responses to specific consumer requests, to provide the specifics of what actually was collected and how it was used. Accordingly, the ATP recommends that the Attorney General clarify that the language in §308(a)(1) should be followed and any "look back" information should not have to be communicated in the privacy policy itself.

A further requirement in §999.308(1)(B) is that the business must, "Describe the process the business will use to verify the consumer request, including any information the consumer must provide." As discussed in Section 4 (*infra.* at pp. 15-17), the required methods and procedures for how a business must handle request verifications are complex and will make it difficult to come up with an accurate uniform description in "plain, straightforward language"

and to avoid the use of “technical or legal jargon.” The final regulations should clarify that the business must provide a “reasonable” description of its procedures.

Another issue that arises today in privacy policies of many testing organizations is the identified use of personal information for research purposes (e.g., to update test norms such as statistical means and standard deviation, conduct item or test fairness analyses). The ATP notes that such research generally uses anonymous test taker information, such as test results based only on gender or other demographics (e.g., age, country). Similarly, in order to comply with federal and state anti-discrimination laws, employers often require testing organizations (as service providers) to keep anonymous aggregated data about the number of job applicants in special populations – the same types of information are commonly kept by employers to protect against discrimination claims.²³

The CCPA makes it clear that a business is free to collect, use, retain, sell, or disclose consumer information that is de-identified or aggregated. *See* Cal. Civ. Code §1798.140(o)(2). The ATP submits it would be helpful for the final regulations specifically to provide examples explaining appropriate uses of such information, including uses in testing, where anonymous personal information has been de-identified and is then aggregated so that no information identified to the consumers is shared or disclosed. Most often, testing organizations include disclosure of such research uses of some personal information on an anonymous and aggregated basis in the test taker agreement, so that they do not have to go back to test takers a second time with a new notice.

4. Issues concerning verification of requests.

In order to respond to requests to know and to delete personal information collected by a business, the Proposed Regulations require different verification procedures based on whether or not the consumer exercising the right maintains a password-protected account with the

²³ These considerations also impact what information a privacy policy discloses on the retention of personal information. If the business has documented needs for specific personal information to comply with federal/state laws, or must provide personal information to a customer for its legal purposes, then the business will be forced to deny requests to delete that personal information. Similarly, test takers usually expect that their test results/scores will be available for as long as they are needed by the actual customer (e.g., employer for as long as it is seeking to fill a job, certification body for as long as a person is seeking certification, consumer for as long as the results have meaning), so retention of test results for many months is quite common.

business.²⁴ When the testing organization uses a password-protected account, the verification required under the Proposed Regulations should be satisfied using the same technology available to enable the business to match the consumer to the account, just as the system enables that consumer to change his/her password; nothing more should be required. *See* §999.313(c)(4). The consumer presumably is starting this process armed with the account information s/he already possesses, and the business will be able to match that information directly to the consumer. Requiring a business to go back to the requester for “re-authentication” is simply redundant and creates an unnecessary burden on the business.

Verification methods that should be required for a non-password account or non-account request ought to focus appropriately on the level of fact-based analysis by the business – to verify the individual’s identity to a “reasonable degree of certainty” if he or she is seeking access to certain categories of personal information or to a “reasonably high degree of certainty” if he or she is seeking access to specific pieces of personal information the business collected. If an individual is requesting the deletion of personal information, the business must verify the identity to a reasonable degree or reasonably high degree of certainty, depending on the sensitivity of the personal information and the risk of harm posed to an individual by an unauthorized disclosure.²⁵

²⁴ For these requests, the Proposed Regulations require “at a minimum” that the business provide consumers with a toll-free telephone number. *See* §999.312(a) and (b). The ATP submits that this requirement is singularly inappropriate. Someone from the business has to transcribe the information (in real time or from audio), which is likely to result in data entry errors and failure to understand what the consumer has said/meant, either of which could result in potential liability for the business. The most accurate way for the consumer to provide request information, including verification information, and for the business to receive it without error, is for the consumer to fill out an electronic or paper form. Audio recording of this information also may result in technical problems, resulting in lost information. Finally, having an audio recording of this information presents an added exposure for the business.

²⁵ For a request from a consumer that has no account with the business, the Proposed Regulations state that the business must verify the request with a reasonably high degree of certainty. “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.” *See* §999.325(c). The ATP submits that this approach represents an unwarranted burden on a testing organization unless the requester has presented documentation from which the testing organization can determine that there is a reasonable likelihood that the consumer in fact took a test with the testing organization (e.g., the name of the test, the date it was taken, the place it was taken) or offered an explanation as to why the requester believes the testing organization has the consumer’s personal information, which evidence may include a statement to that effect in the attestation. Absent such a *prima facie* showing, there is no reason to believe that a [FOOTNOTE CONTINUEUD ON NEXT PAGE]

To a great extent, the differences in the level of verification are based on the business having to conduct a risk analysis of the sensitivity of the personal information and the likelihood that someone other than an actual consumer would attempt to gain access to (or seek to cause harm by deleting) a consumer's information. *See* §999.323(b)(3). It bears repeating that most testing organizations are not generally in the business of conducting marketing/advertising operations based on the use of consumers' personal information; thus, the only basis upon which a consumer should need to make a request is if s/he previously had taken a test from or through the testing organization. Here again, then, we submit that the requester must be able to first demonstrate that s/he has (within the past 12 months) had a relationship with the testing organization that would warrant the business undertaking the verification attempt. Such a requirement is also consistent with the Proposed Regulations language that one factor the business should address is, "Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated." The ability of the requester to provide sufficient information about his/her testing event gives the testing organization the most relevant piece of information from which to verify the request.

The ATP also has a grave concern about the validity of the Proposed Regulation (§999.313(d)(1)) that, when a requester for deletion cannot be verified, the request must be treated as one to opt-out of the sale of personal information. Initially, this requirement is predicated on a false assumption that a business even possesses personal information to begin with, compounded by the mistaken assertion that the business automatically is engaged in selling it. Indeed, if a business actually has determined it possesses any personal information about the requester, except for the apparent lack of verification, there would be no absolutely no reason not to respond, even if a denial is required. The business should not be penalized for the failure of the requester to adequately verify himself/herself. In the context of a testing organization, the ATP once again reiterates its view that any valid request (either for access or deletion) must include evidence from the requester that identifies the test s/he took and the location and date of the test administration. Plus, denial may be required by an exception (e.g., the IP rights of the testing organization). Finally, as noted previously, the requester's test results/scores may be owned by someone other than the requester, and thus, the requester may not have the actual authority to delete the information.

Equally important, the ATP objects strenuously to the requirement that a business permit consumers to make requests through an "agent." The Proposed Regulations requires a business to "explain how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf." *See* 999.308(b)(5). We strongly believe that the covered business must not be charged with the legal responsibility to tell consumers how they can

testing organization would have any personal information on that individual. Spurious requests from consumers who cannot provide specific information about their testing event can only lead to unjustified regulatory burdens being placed on these businesses. *See, also*, fn 26 at p.17.

designate an agent – such responsibility must rest totally with the consumer according to standard legal rules of agency. Similarly, it makes no sense for the Attorney General to establish a procedure for a consumer to abdicate his/her direct relationship with a business in order to pursue his/her rights under the CCPA. Not only does this put an unrelated third party (who has no knowledge about the relationship) into the middle of the issue, but it is particularly troublesome when it comes to verification of the identity of the consumer; when a business cannot get direct access to the consumer to provide additional information, it adds serious complications to the process of a business's legitimate attempt to make the verification.²⁶ If the business needs more information which the agent does not have, the agent presumably then has to go back to the consumer, thereby adding unnecessary time and expense to the process. And equally burdensome, the business has to "verify" that the agent actually has authority to represent the consumer, another additional step to the process. It seems to the ATP that if protecting a consumer's personal information is important to the individual, the person should handle a request on his or her own, rather than sharing that personal information with yet another entity.

Finally, the Proposed Regulations impose an affirmative obligation on a covered business that is not found in the CCPA: "A business shall implement reasonable security measures to detect fraudulent identity verification activity and prevent the unauthorized access to or deletion of a consumer's personal information." *See* §999.323(d); *see, also*, §999.313(c)(6). Although the Proposed Regulations do not define what it means to implement "reasonable security measures," the ATP recommends that the final regulations should adopt a definition based on the Cybersecurity Framework (CSF) developed by the US National Institute of Standards and Technology ("NIST"), as well as public voluntary standards in the ISO 27000 family of information technology management standards, or a similar information security framework. The NIST CSF functions to "aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and

²⁶ An "agent" is unlikely to have any information about the testing event, which makes it impossible for the agent to provide the key fundamental information the ATP has proposed should be required as part of the verification. The Proposed Regulations set up opportunities for spurious agent requests. As one ATP Member has informed us, "we've started getting requests from an organization called [deseat.me](#) that seems to have us in their list of suppliers. Typically these requests are for people about whom we have no knowledge and the only information we get is an email address. And it's unclear whether the request has authority. As such, we are forced to waste a lot of time and energy trying to track down these phantom test takers." If a consumer has a legitimate reason to require an "agent" to administer his/her affairs, a legal option is already available through a power of attorney.

improving by learning from previous activities.”²⁷ Under the CSF, a business’s security plan focuses on five basic functions: (1) identifying critical infrastructure and data; (2) protecting your data; (3) detecting potential cybersecurity events; (4) responding to detected events; and (5) recovering capabilities and/or services that were impacted by a cybersecurity event. As a voluntary standard, the CSF also builds on other public voluntary standards, such as ISO/IEC 27000 *et. seq.* (2018), entitled “Information technology — Security techniques — Information security management systems — Overview and vocabulary.”²⁸ The ATP also recommends citing the ISO standards as part of a definition for the term “reasonable security measures.” The ATP contends that aligning the CCPA with these voluntary standards-based security measures will enable covered businesses to adopt security approaches that will be consistent across different states/countries. Accordingly, references to both the NIST CSF and the ISO standards should be included in the final regulations. Continued reliance by the Attorney General’s Office on the checklist of twenty controls defined by the Center for Internet Security previously announced in 2016 as the “minimum level of information security” (*see 2016 Data Breach Report* (Feb. 16, 2016)), should be expanded. The ATP contends that the mere identification of controls does not provide as much value to a business as concrete steps to deal with data protection.

For example, ISO 27001 provides a management system framework of documents, policies, procedures, and controls that enables an organization to systematically evaluate risks to the confidentiality, integrity and availability of its information and put in place appropriate measures to address the risks and follow other requirements of the standard. A key focus is that the standard requires continual improvement over time. Although organizations are free to select security controls based on an evaluation of their own risks, in general there are 114 controls specified in the standard (compared to 20 specified in the 2016 Report).

Related to the needed definition of “reasonable security measures,” the ATP also recommends that the Attorney General should adopt a “safe harbor” provision in the final regulations stating that, if a business uses standardized commercial encryption techniques to protect consumers’ personal information while they are stored and for transmission to the

²⁷ The Cybersecurity Framework was developed in response to Executive Order 13636, which was directed to critical national infrastructure. Nevertheless, the CSF serves as a useful guide for any business to enhance its information security program. Current version 1.1 was released by NIST on April 16, 2018; version 2.0 is under development. Additionally, NIST is developing a “privacy framework” that is expected to be published in 2020.

²⁸ The ISO 27000 family of standards for information security management systems (ISMS) includes ISO 27001 (an audit/certification requirements framework by which a business may respond to information security risks, compliance, and regulatory requirements). ISO 27002 contains voluntary best practices. A new standard that extends both ISO 27001 and ISO 27002 is ISO 27701 (2019), which specifies requirements and provides guidance for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS).

consumer in response to a verified request, that action shall protect the business from any security violations of the CCPA. While “reasonable security measures” do not automatically include the use of encryption, if a business decides to encrypt personal information in its systems (and for communicating personal information back to a consumer), that action will greatly enhance the level of protection afforded such data. A number of different encryption algorithms are used today for a variety of commercial purposes.²⁹ The final regulations should permit a business to select a commercially-available and industry-accepted encryption algorithm based on its own needs and purposes, and so long as the business encrypts all consumer personal information it collects and uses, the safe harbor should apply.

This “safe harbor” is completely justified inasmuch as the CCPA expressly allows consumers to sue businesses when their “nonencrypted or nonredacted 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.” *See* Cal. Civ. Code §1798.150(a)(1). Clearly, the Legislature itself has focused on when “nonencrypted” data is at risk.³⁰ Accordingly, if a business has encrypted consumers’ personal information, it has taken an affirmative action to remove the risk of unauthorized access and disclosure – even if some personal information were illegally obtained, it cannot be used. In recognition of this, the final regulations must be clarified so that a business is not subject to substantial statutory penalties (of between \$100 and \$750 per incident).

5. Issues concerning responses to requests.

When a business cannot verify the identity of a requester, the Proposed Regulations require it to “provide or direct the consumer to its general business practices . . . in its privacy policy.” *See* §999.313(c)(2). This response is redundant, inasmuch as the requester obviously already has access to the privacy policy and all other notice information made available by the business in order to make the request. Therefore, this Proposed Regulation represents yet another instance of unnecessary burdens being placed on the business; it should be deleted.

²⁹ One such algorithm is the Advanced Encryption Standard (AES) used to encrypt and decrypt electronic information, which was approved for use by the federal government in November 2001 and has since been widely adopted by private industry. Today, AES protects everything from classified data and bank transactions to online shopping and social media apps.

³⁰ The ATP submits such a “safe harbor” is intended at a minimum to cover all liability for a security breach – if a business suffers a breach and all personal information is properly encrypted, none of the personal information is actually exposed. Moreover, the “safe harbor” also should apply to both to the “reasonable security measures” requirements in §999.313(c)(6) and §999.323(d).

In our view, the more important aspects of how a business must respond to requests focus on several specific provisions related to denials of requests. Beyond the clear statement (§999.313(c)(4)) that a business shall not provide key sensitive information (i.e., SSN, driver's license, financial account numbers, account password), the Proposed Regulations also state that the business "shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks." See §999.313(c)(3).³¹ The ATP supports this approach and submits that it provides a business with appropriate flexibility to examine all potential impacts of a request for access. See Section 4, *supra*, at pp. 15-17. Because this provision has broad application throughout a covered business's operations, it would be helpful to have the final regulations include use cases to provide further guidance. For example, a request in a testing setting could involve information that would comprise the security of the requester's test information as well as the business's testing system and/or its test products directly. In such a situation, it would be appropriate for the testing organization to deny access.

Similarly, the Proposed Regulations expressly allow the business to deny a request where disclosure would "conflict with federal or state law." See §999.313(c)(5). As the ATP previously discussed (*supra* at p. 4), secure tests and other test materials often are proprietary intellectual property ("IP") of the testing organization (i.e., test items, test manuals, scoring software, test delivery platforms), which the business must protect against disclosure in order to maintain test security and prevent cheating on the test. Thus, if a request for access to a test taker's personal information involves any actual disclosure of the testing organization's IP, the test taker would not be entitled to access such IP and the business will screen out all such IP from what is made available to test taker.³² Although we submit that federal patent, trademark, copyright, and trade secret rights are easily understood as potential "conflicts" with a consumer's right to access, the Proposed Regulations fail to provide any explicit guidance in this area. To avoid confusion on this important point, the ATP recommends that the final regulations should provide details for how a business is permitted to deny some or all of a request when its federal IP rights conflict with the consumer's right to access.³³ See discussion of the impact of a testing organization's IP, *supra* at pp. 2-3.

³¹ Indeed, the Proposed Regulations allow that if a business maintains consumer information that is de-identified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request. §999.323(c)

³² The protection of the testing organization's IP is also consistent with the usual terms contained in the test taker agreement, so every test taker will have been put on notice about this restricted access. As discussed in fn 6, *supra*, test results/scores are likely to be considered by the testing organization to be at least in part covered IP, which will result in denial/partial denial of requests that would entail disclosure of the testing organization's IP,

³³ Except in the case of trade secrets, a business that owns other IP assets will have evidence of those rights issued by the respective governmental body. The final regulations should merely require the business to provide that publically available information to justify its denial of the request.

Finally, denial of requests to delete personal information requires the use of a “two-step” confirmation process as set forth in §999.312(d). The ATP objects to such a process as completely unnecessary. Where no exceptions exist, the requirement is predicated on what can only be described as a “paternalistic” assumption that a consumer does not really understand what s/he is requesting and then places an obligation on the business to essentially double-check whether the consumer really intends to have his/her personal information deleted. In situations where exceptions apply, the ATP suggests that a business will be communicating with a consumer in fully dealing with a denial so any confirmation step is accomplished as part of the denial process. In either case, the burden on the business is exacerbated if an agent is involved. If the consumer elects to request deletion, regardless of how the business verifies the request, there is no need for any confirmatory step. The final regulations should clarify these points.

On a related issue, the Proposed Regulations also require that consumer access responses should be made portable provided technically feasible. *See* §999.313(c)(7). The ATP has several concerns about this language. First, no single standardized or uniform format for interchanging test data exists, so there is no “technically feasible” way to enable a consumer to port test results/scores. But more fundamentally, test takers do not “comparison shop” among testing organizations for a given test, and a high stakes test for a certain purpose is typically only offered by a specific test owner. Thus, a consumer’s right to “portability” – to take personal information from one business and send it to another testing organization – is practically meaningless. Such portability poses a business challenge, as well as a technical challenge, for organizations that develop or deliver tests, considering the issues of test security, possible conflicts of interest and protection of intellectual property. Thus, the ATP submits that a testing organization would be within its rights to deny a request for test results/scores by arguing that: (1) data portability is not technically feasible; (2) its company assets (e.g., intellectual property rights) must be protected; and (3) the rights of an entity that is paying for the individual test taker’s assessment (e.g., employer) or a test copyright holder (e.g., test author) must be protected.

6. Issues concerning time to respond to requests.

For the requests to know and to delete, a business must acknowledge receipt within 10 days, providing additional information about how the business will process the request. A business must respond within the 45-day deadline set forth in the CCPA (with an additional 45-day extension if the business gives notice to the consumer); the Proposed Regulations clarify that the timeline begins to run upon receipt of the request, “regardless of time required to verify the request.” Given this already compressed timeline, the ATP recommends that the final regulations drop the required acknowledgement – the business has enough to do to begin the verification process and prepare a response within the 45-day period. Moreover, since the consumer will receive a substantive response in most instances within the 45-day period (or a notice of the extension), the value of an acknowledgement is questionable.

7. Issues with respect to the use of “Service Providers”.

The ATP generally endorses the Proposed Regulations concerning the definition of “service providers” (*see* §999.314). However, the Proposed Regulations do not go nearly far enough in identifying the scope of how many service providers operate. This is especially true in the testing industry, where a testing organization that is not directly selling testing services to consumers and has a contractual relationship with the controller automatically should be deemed to be a “service provider.” As such, when a business provides various testing services to or on behalf of the organization that actually owns the test and collects the personal information of consumers, such a business functions as a “service provider.” The Proposed Regulations seem to accept this position by providing: “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.” *See* §999.314(b).

However, the Proposed Regulations are not consistent with the CCPA on several key points. Accordingly, in order to eliminate any confusion, the ATP contends the Attorney General should make changes in the final regulations to fix those discrepancies.

Critically, while the CCPA indicates that a service provider need not reply to consumers’ rights requests, the Proposed Regulations state that “a service provider must provide the specific basis for denying requests from consumers regarding their personal information collected or maintained by the service provider on behalf of the business.” *See* §999.314(d). Yet, the same section of the Proposed Regulations also would require that a service provider direct consumers to submit their requests to the relevant business and to provide the consumer with the contact information for that business “when feasible.”³⁴ Equally confusing, the Proposed Regulations also attempt to clarify that an entity can be a service provider to the extent it collects personal information from consumers as directed by a business as well as where the service provider acts on behalf of another entity that is not a “business” under the CCPA, provided the entity

³⁴ For example, it is common for a testing service organization to provide online software which can be used to deliver to, and score tests for, California consumers. Such an organization is a service provider to test publishers, test sponsoring organizations, or employers. When a consumer requests information from the service provider, it would be inappropriate for the service provider to share that information, but instead it should pass the request to the testing organization that controls the testing event, including making the decisions about the collection and use of personal information. This result is required partly because the service provider may not be able to identify the consumer and partly because the consumer has a contractual relationship with the controlling business, not the service provider. The final regulations should be modified to make this relationship sufficiently clear.

otherwise meets the requirements for a service provider. *See* §999.314(a) and (b).³⁵

Unfortunately, these Proposed Regulations create more doubt and confusion than they achieve clarity in this area. Because of this confusion, the ATP is concerned that testing organizations that are engaged in a variety of services, often performed for owners of tests and testing programs, will be viewed by consumers – and thus, by the Attorney General – as having the primary relationship with a consumer and therefore, be deemed to be the controlling business. This confusion is likely to go unresolved because the Proposed Regulations do not adequately take into account the contractual relationships that exist with a variety of service providers (e.g., test delivery, test scoring, test security) (*see supra.* at 3-5).³⁶ As we noted, it would be useful for the final regulations to adopt (or adapt) the definitions from the GDPR for the entity that determines what personal information is collected and how it is used (i.e., the “controller”) and the entity that follows the instructions of the controller in processing personal information on the controllers behalf, even if that entity may be collecting the information directly from consumers. Absent this clarification, the ATP is concerned that the primary responsibilities for compliance with the CCPA may improperly be shifted away from the controlling business to service providers/processors.

Finally, the Proposed Regulations fail to provide any guidance on the requirements for a “data broker” that were added in the amendments from AB 1202. That amendment defined a data broker as a “business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship, subject to specified exceptions.” In light of that amendment, and the potential for mistakenly requiring a testing organization liable to register as a “data broker,” the ATP reiterates its previous comments about how a testing organization shares personal information, especially test takers’

³⁵ Compared to these inconsistent statements, we note the clarity surrounding the following point: “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.” Despite the apparent straightforwardness of this language, it is still inappropriately vague as to identifying the scope of roles a business may legitimately play as a service provider. The final regulations should provide additional clarity acknowledging the broad scope of services related to an underlying business agreement that should be allowed.

³⁶ The Proposed Regulations clarify that a service provider may “combine personal information received from one or more entities ... to detect data security incidents, or protect against fraudulent or illegal activity. That language perfectly fits the business operations of some testing organizations that provide test security services.

test results/scores with its partners and service providers in order to fulfill its responsibilities to the consumer (*see supra.* at pp. 3-4 and 12-14). In other circumstances, where the third parties involved in the provision of the overall testing services may not have a “direct relationship” with the test takers, that does not make the controlling business a “data broker.” Nor is the third party a “data broker” by virtue of collecting personal information on behalf of the testing organization. First, neither the testing organization nor the third party service provider is not selling or disclosing test taker information for any marketing purpose, but are merely sharing information necessary to enable the other business(es) to complete its portion of the testing services for the specific consumer. Second, both the underlying testing organization and any service providers/partners are part of the “common interest” group providing the testing services to the consumer, so a “direct relationship” should be inferred to exist for each entity engaged in the process.

8. Issues with recordkeeping

The Proposed Regulations require that a business keep records for at least 24 months and include the following information: request data, nature of request, manner of submission and basis for any denial. §999.317(b).³⁷ In addition, businesses that “alone or in combination” (a phrase that is undefined and unclear) receive or share records of 4 million or more California residents would be required to compile detailed metrics on the value of different requests under the statute and median number of days to respond to each, as well as any signed declarations obtained from consumers as part of the consumer verification process.³⁸ §999.317(g).

The Proposed Regulations require a business to post this information as part of its privacy policy – or provide a link to the information from its privacy policy. §999.317(g)(2). This approach represents a novel requirement in U.S. privacy law, and represents an overly-

³⁷ Separately, the Proposed Regulations require that a business provide adequate training for employees on “all of the requirements in the regulations.” *See* §999.3179(a). The ATP supports this mandate in the context of enabling a testing organization to deal with the CCPA along with other state/country-specific laws/regulations in the United States, as well as foreign laws and regulations (e.g., GDPR).

³⁸ We note that the determination as to whether a business has 4 million records suffers from the same problem as for the 50,000 California consumers eligibility requirement – it is often difficult or even impossible to know the residence of some test takers. *See* Comment Section 1, *supra.* at p. 8. As such, the eligibility test for requiring these metrics is unreasonably vague. Moreover, the purpose seems to be more predicated on enforcing the CCPA than to producing any benefit for California consumers. Furthermore, we see no relationship between the number of requests a business may experience to any level of lack of compliance under the CCPA or equally, to any bad reputation a businesses may seem to acquire due to the number of requests it receives.

burdensome and costly mandate for each business to comply.³⁹ When those costs are compared with the largely illusory benefits to consumers of having access to such metrics, the ATP fails to understand what relevance a 2-year record of requests/outcomes has to the business's ability to protect consumer personal information, or even to adopt reasonable procedures for handling consumer requests. Instead, this requirement seems aimed more to giving the Attorney General CCPA enforcement information to use during an enforcement investigation. As such, the ATP submits that the final regulations should drop the requirement to provide this information directly or indirectly through a business's privacy policy.

Especially if the objective is to require the business to retain enforcement related data, it is very troubling that apparently a business may not use its own data for any purpose beyond this reporting. §999.317(c). In reality, a business needs to be able to access all such information about its handling of all consumer requests specifically for the purpose of documenting what it did if the same consumer comes back to the business to complain about what was done/nor done. If the business does not have legitimate access and use to its own business records, it will be unable to document the previous actions taken under the regulations. Accordingly, the ATP recommends that the Proposed Regulations be modified to clarify that a business may use its records as part of its procedures for handling requests and to evaluate and modify its processes.

10. Issues with enforcement.

The ATP is very concerned about how its Members can be in a position to comply fully with whatever final regulations are published, especially inasmuch as it seems highly unlikely that the regulations will not be finalized until the Spring of 2020, which will be only a few months before the presumed July 1 enforcement date. As mentioned earlier, many ATP Members have been adjusting their privacy policies over the past two years, first because of the GDPR, and now because of the CCPA. Nevertheless, until final regulations are published, there are uncertainties in how some issues will ultimately be resolved.

The initial cost of compliance with the CCPA for each business has been estimated at between \$50,000 and \$2 million (or more), depending on the size of the business. Accordingly, ATP Members are likely to rely on their existing data privacy and information security policies until the final regulations are announced. But even that level of uncertainty pales in comparison to the press conference statement by the Attorney General on October 10, 2019, which seemed to indicate he might take enforcement actions for noncompliance between January 1 and July 1, 2020. For obvious reasons, the ATP strongly urges the Attorney General to forestall any enforcement until businesses have seen and can understand the full requirements of the final regulations and can have a reasonable opportunity to finalize their compliance plans. In our

³⁹ To the best of the ATP's knowledge, the GDPR does not require such publication, nor does the new privacy law in India. This requirement is overly burdensome and will cause a testing organization to expend resources to comply that would be better used for protecting the privacy of personal information.

opinion, a six-month delay in enforcement, until January 1, 2021, would make sense. We believe this recommendation is appropriate, because with the 12-month “look-back” period, such an enforcement action commenced on that date would fully enable the Attorney General to take into account all aspects of a business’s compliance after the statutory effective date of January 1, 2020.

CONCLUSION

On behalf of the international testing industry, the ATP has provided comments on the Proposed Regulations for implementing the CCPA. We have articulated a number of unique circumstances that are common in the testing industry. We have indicated that many testing organizations are smaller/medium-sized businesses. Together, we believe these reasons justify modification of the Proposed Regulations when balanced against the rights of individual test takers as consumers.

Among the significant positions set forth in these comments are the following recommendations:

- The final regulations must clarify the definition of “sale” to avoid application of overly-prescriptive privacy requirements to situations where the sharing of an individual’s test results/scores with service providers of the testing organization, which would defeat the very purpose the consumer has in taking the test in the first place.
- The final regulations must clarify the broad scope of services provided by a “service provider” that are completely related to the underlying contract with the covered business, especially in the testing industry where a variety of component testing services are necessary to the accomplish the underlying contract with a consumer for testing services.
- The final regulations must clarify that test results/scores are not to be treated as “personal information.”
- The final regulations must clarify that the intended purpose of the CCPA is to limit the sale, use, and distribution of personal information for commercial marketing/advertising purposes.
- The final regulations must remove and/or reduce the incredibly complex, overly burdensome procedural requirements, which actually defeat the intended purpose of CCPA.
- The final regulations must clarify that the intent of the CCPA is to inform consumers of a business’s privacy practices, regardless of whether the notice comes from the underlying contracting business or one of its service providers.
- The final regulations must not hamper a business’s efforts to protect consumer privacy in a meaningful way or to divert resources away from data protection and compliance.
- The final regulations should more closely parallel those of GDPR, especially the definitions of, and distinctions between, data controller and data processor, in order to

maintain proper accountability for compliance with the organization that has the underlying substantive relationship with the consumer.

- The final regulations must highlight the distinction between inferences made about a person for marketing purposes, and those made in the process of providing testing services (i.e., analyzing and reporting test scores).
- The final regulations must clarify how to calculate the \$25 million revenue and the 50,000 California consumer thresholds (as well as the 4 million consumers for the expanded metrics).
- The final regulations must require that a consumer provide request verification information about his/her relationship with a business, especially where a testing organization is involved (by providing information about the test that was taken, along with the date and place where the test was taken).
- The final regulations must establish an effective “safe harbor” for a business that encrypts consumers’ personal information.
- The final regulations must remove the ability of a consumer to use an agent outside of a traditional Power of Attorney.
- The final regulations must delete and/or modify the record keeping requirements, which in themselves have no benefit to consumers, and to allow a business to use such information to improve its own compliance with the CCPA.
- The final regulations must address and provide guidance on how to handle employee (and job applicant) personal information and business contact information during 2020.
- The final regulations must be published and allowed to be implemented by covered businesses before any enforcement should occur.

Thank you for your attention to the important issues raised by the testing industry about the Proposed Regulations implementing the CCPA by affected members of the testing industry located within and outside of California. The ATP would be pleased to answer any questions the Attorney General's Office may have in response to these comments, including to do so in a face-to-face meeting. For any follow up, please contact our General Counsel at the number or email address shown below.

Sincerely,

ASSOCIATION OF TEST PUBLISHERS



William G. Harris, Ph.D.
CEO
601 Pennsylvania Ave., NW
South Bldg., Suite 900
Washington D.C. 20004

John Weiner, Incoming Chairman of the Board of Directors
Chief Science Officer
PSI Services LLC
611 N. Brand Blvd., 10th Flr.
Glendale CA 91203



Alan J. Thiemann
General Counsel
Law Office of Alan J. Thiemann
700 12th Street, NW, Suite 700
Washington, DC 20005



Message

From: Grant, Jeremy A. [REDACTED]
Sent: 12/6/2019 3:15:52 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments of the Better Identity Coalition on CCPA Proposed Regulations
Attachments: Better Identity Coalition Comments on CCPA Regs - Dec 2019.pdf

The Better Identity Coalition appreciates the opportunity to provide comments to the California Department of Justice on the Proposed Regulations for the California Consumer Privacy Act (CCPA).

As background, the Better Identity Coalition is an organization focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication. Our members – 24 companies in total – are recognized leaders from different sectors of the economy, encompassing firms in financial services, health care, technology, fintech, payments, and security. The coalition was launched in February 2018 as an initiative of the Center for Cybersecurity Policy & Law, a non-profit dedicated to promoting education and collaboration with policymakers on policies related to cybersecurity. More on the Coalition is available at <https://www.betteridentity.org/>.

As we detail in the attached response, the shortcomings of many commonly used identity verification and authentication tools create challenges with certain aspects of privacy legislation and regulation; these shortcomings are likely to put consumers and businesses at risk.

We greatly appreciate your offices' willingness to consider our comments and suggestions and welcome the opportunity to have further discussions. Should you have any questions on our feedback, please contact the Better Identity Coalition's coordinator, Jeremy Grant, at [REDACTED] or the email below.

Jeremy Grant | Managing Director, Technology Business Strategy | Venable LLP

[REDACTED]
600 Massachusetts Avenue, NW, Washington, DC 20001

[REDACTED] | www.Venable.com

This electronic mail transmission may contain confidential or privileged information. If you believe you have received this message in error, please notify the sender by reply transmission and delete the message without copying or disclosing it.



**Comments to the California Department of Justice
Proposed Regulations for the California Consumer
Privacy Act (CCPA)**

December 2019

The Better Identity Coalition appreciates the opportunity to provide comments to the California Department of Justice on the Proposed Regulations for the California Consumer Privacy Act (CCPA).

As background, the Better Identity Coalition is an organization focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication. Our members – 24 companies in total – are recognized leaders from different sectors of the economy, encompassing firms in financial services, health care, technology, fintech, payments, and security.

The coalition was launched in February 2018 as an initiative of the Center for Cybersecurity Policy & Law, a non-profit dedicated to promoting education and collaboration with policymakers on policies related to cybersecurity. More on the Coalition is available at <https://www.betteridentity.org/>.

In the summer of 2018, we published “[Better Identity in America: A Blueprint for Policymakers](#)” – a document that outlined a comprehensive action plan for government to take to improve the state of digital identity in the U.S. Privacy is a significant focus: the Blueprint detailed new policies and initiatives that can help both government and industry deliver next-generation identity solutions that are not only more secure, but also better for privacy and customer experiences.

As a Coalition, we highlighted the concept of privacy as it relates to identity in our Policy Blueprint, noting:

The privacy implications of existing identity tools – specifically the ways in which the inadequacy of some identity systems has placed consumers at risk – have made clear that consumers need better identity solutions that empower them to decide what information they share, when they share it, and in what context.

Accordingly, new identity proofing solutions should be crafted with a “privacy by design” approach. That means:

- *Privacy implications are considered up front at the start of the design cycle – and protections are embedded in the solution architecture*
- *Identity data is shared only when consumers request it*
- *Identity data that is shared is only used for the purposes specified*
- *Consumers can request release of information about themselves at a granular level – allowing them to choose to share or validate only certain attributes about themselves without sharing all their identifying data*

Our Policy Blueprint also highlighted the challenges the country faces when it comes to digital identity, particularly when it comes to the ways attackers have caught up with many legacy identity security tools used for both authentication and identity verification.

With regard to authentication, we noted:

There is no such thing as a “strong” password or “secret” SSN in 2018 and America should stop trying to pretend otherwise. The country needs to move to stronger forms of authentication, based on multiple factors that are not vulnerable to these common attacks.

With regard to identity verification, we highlighted how attackers have caught up with commonly-used knowledge-based tools, noting:

Adversaries have caught up with the systems America has used for remote identity proofing and verification. Many of these systems were developed to fill the “identity gap” in the U.S. caused by the lack of any formal national identity system – for example, Knowledge-Based Verification (KBV) systems that attempt to verify identity online by asking an applicant several questions that, in theory, only he or she should be able to answer. Now that adversaries, through multiple breaches, have obtained enough data to defeat many KBV systems; the answers that were once secret are now commonly known. Next-generation solutions are needed that are not only more resilient, but also more convenient for consumers.

While these solutions were helpful for several years, they also became targets of attack for adversaries. Their goal has been simple: steal identity data in order to aggregate and analyze it – and then turn it against systems that used knowledge of personal data as a means of protection.

A number of Better Identity Coalition members also have seen stepped-up attacks on these knowledge-based systems and learned that merely answering the questions correctly cannot guarantee authenticity; one financial institution commented that if someone correctly answers a knowledge-based quiz too quickly, it is a signal that they might be dealing with an attack from a “bot” rather than a real human being.

As we detail in the sections below, the shortcomings of many commonly used identity verification and authentication tools create challenges with certain aspects of privacy legislation and regulation.

Better Identity is essential to improving privacy and data security

In a world where commerce is increasingly digital, well-designed identity solutions are becoming increasingly important in achieving good privacy outcomes.

- Identity is far and away the most commonly exploited attack vector in cyberspace; 81% of 2016 breaches leveraged compromised credentials to get into systems. Strong identity solutions help protect consumers’ data and guard against identity theft.
- Strong identity solutions are also needed to enable consumers to securely authorize third parties to access their personal data at a granular level (allowing an organization to access some, but not all of their data, and potentially for a limited time period), as well as grant

delegated access rights (when, for example, a consumer needs to authorize a third party access certain data on their behalf).

- New legal mandates to grant consumers the right to know, correct or delete their data depend on the existence of well-designed, robust, digital identity systems.

In practical terms, delivery of these new rights is largely dependent on the ability of the organization holding that data to easily know whether the person demanding access to that data is actually who he or she claims to be. In order to deliver access, correction and deletion, organizations must be able to:

- 1) Validate the identity of a consumer making a request to access or correct their information,
- 2) Securely authenticate them into the system – while keeping others out, and
- 3) Connect them to their information

When properly designed, Identity becomes the “great enabler” of better privacy. But without robust, secure and resilient digital identity systems, any new legal requirement for organizations to deliver access, correction and deletion is likely to inadvertently create a new attack vector for hackers and other adversaries to exploit in their race to steal personal data.

The risks of inadequate identity verification solutions were detailed this summer in a presentation at the Blackhat conference entitled *GDPArrrrr: Using Privacy Laws to Steal Identities*,¹ which detailed how an adversary could exploit GDPR’s new “Right of Access” to gain unauthorized access to a consumer’s data. As we detail below, we are concerned that the proposed regulations to implement CCPA may open up similar attack vectors in California.

Note that CCPA is a law where our members, given their diversity, may have a diversity of views. For this reason, our comments on the proposed regulations are limited to those areas that touch on identity.

We offer the following comments on the proposed regulations:

- 1. The proposal in §999.313 (c)(7) and §999.324 that companies should rely on passwords to verify the identities of consumers asking to see their personal data is likely to put consumers at risk.**

Passwords offer very little security. More than nine billion accounts and 555,278,657 distinct real-world passwords have been compromised, according to the HavelBeenPwned.com

¹ <https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf>

website.² If possession of a password is all that is needed to get a company to release a consumer's data (per the proposed CCPA regulations), Californians should be prepared for criminals and hackers to exploit millions of already-compromised accounts and passwords to access their personal data.

The issue is that the proposed CCPA regulations would make compromised passwords more valuable: whereas today a compromised password allows a criminal to access the account associated with that password, the proposed CCPA regulations would expand what a criminal can do with a compromised password – allowing that criminal to not only access the account, but also demand that a company share all of the information associated with that account.

Given that many companies have customer data that is not readily available through their standard, customer-facing account portals, this will have the impact of increasing the risk to consumers associated with compromised passwords.

Use of Multi-Factor Authentication (MFA) is the best way to mitigate the threats associated with passwords. At the Federal level, the government recognized that release of personal information with nothing but a password created serious risks; Executive Order 13681, issued by President Barack Obama on October 17, 2014, stated *"All agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication, and an effective identity proofing process, as appropriate."*³

California should look to establish a similar baseline of consumer protection by embracing this Federal standard.

Specifically, California should require that consumer requests for data be validated against Authentication Assurance Level 2 (AAL2), as defined by NIST in its Digital Identity Guidelines.⁴ AAL2 details multiple ways that accounts can be protected with MFA, using a combination of knowledge-based (i.e. passwords), inherence-based (i.e., biometrics) and possession-based (i.e. security keys or certificates on a laptop or mobile phone). The Guidelines also make clear that some MFA tools like SMS should not be used, given that attackers have figured out several ways to compromise MFA codes delivered over SMS.

Establishing NIST AAL2 as the standard for identity verification would align California with a well-accepted national standard that sets a meaningful bar for security and would provide clarity to

² For more details, visit www.HaveIBeenPwned.com. This is a free service that aggregates stolen usernames and passwords from major, publicly known breaches and offers a service to notify individuals if their password or data was stolen in a breach. The service also runs a "Pwned Passwords" service that supports the NIST recommendation that user-provided passwords be checked against existing breaches.

³ See Section 3 of <https://obamawhitehouse.archives.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions>

⁴ See NIST Digital Identity Guidelines – Authentication and Lifecycle Management at <https://pages.nist.gov/800-63-3/sp800-63b.html>

businesses looking for firm guidance on how authenticate consumers requesting access to their data.

2. Suggestions in §999.324 that companies mitigate the threat of compromised passwords through use of security analytics tools are sound – but other parts of CCPA may allow consumers to opt out of having companies use these tools to protect their accounts.

The proposed regulations seem to recognize the vulnerabilities associated with passwords, suggesting that companies should be looking to mitigate the threat of compromised passwords by using security analytics tools to detect *“If a business suspects fraudulent or malicious activity on or from the password-protected account.”* (per §999.324 (b)).

We were pleased to see this. At a time when identity is far and away the most commonly exploited attack vector in cyberspace, security analytics solutions are one of the best tools industry has to help guard against these kinds of attacks and prevent fraud. Many Chief Information Security Officers (CISOs) look to the use of these products as a best practice and are increasingly deploying them alongside traditional “strong authentication” products to protect against breaches.

But use of security analytics tools requires data – and CCPA itself is vague as to whether consumers (or fraudsters posing as consumers) could request their data not be used for security and fraud prevention.

As backdrop, Europe’s General Data Protection Regulation (GDPR) did a decent job here: while it limits the collection of data in many circumstances, it also highlights that when it comes to protecting security and preventing fraud, there are cases where an entity may have a “legitimate interest” in processing personal data – including in cases where such data can be used to deliver and develop secure authentication or verification capabilities and technologies. This “carve out” has allowed the use of data-based security and consumer protection solutions to flourish.

In contrast, CCPA has more ambiguous language that may allow consumers to opt out of having their data used to protect against malicious, deceptive, fraudulent, or illegal activity.⁵ This ambiguity is already inhibiting the deployment of security analytics tools that can guard against

⁵ Specifically, §1798.120 discusses a consumer’s right to opt out of the sale of their personal information – but does not create any exception for *“[d]etecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.”* It is unknown whether these omissions were deliberate or a drafting error – the inclusion of a security and fraud prevention exception in other parts of CCPA leads one to believe it was the latter. Many attorneys and companies, however, have interpreted this clause to mean that there is nothing that would prevent a consumer (or someone posing as one) from demanding that a company refrain from collecting or using personal information in to protect against fraud, or – in the case of security vendors – from selling products that make use of that information to help other companies protect themselves.

the kind of password-based attacks the proposed regulations seem to anticipate, placing consumers at risk.

Given the ambiguities of CCPA, the best thing the California Department of Justice could do here would be to clarify the final regulations to state:

- 1) Businesses should, wherever feasible, be using security analytics tools to detect suspect fraudulent or malicious activity on or from password-protected accounts, and
- 2) Businesses should be free to use data in security analytics tools to assure security and prevent fraud, provided that they are not collecting information for “security” and then turning around and using it for other purposes.⁶

This clarification would address a much-needed area of concern in CCPA, and would be consistent with language in the CCPA definitions section (§1798.140(d)(2)) which states that: *“Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity”* is a “business purpose.”

3. The proposed process for companies to verify consumer identity in situations where the consumer does not have a password-protected account is based on an obsolete “knowledge-based” approach that will put consumers and businesses at risk.

As drafted, §999.325 of the regulations call for companies that require a “high degree of certainty” on identity verification to rely on *“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.”*

There are two problems with this approach:

- a) The National Institute of Standards and Technology (NIST) has specifically cautioned against use of Knowledge-Based Authentication (KBA). Per NIST guidance⁷:

Knowledge-based authentication (KBA), sometimes referred to as “security questions,” is no longer recognized as an acceptable authenticator by SP 800-63. This was formerly permitted and referred to as a “pre-registered knowledge token” in SP 800-63-2 and earlier editions. The ease with which an attacker can discover the answers to many KBA questions, and relatively small number of possible choices for

⁶ Note that Facebook earlier this year was revealed to have been collecting phone numbers under the auspices of “security” only to also be using the data for marketing purposes. See <https://techcrunch.com/2018/09/27/yes-facebook-is-using-your-2fa-phone-number-to-target-you-with-ads/>. We believe this sort of behavior should be banned.

⁷ See <https://pages.nist.gov/800-63-FAQ/>

many of them, cause KBA to have an unacceptably high risk of successful use by an attacker.

California would thus be establishing a regulation calling for an approach to identity verification that conflicts with national standards.

- b) This proposed process is not based on any standard, nor is there any way to measure its efficacy.

The threshold of what is “reliable for the purpose of verifying the consumer” leaves a great deal open to interpretation – and creates multiple opportunities for impersonation and error.

The challenges businesses and governments have faced in determining what data elements are “reliable for the purpose of verifying the consumer” have existed for years, with little resolution. Companies have struggled to find data sets that are 1) unique to a user, 2) secret (and thus meaningful), and 3) easy enough to remember that they are usable as a security tool.

These challenges are so acute that security researchers years ago created a flowchart to parody them, with the use case of trying to establish whether noted MC Rob Base – of legendary hip-hop duo Rob Base and DJ EZ Rock – is in fact who he claims to be.

As noted in Figure 1, an identity verification process can be constructed for Rob Base with four distinct elements, based on the opening verse of the 1988 hit “It Takes Two.”⁸

The four pieces of personal information depicted in Figure 1 meet criteria 1 and 3 – they are unique to the user (at least in aggregate) and easy enough for the user to remember. However, they are not secrets – and thus not useful for security purposes.

Moreover, even if the data points were secrets, the idea is that they are “shared secrets” known by both the consumer and a business. The last ten years have demonstrated that most security solutions based on

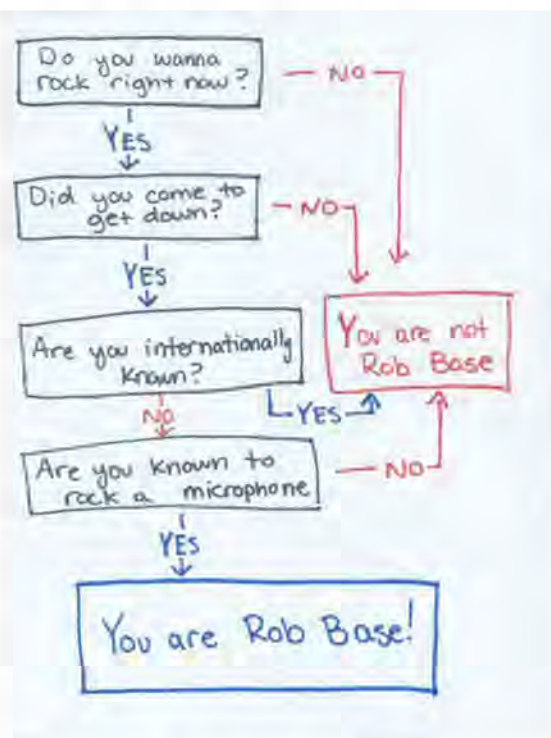


Figure 1: “Are You Rob Base?”

⁸ See <https://www.youtube.com/watch?v=phOW-CZJWTO>

“shared secrets” are doomed to fail, as a secret possessed by two parties tends not to stay a secret for long. Attackers have caught up with these solutions. The examples provided in the “illustrative scenarios” in §999.325 are examples of so-called “secrets” that are not reliable for security purposes.

In summary, while it takes two to make a thing go right, California setting a threshold of three data elements to prove identity is going to go wrong. The “Are You Rob Base” approach to identity verification should not be enshrined in California regulations.

We note that § 999.325 of the draft regulations do call for a consumer to provide a “signed declaration under penalty of perjury” alongside their assertion that they are “who they claim to be” – but we do not believe this will help. If a criminal is trying to impersonate someone to steal their data, it is unlikely that they will be worried about a perjury charge at a time when they are already breaking the law.

While we believe this proposed approach to identity verification is problematic, there are two steps that California could take to improve them – better protecting consumers and businesses alike.

1. Rather than call for businesses to “match 3 pieces of data” – a non-standard approach that will open California consumers and businesses to increased identity fraud – California should instead require that consumer requests for data be validated against Identity Assurance Level 2 (IAL2), as defined by NIST in its Digital Identity Guidelines.⁹ Establishing NIST IAL2 as the standard for identity verification would align California with a well-accepted national standard that sets a meaningful bar for security, and provide clarity to businesses looking for firm guidance on how to validate the identities of consumers requesting access to their data.

An added benefit of aligning California regulations with this NIST standard is that doing so will prevent the minimum bar from being tied to a static standard or technology, as the NIST standard is updated every few years to reflect both new technology advances, as well as evolution of threats against identity solutions. Thus, as new methods to achieve IAL2 compliance are devised, the California regulation will automatically support their adoption – rather than being tied to any particular technology or methodology. Threat is always evolving, and a regulation that calls for a specific technology or approach may, in fact, put consumers at risk when adversaries catch up to what was acceptable at the time the rule was written.

⁹ See NIST Digital Identity Guidelines – Enrollment and Identity Proofing Requirements at <https://pages.nist.gov/800-63-3/sp800-63a.html>

2. Participate in the Driver's License Data Verification service (DLDV).¹⁰ DLDV is of the best tools in the market for remote identity verification – created and supported by more than 40 states to help commercial entities validate driver's license and state ID card information to verify identity and combat identity fraud. Government is the only entity that authoritatively confers identity; government is thus in the best position to verify the identities that it issues.

Note that DLDV is designed up front to protect privacy: states do not share or reveal personal information through DLDV, they only provide a "Yes/No" answer as to whether identity data provided to open a new account matches what the state has on record, and only with a consumer's consent. This consent-based approach enhances privacy and protects against the unauthorized disclosure of Californians' information.

California is one of a handful of states that do not yet participate in DLDV – this means that California businesses are at a disadvantage when it comes to authenticating identity relative to 40 other states. At a time when California businesses are being asked to take on new identity verification obligations that exceed those imposed on businesses in other states, the least the state could do would be to allow California businesses the ability to validate identities against DLDV.

4. Other items

In addition to the points above, there are a number of other aspects of the proposed regulations where specific provisions or wording are problematic. These include:

- § 999.313 (Responding to Requests to Know and Requests to Delete). Subsection (d) of this section states:
For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified and shall instead treat the request as a request to opt-out of sale.

As written, this would require businesses to convert an unverifiable request to delete into an unverifiable request to opt-out. If an identity cannot be verified, it may be a sign of fraud. Given this, why should it be treated as an authoritative request that binds a business to take action?

- § 999.324 (Verification for Password-Protected Accounts). This section would require that a business *"require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data."* While we have concerns about the ways in which password-protected accounts may be exploited under this section, if someone has

¹⁰ The DLDV is owned and operated by the American Association of Motor Vehicle Administrators. See: <https://www.aamva.org/DLDV/>

already authenticated into their account, it is not clear what security value can be gained by requiring someone to authenticate again before a deletion.

We greatly appreciate your offices' willingness to consider our comments and suggestions and welcome the opportunity to have further discussions. Should you have any questions on our feedback, please contact the Better Identity Coalition's coordinator, Jeremy Grant, at

[REDACTED]

Message

From: Frank Salinger [REDACTED]
Sent: 12/6/2019 1:40:43 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Toni A. Bellissimo [REDACTED]
Subject: Comments of the Card Coalition
Attachments: CCccpaAGFINALsigned.pdf

Attached is the comment letter filed on behalf of the Card Coalition relating to proposed rules implementing the California Consumer Privacy Act. The Coalition appreciates the opportunity to share its views on this crucial matter.

Frank M. Salinger

Public Policy Law Practice
[REDACTED]

www.franksalinger.com

For my tweets about politics: <https://twitter.com/KStreetLawyer>

Notice: If received in error, please delete and notify sender. Sender does not waive confidentiality or privilege and use or transmittal of any content is prohibited. Please take notice that the transmission of an email inquiry itself does not create an attorney-relationship.



Card Coalition P.O. Box 802 Occoquan, VA 22125-0802 ☎ 703.910.5280

December 6, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013
Filed via email at PrivacyRegulations@doj.ca.gov

Re: California Consumer Privacy Act Rulemaking

Dear Attorney General Becerra:

The Card Coalition respectfully submits these comments in response to the Notice of Proposed Rulemaking published on October 12, 2019 relating to 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” or “Act”).¹

I. POLICY CONCERNS

a. The Final Regulation Should Be Delayed

Prior to the publishing of the proposed rulemaking, the underlying statute was amended on five occasions.² At this writing, it also appears likely that a ballot initiative will qualify for the 2020 election making further changes to the CCPA and imposing new requirements on your office.³

Given how rapidly technology, and individual expectations in light of that technology, is evolving, as well as the difficulty of responding to ever-changing referendum language, going forward with this rulemaking is precipitous.

¹ The Card Coalition consists of major national card issuers and related companies with an interest in state legislative, executive, and regulatory activities affecting the credit card industry and consumers. We are the only national organization devoted solely to the credit card industry and related legislative and regulatory activities in all 50 states. To learn more about the Card Coalition and our members, please visit www.cardcoalition.org.

² CA AB 25 (Chapter No. 2019-763), CA AB 874 (Chapter No. 2019-748), CA AB 1146 (Chapter No. 2019-751), CA AB 1355, (Chapter No. 2019-753); and CA AB 1564 (Chapter No. 2019-759).

³ 2020 Ballot Initiative No. 19-0021.

As you will see below, we believe a number of the proposed regulations make substantive changes beyond the scope of CCPA, which are better addressed through the legislative process or by referendum.

With this current political backdrop, we urge you to postpone the final regulation until the totality of the CCPA takes effect and, instead, issue practical, compliance-based guidance as the business community works to develop and implement processes and procedures to comply with the legislative intent of the CCPA.

b. The CCPA and Entities Subject to Comprehensive Privacy Regulation

The Card Coalition recognizes the importance of consumer privacy in today's increasingly technology-based business world. While some industries lack sufficient regulation, the payment card industry is subject to comprehensive federal regulation, including a robust and effective privacy regime. We believe policymakers should recognize that the global payment system requires transparent rules of the road on a national scale.

While we recognize the challenges inherent in crafting regulations that will apply to the entire business community, our comments are informed by the fact that privacy related to payment cards is subject to an existing comprehensive statutory and regulatory regime protecting the privacy of consumer information held by financial institutions.⁴

For example, unlike many types of businesses that hitherto have not been subject to oversight relating to privacy, financial institutions are already subject to the following relevant federal statutes. The Gramm-Leach Bliley Act of 1999 ("GLBA") already protects the privacy of consumer information held by financial institutions. The GLBA requires companies to provide consumers privacy notices that explain information-sharing practices and give consumers the right to limit sharing of some personal information.⁵ Similarly, the California Financial Information Privacy Act (CFIPA), the state equivalent to GLBA, additionally regulates these entities. We note the CFIPA is listed in the exemptions provided in Section 1798.145(e).

The GLBA also distinguishes between "consumers" and "customers," the latter having an ongoing relationship with their financial institution. Consumers receive a privacy notice from a financial institution only if the company shares the consumers' information with unaffiliated companies; while customers must receive notices regularly.

⁴ See, e.g., Gramm-Leach Bliley Act of 1999 (Title V of the Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999) (codified at 15 U.S.C. §§ 6801, 6809, 6821, and 6827) (full-text); 12 C.F.R. part 1016 (implementing privacy rules pursuant to GLB Act); Right to Financial Privacy Act of 1978 (RFPA), Pub. L. No. 95-630, § 1114, codified at 12 U.S.C. § 3401 et seq. (1978) ; *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (2005); *Consumer Compliance Risk Management Guidance on Social Media* (2013) ; *Authentication in an Internet Banking Environment* (2015).

⁵ Ibid.

These privacy notices are clear, conspicuous, and accurate statements of the financial institution's privacy practices. They include what information the financial institution collects about its consumers and customers, with whom data is shared, and how it protects and safeguards the information. The notice applies to "nonpublic personal information" the financial institution gathers and discloses about its consumers and customers; in practice, that information may be most—or all—of the information a company has about them. Moreover, government regulators have issued design templates for the notices⁶, which are a safe harbor for financial institutions that use them – virtually all do.

Consumers and customers alike may opt out of having their information shared with certain third parties or the financial institution's affiliated companies. The law further restricts how entities who receive nonpublic personal information from a financial institution can, in turn, use that information. The law also forbids financial institutions from disclosing their customers' account numbers to non-affiliated companies for marketing purposes.

In addition, the Right to Financial Privacy Act of 1978 ("RFPA") protects the confidentiality of personal financial records by creating a statutory Fourth Amendment protection for bank records. The RFPA requires federal agencies to provide account holders with notice and opportunity to object before a bank, or other specified institution, can disclose personal financial information to a federal government agency—exceeding the accountholder protection found in a number of similar state laws.⁷

While the CCPA does contain a— limited and rather chunkily drafted—GLBA exception⁸, it should be supported with a safe harbor for already comprehensively regulated businesses like financial institutions. We note that, unlike unregulated businesses, financial institutions undergo regulatory compliance examination by state a federal agencies.

c. The Need for Safe Harbors

The CCPA is the progeny of a privacy referendum filed at the behest of the Californians for Consumer Privacy ("CFCP") in 2017 to be placed on the ballot in 2018.⁹ In cooperation with state legislators from both chambers, the referendum's sponsor withdrew his petition, and the referendum was replaced with what ultimately became the CCPA.¹⁰

⁶ See Appendix to 12 CFR §1016.

⁷ *op. cit.*

⁸ CCPA §1798.145(e)

⁹ Initiative 17-0039.

¹⁰ A brief history and timeline are available at <https://www.caprivacy.org/about-us>

During the consideration of the legislation, the CFCP's founder testified the CCPA was intended to provide a safe harbor to protect businesses operating in good faith and taking reasonable precautions to protect customers' data from disclosure.¹¹

While we believe CFCP's testimony applied to all covered entities, at a minimum, we believe safe harbors should be extended to entities operating under existing privacy regimes offering verifiable standards. This is not a novel legal approach.

As part of the Ohio Attorney General's CyberOhio initiative to protect consumers and businesses alike from unsafe network and data storage practices, that state's legislature enacted the Ohio Data Protection Act which provides a safe harbor to firms that reasonably conform to one of eight frameworks developed by the National Institute of Standard and Technology (NIST). The GLBA is one of these enumerated frameworks.¹²

We recommend the Attorney General use the authority granted by the CCPA to provide a safe harbor for businesses that maintain appropriate data security practices promulgated by federal regulators or recognized national and international standards-setting organizations.¹³

II. AREAS OF OPERATIONAL CONCERN IN THE PROPOSED REGULATION

a. Proposed §999.305(a)(3) – requiring additional explicit consent for certain data uses

The requirement that an entity must “directly notify” and “obtain explicit consent” from consumers in order to use a consumer's personal information for any other purpose than what was described at the time of collection goes beyond the scope of what the underlying statute requires. Section 1798.100 (b) clearly states that use of collected personal information for additional purposes should be subject to further *notice* requirements only.

The drafters of the CCPA acknowledged that the extra step of obtaining explicit consent from a consumer should only be taken when the use of personal information was materially significant, namely the sale of a minor consumer's personal information¹⁴, participation in an enti-

¹¹ See *Understanding the Rights, Protections, and Obligations Established by the California Consumer Privacy Act of 2018: Where should California go from here? Informational Hearing Before the Comm. On Privacy and Consumer Protection*, 2019 Leg. Sess. (Cal. 2019) (statement of Alastair Mactaggart, Chairman, Californians for Consumer Privacy), available at <https://www.assembly.ca.gov/media/assembly-committee-privacy-consumer-protection-20190220/video>.

¹² 33 Ohio Rev. Code Ann. §§ 1354.01-1354.05.

¹³ See, for example: International Organization for Standardization (ISO), Payment Card Industry Security Standards Council (PCI SSC).

¹⁴ 1798.120(d).

ty's financial incentive program¹⁵, and retention of a consumer's personal information for the purposes of peer-reviewed scientific, historical, or statistical research in the public interest¹⁶.

Requiring explicit consent beyond these well-defined use cases overreaches and eliminates the needed nuance for when obtaining additional consent is necessary and meaningful to protect consumers' rights.

b. Proposed Section § 999.308 (b)(1)(d) - collection of personal information

This provision would require the disclosure of a very high level of detail relating each category of personal information collected including, the categories of sources from which the 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.

Doing so would be almost impossible for any company to operationalize and would not be beneficial to or understandable by the consumer. As drafted, the notice shall be written in a manner providing consumers "a meaningful understanding of the categories listed." We believe it is doubtful, at best, that even the most sophisticated consumer could evaluate this information and determine whether the information collected or its sources are out of the ordinary or commercially unreasonable.

c. Proposed §999.313(d)(1) – treating an unverified request to delete as a request to opt-out

With no lack of irony considering the draft relates to privacy, this provision—not found in the CCPA—would force covered entities to treat an unverified request from an unidentified person as a valid request to opt-out of the sale of information.

As a matter of public policy—and good customer relations practices—no business should be required to take any action when the business is unable to verify the identity of the requester. To do so may harm the customer who may not receive a beneficial offer or service because of the action of a total stranger—whether in error or with malice.

We note this provision is particularly troublesome in a situation where the requestor cannot be verified and has a common name. If "John Smith" submits a request to delete without verification, are all "John Smiths" to be opted out? What is a covered entity to do in the case of customers whose national origin has limited surnames, e.g., Korean or Icelandic names?

We urge you to strike this section.

d. Proposed §999.313(d)(3) – deletion on backup systems

We presume that this section intends to assure covered entities that deleted data need not be removed from backup systems until the systems are used to restore information to the primary system. Unfortunately, the draft uses the overly-broad term "accessed." In reality, backup sys-

¹⁵ 1798.125(b)(3).

¹⁶ 1798.105(d)(6).

tems are “accessed” when additional information is backed up—a frequent occurrence that often occurs before a restoration. Either clarification should be provided or “accessed” should be replaced with restored.”

e. Proposed §999.313(d)(4)(d)(6) – deletions

These sections relating to requests to delete, assume that a covered entity actually has verifiable information pertaining to the requesting consumer, however, they do not allow for a circumstance in which the covered entity holds no information pertaining to that consumer (or cannot verify that the information it holds belongs to the requesting consumer).

This presents the covered entity with the dilemma of how to respond when it has not necessarily denied the consumer’s request, but also has not deleted any information.

f. Proposed §999.314(d) – service providers

As drafted, this section proposes that service providers respond to requests for access to personal information when, in contrast, the statutory obligation to respond to requests for access falls to the covered entity, including instances where the covered entity uses a service provider to process personal information.

This provision also requires service providers to build a response mechanism of some kind, rather than relying on the entity that owns the information to direct the actions of the service provider.

This is an issue that, under the existing statutory language, should be handled in contract negotiations between the covered entity and its service providers rather than being mandated in an extra-statutory regulation. We note that, in the case of payment cards, vendor management is governed by the existing regulatory structure.¹⁷

g. Proposed §999.315(c) – browser privacy settings

This section requires covered entities to treat undefined user-enabled controls to identify browser privacy settings and plugins and treat them as opt-out of sale requests—a requirement not found in the CCPA. In reality, websites generally do not look for these settings and plugins. Moreover, and as discussed below, such signals to specifically opt out of the sale of data may not currently exist.

There are myriad “user-enabled privacy controls,” which may differ depending on the operating system used by the consumer (*e.g.*, Apple IOS, Chromebook, Microsoft all have differing privacy features). We are unclear how consumers are to know which “user-enabled privacy controls” are adequate to make an opt-out from sale request.

Privacy settings are unique to and identified with a browser, not an individual. So even if a website is looking for a privacy setting, all the website will know is that that browser is requesting privacy but it will not know who the user is in order to opt them out of sale. And where

¹⁷ See, for example: The Bank Service Company Act (12 U.S.C. 1861 *et seq.*)

the website can identify the user (perhaps through a password log in), if the user is using a borrowed computer where the browser privacy setting indicates privacy, the user likely will not know that the setting has been activated, resulting in them not having access to offers and advertisements that they would otherwise want.

Additionally, which of these settings will your office consider as “privacy” settings that trigger regulatory obligations for the covered business? What is a covered business’s obligation to build technical solutions to determine whether a “user-enabled privacy control” exists? What are the technical specifications for that kind of solution? Will your office make that determination?

We believe this section finds both covered entities and your office unprepared from the consumer, business, regulatory compliance, and enforcement perspectives. We urge you to strike this section.

h. Proposed §999.317(g)(1) – required metrics display

This section requires a covered entity that receives, sells, or shares the personal information of 4 million or more customers to compile specific metrics and to publish those metrics in an online privacy policy. Nowhere does the CCPA require compilation or publication of this (or similar) data. Furthermore, the 4 million consumer threshold appears arbitrarily determined and has no discernible basis. In fact, it is doubtful that the CCPA authorizes your office to issue this requirement. The relevant authority contained in the CCPA allows your office to establish rules and procedures for 1) facilitating and governing the submission of consumer requests to opt out, and 2) governing business compliance with opt-out requests.¹⁸ Providing consumers with statistics that have little meaning to their personal privacy concerns does neither of these things, nor does it further the purposes of the CCPA.¹⁹

The mandated metrics are not meaningful to consumers and should not be displayed as part of the privacy policy. For example, the number of requests to know that are denied by a covered entity is not necessarily indication of an entity’s avoidance of the Act, but rather can be a measure of the effectiveness and due diligence of the protection of consumer information from fraudulent inquiries.

As noted above, if consumers are permitted to use user-enabled browser signals or other user “privacy” settings to send an opt-out message or signal, the underlying metric will not necessarily capture the automated opt-outs.

We recognize your office may need this data in the course of an enforcement action, but publication does not benefit the consumer in any manner. It seems the only beneficiary of publication may be the trial bar seeking to chip away at the legislature’s rejection of a broad private

¹⁸ Cal Civ. Code §1798.185(a)(4)

¹⁹ Cal Civ. Code §1798.185(b)(2)

right of action under the CCPA. We urge you to strike this potentially barratrous section issued under questionable authority.

i. Proposed §999.331 – relating to minors


This section is triggered by a covered entity's knowledge that it collects or maintains personal information pertaining to minors and requires the establishment of a process for opt-in to sale. It appears, however, that in the case where a covered entity holds personal information about minors but does not sell personal information, it is still required to build a process to permit minors to opt-in to sale.

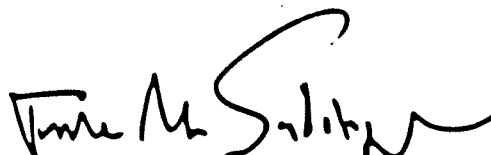
We recommend that, if the business does not sell minors' personal information, it need not be required to build an opt-in process.

III. CONCLUSION

The Card Coalition appreciates the opportunity to share our views on the Proposed Regulation and would be pleased to discuss our specific concerns outlined above. Thank you for your consideration.

Respectfully submitted,


Toni A. Bellissimo
Executive Director


Frank Salinger
General Counsel

Message

From: Blenkinsop, Peter [REDACTED]
Sent: 12/6/2019 11:59:50 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments of the International Pharmaceutical & Medical Device Privacy Consortium ("IPMPC")
Attachments: IPMPC Comments on Proposed CCPA Regulations.pdf

Dear Attorney General Becerra,

On behalf of the International Pharmaceutical & Medical Device Privacy Consortium ("IPMPC"), I am pleased to submit these comments on the proposed regulations under the California Consumer Privacy Act (CCPA). Further information concerning the IPMPC can be found at <https://www.ipmpc.org>.

Thank you for your consideration.

Sincerely,
Peter Blenkinsop
IPMPC Secretariat

Peter Blenkinsop
IPMPC Secretariat
Drinker Biddle & Reath
1500 K Street, NW, Ste 1100, Washington, DC 20005
[REDACTED]



IPMPC
International Pharmaceutical &
Medical Device Privacy Consortium

Drinker Biddle & Reath LLP is a Delaware limited liability partnership. The partner responsible for the firm's Princeton office is Dorothy Bolinsky, and the partner responsible for the firm's Florham Park office is Andrew B. Joseph.

This message contains information which may be confidential and privileged. Unless you are the intended addressee (or authorized to receive for the intended addressee), you may not use, copy or disclose to anyone the message or any information contained in the message. If you have received the message in error, please advise the sender at Drinker Biddle & Reath LLP by reply e-mail and delete the message. Thank you very much.



IPMPC

International Pharmaceutical &
Medical Device Privacy Consortium

December 6, 2019

Mr. Xavier Becerra
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street, First Floor
Los Angeles, CA 90013

By Email to: PrivacyRegulations@doj.ca.gov

Re: CCPA Proposed Regulations

Dear Attorney General Becerra,

The International Pharmaceutical & Medical Device Privacy Consortium (“IPMPC”) welcomes the opportunity to provide comments on the proposed regulations under the California Consumer Privacy Act (CCPA).

The IPMPC is comprised of chief privacy officers and other data privacy and security professionals from a number of research-based, global pharmaceutical companies and medical device manufacturers.¹ The IPMPC is the leading voice in the global pharmaceutical and medical device industries to advance innovative privacy solutions to protect patients, enhance healthcare, and support business enablement.²

The IPMPC is concerned that some of the requirements in the proposed regulations go beyond the requirements laid out in the statute and create burdensome obligations for businesses

¹ IPMPC members may also operate related businesses, including CLIA laboratories.

² More information about IPMPC is available at <https://www.ipmpc.org/>. This filing reflects the position of the IPMPC as an organization and should not be construed to reflect the positions of any individual member.

without creating proportional benefits for consumers. In particular, we are concerned with the following requirements related to the notice at collection of personal information:

- Section 999.305(b)(2) would require that the notice state the business or commercial purposes for which the information will be used “for each category of personal information.” This requirement will lead to significant redundancy and unnecessary length of privacy notices. In many cases, all categories of information collected from a consumer are used for the same set of purposes. For example, a company providing voluntary patient support programs will require (at least) a patient’s name, contact information, medical information, and health insurance information. Rather than permitting a company to say “We collect your name, contact information, medical information, and health insurance information to provide our voluntary patient support program,” the regulations appear to require a company to provide the notice in this format:

We collect your name to provide our voluntary patient support program.

We collect your contact information to provide our voluntary patient support program.

We collect your medical information to provide our voluntary patient support program.

We collect your health insurance information to provide our voluntary patient support program.

The amount of repetitive text required above would only increase once disclosures about sources of information and any information sharing are added.

Businesses should be permitted to aggregate or group the categories of personal information when the information that must be disclosed is the same. Requiring differentiation by category of personal information will lead to long, repetitive notices that will be difficult for consumers to understand.

- 999.305(b)(4) requires that the notice include a link to the business’s CCPA privacy policy or the web address of the policy. This paragraph should be amended to make clear that in the case of employees, this requirement can be satisfied by directing individuals to the relevant employee privacy policy, whether online (including on a company’s internal extranet) or offline (e.g., in an employee manual).

In addition to the above concerns with the notice at collection of personal information, the IPMPC is also concerned with the requirement that “[i]f the business intends to use a consumer’s personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose” (emphasis added). This requirement for explicit consent is unnecessary where the consumer’s intentions are clear from his or her actions.

The IPMPC encourages the Department of Justice to publish samples of the various types of notices and responses to “requests to know” that would be required under the proposed regulations. This will aid businesses in their compliance efforts.

Finally, the IPMPC notes that there are various circumstances in which a business is not permitted to disclose specific pieces of information in response to a consumer’s request to know. In particular, Section 999.313(c)(3) states that “[a] business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer’s account with the business, or the security of the business’s systems or networks” (emphasis added). We suggest modifying the underlined text to read: “a substantial and articulable, or otherwise unreasonable, risk.” Moreover, we encourage the Department to add “medical information” and other data elements the unauthorized disclosure of which could trigger a breach notification requirement under California law to the list of data elements in Section 999.313(c)(4) that do not require disclosure in response to a request to know specific pieces of information.

We thank you for the opportunity to provide these comments.

Sincerely,

A handwritten signature in black ink, appearing to read "Peter Blenkinsop". The signature is fluid and cursive, with the first name "Peter" and last name "Blenkinsop" clearly distinguishable.

Peter A. Blenkinsop
IPMPC Secretariat

Message

From: Mark Micali [REDACTED]
Sent: 12/6/2019 10:26:13 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments of The Nonprofit Alliance on Proposed Regulations to the CCPA

The Nonprofit Alliance (TNPA) appreciates the opportunity to comment on the Proposed Regulations to the California Consumer Privacy Act. TNPA is concerned that the draft regulations in their current form will negatively impact the nonprofit community and its ability to provide important services to Californians. In their current draft form the regulations will add costs to nonprofits' operations, thus resulting in fewer funds available to carry out their important missions. In fact, nonprofits could face a downward spiral of ever-increasing fundraising costs as the cost of compliance to CCPA raises the overall cost of data, leaving fewer dollars to provide services. In essence, without data being financially accessible to nonprofits, the vitality of this sector will be damaged in the State of California – every dollar more that nonprofits need to pay for data is a dollar less that they can spend on their programs. Specifically, our concerns with the regulations in their current draft form are as follows:

1. Section 999.305(d) includes a requirement that in order to sell a California resident's personal information, an organization that "does not collect information directly from consumers" must either directly give the consumer CCPA specific notice of the opt-out right or go through an extensive process of gathering signed attestations from each data source for that consumer together with an example of the privacy notice given to the consumer from the data source. These attestations must be disclosed to the consumer, upon request. This creates numerous issues:
 - a. The first option for compliance under this section (direct CCPA specific notice to consumers by each organization selling their data) will favor larger companies and those (such as social media platforms and those that provide digital products directly to consumers) and also encourage them to associate all data they have with individual consumers. Large consumer platforms like social media companies or consumer digital apps/tools/search companies often have a pre-existing communications channel to present notices to a consumer (and they routinely do so), so they are uniquely positioned to use direct notice under this first option. For any organization without this kind of pre-built communications channel with consumers, direct contact must be initiated, which could be expensive (and likely annoying to consumers – see point d, below).

This could be very harmful, especially for small to medium sized businesses and nonprofit organizations because they will almost certainly see increased costs and decreased innovation as a result. Small to medium sized businesses and nonprofit organizations often rely on smaller, newer companies to provide affordable marketing services and innovative marketing solutions that match their unique needs. But these smaller, more responsive service providers are those most likely to be decimated by this rule. These service providers will likely find the cost of giving direct individual notice to consumers cost-prohibitive – typically lacking direct relationships and communications channels with consumers they would have to pay to give these notices, and update them over time. As these companies are pushed out of the marketing services space, the larger companies (and especially those with existing consumer relationships, like the social data platforms) are further entrenched and can raise prices for small to medium sized businesses and nonprofit organizations while offering them products that are less customized to their needs. This type of anti-competitive effect has already been observed in the EU since the institution of GDPR.

- b. It is worth noting that prescribing direct notice requirements will result in rafts of communications targeted to California consumers who may not care to read them, cluttering email inboxes, web browsers and other communications channels.
 - c. Like the first option for compliance under this section, the second option for compliance under this section will greatly burden most organizations who seek to use it, causing increased prices and decreased competition and innovation. In addition, it may directly impact small businesses and nonprofit organizations' budgets for actions they will be required to take (which the CCPA expressly sought to avoid). If all recipients of personal data who sell personal data are required to gather attestations, they will institute this process with all their data sources. They will not be able to rely on any previous contracts or attestations since no one could have included the required CCPA-specific notification language because those rights (and that language) did not exist until very recently. **The way the proposed rule is written there is no exclusion for small businesses or nonprofit organizations. They too will have to provide attestations to multiple business partners, and will thereby be swept up in CCPA compliance for those data sharing relationships that might qualify as a CCPA "sale," which is the direct opposite of the express intent of the Legislature.**
 - d. This provision also directly contravenes the Legislature's determination that sources of data were to be disclosed at the categorical level, not the individual level. If consumers are to be provided with copies of every attestation for every source of data, this will likely disclose the identity of the individual data sources, which was a requirement specifically not included in the CCPA. These types of disclosures were intended to be made categorically, not individually.
 - e. If the goal is to provide California consumers more opportunity to exercise their rights under the CCPA, this can be accomplished in multiple less-burdensome ways that avoid these economic, competitive and societal harms. We need not discriminate against smaller service providers and inundate consumers with pop-ups, emails, letters or other communications giving them notice of standard legal rights under the CCPA to meet these goals. For example, with the recently passed bill AB 1202, the CCPA already provides a mechanism for public notification of certain sellers of data, and industry participants could use that registration to voluntarily provide as part of their registration a link to where California consumers can read about and exercise their opt-out rights. Perhaps this exemption to needing to give direct notice of collection could be modified to cover those organizations that voluntarily choose to do this. Alternatively, industry groups could provide annual mass-media notifications in CA media, listing a website where consumers may go to find their members and links to the CA privacy disclosures of those members. Either of these would increase consumer awareness without creating huge, unworkable burdens for businesses and for organizations that were intended to be exempt from the CCPA.
2. Section 999.314(d) requires that service providers who decline to delete information they hold on behalf of another organization identify contact information for that organization. That is very problematic.
- a. This again goes outside the overall structure of individual company compliance with the CCPA and requires extending an organization's compliance to potentially hundreds or thousands of other organizations. The structure of the CCPA was properly designed to put the party who determines the use of the data (for whom the service provider provides the services) in control of and responsible for interfacing with the consumers whose personal data is in the data, which is appropriate. This would expose confidential client relationships and harm businesses, nonprofits and their partners and clients.
 - b. This also could be used in an unfair method by competitors to identify the clients of service providers for whom the service provider hosts consumer personal information, essentially requiring disclosure of proprietary client lists.

3. Section 999.315(f) includes a requirement that a business receiving an opt-out request notify those parties to whom it has sold personal information within the prior 90 days of the opt out and instruct them to not further sell the information and inform the consumer when that is done. This requirement will be costly, both operationally and financially to nonprofit organizations.
 - a. This again exceeds the clear intent of the CCPA, which has its focus for data sellers being individually responsible to make disclosures to consumers and honor consumer rights when exercised. This will create a lot of additional notifications and work for non-data-sellers, and extend data sellers' obligations beyond their own organization. This is not necessary to give quick effect in the marketing industry to a consumer's choice.

Consumers will already see their choices perpetuated throughout the marketing industry without this new requirement. Typical practice in the marketing industry is that any data sale is a limited-duration license, with periodic data updates for longer-term licenses. For example, a direct mail marketing list is typically licensed for only one mailing. The next time the list is licensed, the consumer will no longer be in the list if the consumer opted out with the list provider. Similarly, when organizations license inferences about a consumer for their internal data analysis, that is typically done for a specified period of time, with periodic updates to the inferences throughout the term of the license. In that situation a consumer's request would be honored by the data seller in the next update after the opt out occurs, or at the very least following the term of the license. In other words, a consumer who exercises the right to opt out will see that right steadily propagated throughout the marketing data industry without needing to have an extremely burdensome ongoing requirement for one-off notices for each consumer who makes a request.

- b. As written this would impose opt-out requirements on buyers/licensees of data, regardless of whether they are themselves covered by the CCPA, including nonprofit organizations and those who have no California nexus if any way they share data might count as a sale, which contravenes the express Legislative intent to exclude nonprofits and to govern businesses who operate in meaningful ways in California.

Mark Micali
Vice President, Government Affairs



The authoritative voice of nonprofits to promote, protect, and strengthen the philanthropic sector.

www.TNPA.org

1319 F St. NW, Suite 402 | Washington, DC 20004

Message

From: Halpert, Jim [REDACTED]
Sent: 12/6/2019 9:13:57 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Kingman, Andrew [REDACTED]
Subject: Comments of the State Privacy & Security Coalition
Attachments: StatePrivacyandSecurityCoalitionCCPARegComments.pdf
Importance: High

Dear Privacy Regulations Coordinator,

Attached please find the comments of the State Privacy & Security Coalition.

Thank you very much for your consideration – Jim Halpert

Jim Halpert

Partner, co-Chair Global Data Protection, Privacy and Security Practice



DLA Piper LLP (US)
500 Eighth Street, NW
Washington, DC 20004
United States
www.dlapiper.com [\[dlapiper.com\]](http://dlapiper.com)

The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use, disclosure, dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please reply to the sender and destroy all copies of the message. To contact us directly, send to postmaster@dlapiper.com. Thank you.

State Privacy and Security Coalition, Inc.

COMMENTS TO THE ATTORNEY GENERAL

December 5, 2019

California Department of Justice

Attn: Privacy Regulations Coordinator

300 Spring Street

Los Angeles, CA 90013

PrivacyRegulations@doj.ca.gov

Re: Comments Regarding Title 11(1)(20): CCPA Proposed Text of Regulations

I. Introduction

The State Privacy & Security Coalition is a coalition of 29 companies and 6 trade associations across the retail, payments, communications, technology, fraud prevention, tax preparation, automotive and health sectors. We work for laws and regulations at the state level that provide strong protection for consumer privacy and cybersecurity in a consistent and workable matter that reduces consumer confusion and unnecessary compliance burdens and costs.

Our Coalition worked with Californians for Consumer Privacy and consumer privacy groups on amendments to clarify confusing language in the CCPA, to reduce the risk of fraudulent consumer requests that would create risks to the security of consumer data, and to focus CCPA requirements on consumer data, consistent with the title of the law.

We very much appreciate that the draft Regulations address a number of outstanding confusing aspects of the CCPA and take the risk of fraudulent “pretexting” requests seriously. At the same time, we urge the Attorney General’s Office to amend the final rules to make them more workable, more consistent with the text of the CCPA, and avoid needless areas of inconsistency with the California Privacy Rights Act Initiative (“CPRA”), No. 19-0021, filed Nov. 13, 2019, which may well be adopted by California voters in 2020.

II. AG’s Office should not issue rules that differ from both the statute and CPRA

The CCPA has already been amended and changed twice. The rules will change CCPA requirements *a third time*.

If approved by the voters in 2020, the CPRA will make further changes in 2023 and will move authority over this area of the law to a new agency, and will require rulemakings by that new agency in 14 more areas. These repeated changes make the CCPA a “moving target” and create needless and wasteful uncertainty.

State Privacy and Security Coalition, Inc.

The AG rules go beyond both the statute and CPRA in several problematic and onerous ways. Unless corrected before the final rules are issued, these changes would create anomalous and burdensome requirements that do not significantly advance consumer privacy and that would be erased in 2023.

These potentially temporary requirements could very well create further uncertainty and confusion, with consumers seeing mandatory notices and rights that would disappear in 2023. This back and forth would not advance privacy. Furthermore, there are significant arguments that these requirements exceed the AG's Office's authority to interpret the statute.

For all these reasons, it is a far better course for the AG's Office to remove these temporary, outlier requirements from the final rules.

III. Do Not Sell Signals Should Not Be Included as a Requirement in the Final Rules

In contrast to CPRA, § 999.315(c) of the draft Rules would require all businesses that collect information online to honor "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." The opt-out would need to be honored within 15 days of the rules taking effect.

By contrast, CPRA would provide businesses with a choice between honoring the do not sell opt-out signal and posting a Do Not Sell my personal information link. CPRA would provide for two rulemakings to clarify the requirement. CPRA, § 1798.185(a)(19)-(20). It would also make this requirement effective in 2023, only after the rulemakings regarding practical implication issues. CRPRA, § 31.

It makes far more sense for the AG Rules to defer to this element of its rulemaking. First, there is currently no user-enabled privacy control that sends a "do not sell" message, must less deployment of protocols for a downstream system for receiving and implementing the signal. This sort of requirement cannot be implemented in the near term along with the rest of the final regulations. It is important to allow time to develop and implement a technical standard for the privacy controls.

Second, this part of the proposed rule is vague as to which controls must be honored and which must not. It also contains no process at all for clarifying the requirement and how it would be implemented technically. It actually requires a further rulemaking to develop real rules on this issue and then time for the development of a technical standard then deployment of technology to make the privacy control effective. This would serve no purpose because the new agency is called upon to issue these rules in 2023.

Third, the CCPA itself contains no provision authorizing the AG's Office to impose this requirement and no mention of whatsoever of any "do not sell" technology. It is therefore doubtful that the AG's Office has this authority until CPRA is approved by California voters and take effect. Finally, as a practical matter, the requirement may necessarily apply outside the borders of California, in violation of the Dormant Commerce Clause to the US Constitution. All these considerations point strongly toward

State Privacy and Security Coalition, Inc.

waiting for CPRA rulemaking regarding how to implement a signal requirement.

IV. The Requirement to Obtain Opt-in Consent for Any Uses Not Specified in the Notice at Collection Should Be Removed

This opt-in requirement in § 999.305(a)(3) is contrary to the express language of CCPA § 110(b), which provides that business “shall not . . . use personal information collected for additional purposes without providing the consumer with *notice* consistent with this section”. The CCPA is very clear about the few places where it requires opt-in consent, and never requires opt-in consent for uses of personal data, so that there is no ambiguity at all in the statute to support this interpretation. CPRA is equally clear on this point.

Furthermore, well established privacy frameworks, including the FTC framework and the EU General Data Protection Regulation, permit additional uses of personal information that are consistent with the original purposes for collection and notice provided. Consistent with the CCPA, a consumer who receives notice of a business’ use of personal information for new purposes can submit a request to delete personal information, a right to know request, or a request to opt out of the sale of personal information. These protections are sufficient to maintain the consumer’s control of a business’ uses of her data.

What is more, requiring opt-in consent if the notice of uses is not broad enough would contravene the purpose of shorter notice at collection by strongly incentivizing businesses to provide overbroad notices of potential uses of personal information to avoid the need to contact state residents down the road to request opt-in consent.

V. Excessive Notice Regarding and Presumption of Illegality of Financial Incentives Should Be Pared Back

Section 999.336(a) impermissibly changes the concept of “discrimination” in the CCPA by creating a presumption that *all* price and service differences are unlawfully discriminatory if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or the regulations. This provision reverses language in the statute which permits reasonable price and service differentials. This proposed subsection is contrary not only to the CCPA text, but also to CPRA, which would add an express exemption for loyalty and reward programs that meet the requirements of CPRA Section 1798.125. *See id.* at § 1798.125(a)(3).

Section 999.307(b)(5) a. and b. would add detailed notice requirements to explain a “good faith estimate” of the value of a consumer’s data (something that is very difficult to estimate with any accuracy), as well a description of the method used to calculate that value. These requirements are contained neither in the CCPA, nor in CPRA and would add extensive detail that has nothing to do with providing notice to the consumer of the consumers of the terms of the incentive program. The CCPA notice requirements already significantly lengthen privacy policies, increasing the risk that consumers

State Privacy and Security Coalition, Inc.

will tune out and not read them. This further detail, which has no basis in CPRA or the CCPA, should be removed.

Section 999.336 defines a financial incentive as a “discriminatory practice”, but allows for price or service differentials if the requirements of a new model to value data are followed under a wholly new proposed formula set forth at Section 999.337. The proposed rules cabin the “reasonableness” valuation by proposing 8 factors that can be used alone or in combination to arrive at a price discount. There is absolutely no record to support that any of these methods “reasonably” approximate the value of a customer’s data. Nor can they. The value of an individual’s personal data to a product offering to many customers cannot be based on any of these 8 factors offered by the AG’s office without any empirical support to suggest they are reasonable.

VI. The Range of Personal Information Subject to CCPA Rights Requests Should Be Aligned With § 1798.145(j)(3) of the Initiative

The CPRA Initiative recognizes in this subdivision that responses to the CPRA rights requests should not apply to personal information that as a practical matter a business cannot retrieve without accessing additional data or technology that the business or service provider does not access in the ordinary course of business.

This is an important clarification to add to § 999.313 and .315 of the draft regulations to clarify that businesses need not engage in extraordinary eDiscovery searches to try to locate every bit of the broad range of personal information that might be located somewhere in their systems -- including in unstructured formats and that are never used in the ordinary course of business -- in order to comply with CCPA rights. This would create a perverse and anti-privacy incentive to make all these data that the business does not use and cannot easily retrieve much more readily retrievable and thereby more usable by the business.

This clarification is pro-privacy, would anticipate a specific provision in the CPRA that is likely to go into effect in 2023, and would significantly reduce unnecessary compliance costs from CCPA rights requests.

VII. The Data Elements That May Not Be Disclosed In Response to a Consumer Request Should Expand With Data Elements That Can Trigger Data Breach Class Action Risk Under § 1798.150(a) of the CCPA.

We strongly support the prohibition in § 999.313(c)(4) against disclosing SSNs, drivers’ license numbers and other government-issued ID numbers, health insurance or medical identification numbers, account passwords, or security questions and answers. Consumers know this information and there is no reason to create risk of requiring disclosure of these data elements in response to “right to know” requests.

However, this list should be amended to include a cross reference Section 1798.150(a)(1)’s reference to Section 1798.81.5(d)(1)(A), which sets forth certain data elements for which “reasonable

State Privacy and Security Coalition, Inc.

security” is required . For example, this year the legislature at the request of the Attorney General amended Section 1798.81.5(1(A) to add biometric data, thereby creating data breach class action risk for these data. If the legislature (and the Attorney General) believe that additional data elements such as biometric data warrant potential class action enforcement under Section 1798.150(a)(1), then § 999.313(c)(4) should relieve businesses of the obligation to turn over these specific pieces of personal information in response to a CCPA “right to know” request.

Including this “expander” is not only good for consumer data security, it is also the only fair result for businesses subject to CCPA, because CCPA both creates the risk of large class actions and affirmative “right to know” requirements that expose businesses to this risk.

VIII. For Similar Important Security Reasons, the Final Regulations Should Exempt Personal Information That Is Used Solely For Fraud or Misrepresentation Prevention or Cybersecurity from Do Not Sell, Deletion and Right to Know Requests

Section 1798.105(d)(2) of the CCPA recognizes the importance of personal information for security purposes by including an exemption from the deletion right for personal information that is necessary to retain in order to

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

This same important interest applies with regard to the risk that fraudsters and hackers will use the “right to know” to: (1) learn what specific data and types of data elements are used by a business for authentication and other security purposes, and (2) block “sale” of personal information by fraud prevention and cybersecurity services to customers that is important to prevent “malicious, deceptive, fraudulent, or illegal activity”.

For the same reasons that prompted the Attorney General’s Office to propose the verification and security requirements in the proposed regulations, the final regulations should contain narrow exemptions to “right to know” and “do not sell” requirements for personal information *“to the extent that this personal information is used solely to protect against malicious, deceptive, fraudulent, or illegal activity.”* These two narrow revisions would advance the goals of the regulation by preventing bad actors from using rights in the CCPA to circumvent the verification and security requirements that the final regulations include to protect consumers. They would also avoid the significant unintended consequence of the CCPA right being used as a sword by bad actors to perpetrate fraud and cybersecurity attacks that undermine California consumers’ privacy and make them less safe.

IX. The Exemption for Service Provider Use of Personal Data for Security Purposes in § 999.314(c). Must Be Amended to Add the Other Exempt Purposes under § 1798.145.

State Privacy and Security Coalition, Inc.

The limitation in § 999.314(c) of the draft regulations against service providers using personal data they receive to provide services to any other person or entity with the exception of security services needs to be amended to be consistent with the definition of a "service provider" in § 1798.140 of the CCPA. The statutory definition expressly allows use of personal data for any purpose that is expressly allowed under the statute.

Without this important clarification, this provision would limit a service provider's capacity to utilize its data for legitimate CCPA business purposes agreed to and defined within the boundaries of a contract, in circumstances in which personal information will not be sold, but only used to provide services. The CCPA already subjects service providers to robust requirements. This subsection of the final rules must be amended to allow these other important, statutorily permitted purposes.

Respectfully submitted,



Jim Halpert, General Counsel
State Privacy & Security Coalition

Message

From: Pam Dixon [REDACTED]
Sent: 12/6/2019 11:14:36 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments of the World Privacy Forum re: CCPA NPRM
Attachments: Comments_WPF_CCPA_06Dec2019_fs.pdf

Attached please find the comments (PDF) of the World Privacy Forum regarding the CCPA Notice of Proposed Rulemaking.

Thank you for the opportunity to comment,

Pam Dixon

Pam Dixon
Executive Director
World Privacy Forum
[REDACTED]

[3 Monroe Parkway](#)
[Suite P #148](#)
[Lake Oswego OR 97035](#)
www.worldprivacyforum.org / @privacyforum



Comments of the World Privacy Forum

Regarding

Notice of Proposed Rulemaking, California Consumer Privacy Act

Sent 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

December 6, 2019

Dear Attorney General Becerra:

Thank you for the opportunity to comment on the Notice of Proposed Rulemaking for the CCPA. We appreciate the work and thought that went into the draft rules.

The World Privacy Forum is a nonprofit, non-partisan 501(c)(3) public interest research group. We have published respected privacy research and analysis in multiple areas, including AI, health, identity, data brokers, biometrics, and others. We have testified before Congress and federal agencies, most recently testifying about the FCRA and data brokers before the Senate Banking full committee in June of this year. We regularly submit comments on a wide variety of agency regulations affecting privacy and security matters. You can find out more about our work and see our reports, data visualizations, testimony, consumer guides, and public comments at <https://www.worldprivacyforum.org>. WPF is incorporated and registered as a non-profit in California, and we have worked in the state for more than two decades. We are also registered in Oregon.

Our primary comments regarding the proposed regulations focus on procedures, policies, and rules for consumers regarding requests to delete, to opt out, or to know. The implementation of the opt out, deletion, and right to know requests have significant potential to create serious new risks for consumer abuse and fraud. We have proposed solutions where possible.

We have concerns relating to the potential that CCPA implementation creates increased consumer identity silos and increased uses of "strong identity" systems, such as biometrics, to verify consumer requests.

And finally, we find much to object to regarding the proposed uses of the terms *deidentification* and *aggregation* to stand in for effectuating a consumer's request for *deletion* of data. We see this as an issue that will prove problematic for consumer privacy over time.

Albeit unintentional, the potential for consumer harm in the CCPA and its implementation concerns us. The challenges are significant enough to warrant comment, attention, and further action.

Comments on § 999.306: Notice of Right to Opt-Out of Sale of Personal Information

The proposed regulations state that businesses shall include certain information in the opt-out notice. We affirm the inclusions discussed in 1-4. We object to (5). The provisions are as follows:

- (c) A business shall include the following in its notice of right to opt-out:
 - (1) A description of the consumer's right to opt-out of the sale of their personal information by the business;
 - (2) The webform by which the consumer can submit their request to opt-out online, as required by Section 999.315(a), or if the business does not operate a website, the offline method by which the consumer can submit their request to opt-out;
 - (3) Instructions for any other method by which the consumer may submit their request to opt-out;
 - (4) Any proof required when a consumer uses an authorized agent to exercise their right to opt-out, or in the case of a printed form containing the notice, a webpage, online location, or URL where consumers can find information about authorized agents; and
 - (5) A link or the URL to the business's privacy policy, or in the case of a printed form containing the notice, the URL of the webpage where consumers can access the privacy policy.

We disagree with the provision in (5) that allows a printed form containing the notice to simply list the URL of a webpage where consumers can then later access the privacy policy using an Internet connection. When the opt out notice is given in paper form, the privacy policy must be made available at that time to consumers in full, in either paper form, or displayed in full on a tablet or other available device. In the HIPAA context, the Notice of Privacy Practices is made available in paper form for patients who ask for it. This is the right decision and is an inclusive and fair decision.

Creating a need for a consumer to go *online* to access a digital privacy policy for a *paper notice* is problematic, and in particular for vulnerable individuals who may not have easy or free access to the Internet at the moment they are reading the notice, when the information is relevant. It is important to remember that not everyone has fully shifted to digital, and those people who have not made the shift may not have done so due to factors that make them vulnerable. It is still important to provide paper privacy policies to people when a paper notice is the primary method used for notification.

Comments regarding Article 3. Business Practices for Handling Consumer Requests § 999.313. Responding to Requests to Know and Requests to Delete

Comments regarding (c)(1): Information that shall not be included in disclosures to consumers

The proposed language states:

- (1) For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business shall not disclose any

specific pieces of personal information to the requestor and shall inform the consumer that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (c)(2).

There is a balance here. On one hand, some businesses may abuse this section and use it as a broad excuse to deny many consumers disclosure based on a failure to verify identity. This would be a negative outcome. We encourage the Attorney General to carefully track the metrics of declined opt outs and make those results public, along with the reasons for the declined requests.

In considering the risks to consumers in disclosures effectuated by a bad actor, it is our analysis that it is initially better for consumer safety to err on the side of safety. And it is for safety reasons we support the language in (c)(1) at this time. We reserve our judgement for what the opt-out metrics reveal about consumer and business opt-out patterns.

Comments regarding (c)(4): Types of information that shall not be shared.

The proposed language states:

(c) Responding to Requests to Know

(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.

We agree that SSN, DL numbers, and the other consumer information mentioned in (c)(4) are appropriate to not disclose. We believe that for safety purposes, a business must also not disclose a consumer's home address or precise geolocation data that would allow the inference of a precise home address (or school address.)

The release of consumer home address data provides too many potential physical safety dangers to individuals whose information will be sought by fraudsters and bad actors. In cases of victims of crime, including domestic violence, sexual assault, and stalking, safety considerations for these individuals include the need to protect home addresses in particular.

Because it is entirely inappropriate to ask vulnerable individuals to self-identify or prove they are members of a vulnerable class, we recommend the inclusion of home address as a item that should not be shared. (Excepting businesses that maintain a password protected self-service portal, as described in the regulations in (c)(7).)

Comments regarding (d)(2) Responding to Requests to Delete

We profoundly disagree with the proposed language allowing "delete" to mean aggregation or deidentification. The language states:

(2) A business shall comply with a consumer's request to delete their personal information by:

- a. Permanently and completely erasing the personal information on its existing systems with the exception of archived or back-up systems;
- b. De-identifying the personal information; or
- c. Aggregating the personal information.

This language sets a deleterious precedent, negating the plain meaning of “delete.” Holding data is holding data, even if it is deidentified. White box analytics, which we describe more completely below, is a technique already in use today that allows for data analytics to be accomplished using deidentified data. Deidentifying data does not negate its usefulness to business. Beyond white box issues, deanonymization techniques continue to advance rapidly, meaning that even the most stringent definition of deidentification or aggregation will not hold the same meaning as *delete*. These three terms are not interchangeable. Delete means delete. Deidentification does not mean deletion.

First, we want to note that white box analytics and other machine learning techniques allow for the use of deidentified data to conduct analytics. White box analytics enables the use of deidentified data to accomplish data goals. This type of analytic technique is part of a well-understood privacy-by-design arsenal. Data should, when practicable, be robustly deidentified at the source, so that data comprising the basis of important statistical research is gathered, but can be made less risky to data subjects. With white box approaches, using raw data for analysis is not necessary. Reducing the spread and use of raw data for analytics is an important aspect of a more evolved data use policy.

White box analytical techniques are already being used in the financial sector to determine “KYC” or know your customer information using only deidentified data. As a precise example, companies such as ThreatMetrix conduct financial sector KYC analysis using only hashed personal data in a white box machine learning model — this is a best practice. The company does not work with the raw data, therefore it does not know the private details of each individual, but the analysis will tell them the probability of the individual being a “known” individual. KYC duties are fulfilled, and privacy and safety are preserved. There is still a need to prevent improper use of the analytic results in this model, because data that is deidentified is still usable.

Second, this language does not acknowledge the large research literature on deidentification and aggregation which has unambiguously demonstrated that deidentified data and aggregated data may be de-anonymized. This is true even for HIPAA datasets, which have carefully defined standards for de-identification. See for example, the seminal work on deidentification and deanonymization of Dr. LaTanya Sweeney <http://www.latanyasweeney.org/work/identifiability.html> and Arvind Narayanan <http://randomwalker.info/publications/de-anonymization-retrospective.pdf>.

If only three articles could be read on this topic, these three articles are key:

1. A. Narayanan and V. Shmatikov, *Robust de-anonymization of large sparse datasets* in the 29th IEEE Symposium on Security and Privacy, 2008, pp. 111–125. This is a famous paper and will afford background on why the prospect of calling deletion deidentification is so dangerous.
2. A. Narayanan and V. Shmatikov, *Robust De-Anonymization of Large Sparse Datasets: A decade later*, 2019. This 2019 update gives perspective on the original seminal paper.
3. L. Sweeney, *k-anonymity: A model for protecting privacy*, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 05, pp. 557–570, 2002. This paper by LaTanya Sweeney is utterly seminal and is important in understanding HIPAA deidentification.

Third, if California wants to incentivize businesses to aggregate and deidentify data, that is fine and we support that — but not when aggregation and deidentification takes the place of the plain meaning of delete. This presents a very meaningful policy shift, and is not appropriate.

If California is willing to put in its CCPA regulations a definition of deidentification that is **at least as strong as the HIPAA de-identification standard, and requires that the data meant to be deleted is never reused in any analytics again, nor to target scoring or other activities**, we are willing to go that far, as long as the term *delete* is disambiguated from the term *deidentify*. **Deleting data does not mean deidentifying data**. HIPAA provides the option of a safe harbor or expert analysis. HIPAA does not assert that deidentification is actual *deletion*.

This is a crucial point. Will the Attorney General honor the CCPA intent of deletion? Or will the regulations create an analytics loophole that allows entities to continue to use data as long as it is deidentified? We urge the Attorney General to differentiate between creating a safe harbor for businesses that deidentify data and do not reuse the data for any purpose, and the term *deletion*. Deletion of data means, to the public, that the company will no longer hold the data, and in fact will not use the data.

Fourth, even if the term “deidentified” is better defined, the term “aggregate” covers a great deal of ground, and we do not believe it can reasonably be included in this section. *Deleting data* does not mean to *aggregate the data*. No matter how cleverly defined.

Fifth, the Attorney General may be surprised to learn that a number of data brokers are declaring that they are not subject to the CCPA, because they *aggregate* and *deidentify* consumer data. We predict that aggregation and deidentification will be a major challenge for if these tools are articulated in relation to *deletion* in the proposed regulations.

Sixth, we note that successful deidentification may be problematic for small and medium sized enterprises (SMEs) who may not have a cushion of millions of members in their datasets to assist with sparsity issues. SMEs may also lack the technical knowledge to properly deidentify, or the funding to do so reliably. And certain very small businesses may not be able to adequately deidentify consumer data if the number of consumers involved is too small.

Seventh, one of the threat models behind the right to delete was the fact that companies, when they have acquired large volumes of consumer information, are then in a position to be compelled by search warrants to yield that personal information. There is an technological “arms race” between deidentification techniques and reidentification or deanonymization techniques. Will search warrants be served on deidentified data that technology can unlock now or in the future? We again assert that as long as a company is holding data, it is holding data, even if in deidentified form. Deidentified today is deanonymized tomorrow.

We state again that deletion does not mean the same thing as aggregation or deidentification. We note that the current regulations are written in an undesirable construction. If the state wishes to use deidentification as a safe harbor, then the following conditions must be present:

1. Deidentification is clearly stated to be a safe harbor, **but is not characterized as deletion**.
2. Deidentification must be to a HIPAA standard or better and must include specific requirements for deidentification, such as expert determination and/or removal of specific elements that create a safe harbor. We refer you to the HHS Guidance on Deidentification under HIPAA: <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard>.
3. Aggregation is not appropriate to include here in any definition or construction. Aggregation is not deletion. It is something else. Again, there is nothing wrong with encouraging businesses to use data in the aggregate. This is something we encourage as well. But we do not ever state that using data in the aggregate is like deleting the data.

4. Companies using deidentification for a safe harbor would need to certify in their privacy policy that they have met the deidentification standard (which should not be less than the HIPAA standard) and affirm that they will not themselves re-identify or seek to re-identify the data or reconstruct the relevant dataset using third parties, etc. They should also affirm that they will not use deidentified data that was subject to a deletion request from one or more consumers for further analysis, such as ad targeting.

We strongly urge the Attorney General to convene a task force to look specifically at this issue of deletion, deidentification, aggregation, and de-anonymization. Experts such as LaTanya Sweeney and Arvind Narayanan need to be brought in to provide background and context. A much more deliberative and **scientifically based and informed process** needs to be brought to bear on this implementation issue. California should not redefine *delete* as *aggregate* or *deidentification*.

§ 999.317. Training; Record-Keeping

There is much that could be improved in this section. Here we focus on one aspect, (b), which states:

(b) A business shall maintain records of consumer requests made pursuant to the CCPA and how the business responded to said requests for at least 24 months.

This section should state that the records of consumer requests should be maintained in a secure manner, and ideally be encrypted. Consumer requests over 24 months may include a considerable amount of personal data, and represent a data breach risk, depending on how the data is managed and stored.

Article 4. Verification of Requests

§ 999.323. General Rules Regarding Verification

General Comments about Verification

The verification aspects of effectuating broad consumer rights under the CCPA was always going to be challenging to implement. We were hoping that the AG would undertake a formal public discussion and inclusive multistakeholder process regarding verification risks, mitigations, and new research and methodologies in the field. We were hoping this process would be grounded in facts and be scientifically informed. Generally, we find that the verification section needs much more work, and requires the benefit of expert technical input on verification. There are numerous verification technologies and architectures available today. Identity verification is a meaningful research area in its own right, and many advancements have been made in the past 5 years.

The proposed regulations have not articulated the range of important technologies and systems being implemented today for privacy-protective identity authentication and verification. For example, new technologies and methodologies have emerged and are in use that can be highly trusted to verify identity, yet also provide only a yes/no response to businesses based on zero knowledge proofs. There is not a need for businesses to always build up huge stores of new identity silos for the purposes of eventual opt out. There are additional architectures that are in use today that would be helpful that could be further explored.

The regulations appear to be unaware of the risks that various large data breaches, particularly the Equifax data breach, have had on identity verification. Pieces of data that businesses have, such as SSNs and other such data, may well be compromised. This is part of why newer technologies and methodologies have replaced or enhanced the “pieces of data” methodology.

Again, it would be beneficial for the AG to convene a task force or work group to bring forward the best-of-class options in this particular set of privacy-enhancing identity technologies and to find ways of encouraging improved outcomes for privacy by using these technologies. Otherwise, the mountain of data retention requirements for CCPA is going to have the long-term effect of creating unexpected consequences from the high volume of newly created data and identity silos.

Specific Comments about Verification

The proposed guidelines state:

(c) A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, and for security or fraud-prevention purposes. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 999.317.

and

(e) If a business maintains consumer information that is de-identified, a business is not obligated to provide or delete this information in response to a consumer request or to re- identify individual data to verify a consumer request.

We note that the term *delete* in (c) is used in what consumers could construe to be a plain meaning. In (e), the term *delete* is modified to essentially mean information that is deidentified. The term deidentified is defined in the CCPA statute, but it is not defined to a strict enough standard in the regulations so as to protect consumers from the serious risks and probabilities of reidentification or de-anonymization or analytic re-use. We have already discussed these issues earlier in these comments. We reference those arguments here, and repeat our serious concerns with this language.

We urge the Attorney General to rethink the approach of using delete and deidentification interchangeably, which will surely change the meaning of *delete* in precedential ways that are unhelpful for consumer privacy protection. If a safe harbor is contemplated, then it should be called a safe harbor, and it should meet at least the level of HIPAA deidentification standards. The use of deidentification should be noted as a safe harbor, and not as a deletion. We do not object to a safe harbor. We object to deidentification or aggregation being defined as deletion. We note that no deidentification will remain impermeable for all time; deidentification techniques advance alongside de-anonymization techniques.

§ 999.325. Verification for Non-Accountholders

Two sections are of particular concern here:

(b) A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business, which the business has determined to be reliable for the purpose of verifying the consumer.

(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.

The procedures presented in (b) and (c) regarding numbers of pieces of data for authentication needs to be fully quantified and quality-tested. There should be full documentation of why this is the best method, and it needs to include definitive numbers about the methodology and results. The proposed methods should be tested and compared against other methods that exist today, and the proposed methods should be submitted to routine testing for effectiveness and accuracy, among other items.

We believe these regulations would benefit greatly from more time and much more expert-level input on this point, and more data points regarding effectiveness of verification methods, as well as acceptable options. Future-proofing could be achieved here in a number of ways. We encourage the Attorney General to surface how verification language might be future proofed in a working group or further multistakeholder process.

Conclusion

We can appreciate the amount of work and thought that went into this proposed rulemaking. However, the Attorney General has more work to do to create a detailed, evidence-based implementation of the CCPA.

We urge the Attorney General to convene one or more task forces to look specifically at the issues of deletion, deidentification, aggregation, de-anonymization, and verification, and to make sure the leading technical researchers in each area are involved in that process or processes. We are particularly concerned that the precedent in the proposed language around aggregation and deidentification as equal to deletion is deleterious in ways that will damage consumer privacy interests deeply going forward, in California and elsewhere.

We are also concerned that, given the definition of *delete* and the procedures for verification put forward in these proposed regulations, that there is every reason to be concerned that businesses will create new silos of consumer demographic and identity information as they attempt to comply with the regulations, creating breach liabilities for businesses and risks for consumers. The regulations are not specific enough on this point of ensuring data and identity silos are not created.

Overall, the regulations can do much more to assist businesses and consumers with privacy-friendly identity verification options. The regulations as currently proposed do not seem to be aware of the newer techniques for privacy-protective verification of identity. Where these options would work, they are preferable. We again encourage the Attorney General to convene a workgroup on these options, ensuring that technical experts in identity and verification are invited to provide data and factual documentation of various verification methods and effectiveness of those methods, as objectively quantified.

And finally, if there was just one thing we could change in these proposed regulations, we would choose to remove the redefinition of *delete* to mean *deidentify* or to *aggregate* data. We agree that businesses can and should be incentivized to use deidentification techniques, but these techniques should not be characterized as actual deletion. Instead of characterizing deidentification as deletion, it may be characterized as a safe harbor. This is fine, as long as the standard for deidentification is at least as strong as HIPAA, is specific, and does not allow for ongoing use of deidentified data that was subject to one or more deletion requests.

We stand ready to help address and work to resolve the issues we have raised in these comments. We are aware that the issues CCPA raises for businesses and consumers are complex, and there are not easy answers. That is why we believe more dialogue — and understanding — between stakeholders working in good faith is necessary. While appreciating the challenges involved, we urge you to take more time and gather more technical input on the specific tensions we have discussed. Thank you for your time and attention.
Respectfully submitted,

/s

Pam Dixon
Executive Director,
World Privacy Forum
www.worldprivacyforum.org

Message

From: Howard Fienberg [REDACTED]
Sent: 12/6/2019 10:25:41 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Blake Edwards [REDACTED] Stuart L. Pardau [REDACTED]
Subject: Comments on CCPA draft regulations
Attachments: Insights Assoc CCPA Reg Comments 12-6-19.pdf

Attached are the comments of the Insights Association on the draft CCPA regulations.

Sincerely,
Howard Fienberg
VP Advocacy
The Insights Association
[REDACTED]

1156 15th St, NW, Suite 700, Washington, DC 20005
<http://www.InsightsAssociation.org>

(In 2017, CASRO and the Marketing Research Association (MRA) merged to form the Insights Association, representing the marketing research and data analytics industry.)



The Honorable Xavier Becerra
Attorney General, State of California

Privacy Regulations Coordinator
California Office of the Attorney General

Email: privacyregulations@doj.ca.gov

December 6, 2019

Dear Attorney General Becerra

The Insights Association (“IA”) submits the following comments regarding the proposed regulations¹ implementing the California Consumer Privacy Act (“CCPA”) (CAL. CIV. CODE, § 1798.100 et seq.).

IA represents more than 530 individual and company members in California, with more than 5,300 members in total. Virtually all of these members will fall within the jurisdiction of the CCPA due to the fact that personal information of California residents is collected and transmitted for legitimate purpose by marketing research and data analytics companies and organizations in most instances.

IA is the leading nonprofit trade association for the marketing research and data analytics industry. IA’s members are the world’s leading producers of intelligence, analytics and insights defining the needs, attitudes and behaviors of consumers, organizations, employees, students and citizens. With that essential understanding, leaders can make intelligent decisions and deploy strategies and tactics to build trust, inspire innovation, realize the full potential of individuals and teams, and successfully create and promote products, services and ideas.

What is “marketing research”? Marketing research is the collection, use, maintenance, or transfer of personal information as reasonably necessary to investigate the market for or marketing of products, services, or ideas, where the information is not otherwise used, without affirmative express consent, to further contact any particular individual, or to advertise or market to any particular individual. An older definition of marketing research, used in California S.B. 756 in 2017, was “the collection and analysis of data regarding opinions, needs, awareness, knowledge, views, experiences and behaviors of a population, through the development and administration of surveys, interviews, focus groups, polls, observation, or other research methodologies, in which no sales, promotional or marketing efforts are involved and through which there is no attempt to influence a participant’s attitudes or behavior.”

The CCPA will have a profound impact on the business community, including the marketing research and data analytics industry. According to the August 2019 estimate from Berkeley Economic Advising and Research for the Attorney General’s office, compliance with CCPA regulations (not including compliance

¹ <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf>

with the statute itself) would amount to \$467 million to \$16.454 billion per year.² In this regard, we appreciate the opportunity to submit IA's recommendations on the draft regulations.

Our primary concerns focus on: (1) limiting the "authorized agent" concept to minors, and elderly or incapacitated individuals; (2) exempting marketing research from notices of financial incentives for research participation or, alternatively, providing for an opt-in regime in place of the notices; (3) allowing for email requests in lieu of an interactive webform; (4) clarifying how § 999.315 relates to existing "Do Not Track" requirements, and delaying implementation of this requirement; (5) setting the response times for requests to know or delete and opt-out requests at a uniform 45 days; and (6) issuing further guidance on how CCPA applies to personal information collection via telephone.

1. Limit the "authorized agent" concept to minors, and elderly or incapacitated individuals.

Under the draft regulations, a consumer may designate an authorized agent³ to submit opt-out requests, and requests to know and delete. Per § 999.326, when a consumer makes a request through an authorized agent, "the business may require that the consumer: (1) Provide the authorized agent written permission to do so; and (2) Verify their own identity directly with the business."

As currently drafted, there would be no tangible limitation on this procedure; anyone could submit a request through an authorized agent.

This option will be unnecessary in most cases, increase paperwork associated with the verification process, and open the door for fraudulent requests. Except in cases where the consumer is a minor, or someone who genuinely needs an authorized agent to submit a request (such as an elderly or incapacitated individual), requiring requests to be submitted by consumers themselves would better serve CCPA's purpose.

2. Exempt marketing research from notices of financial incentives for research participation or, alternatively, provide for an opt-in regime in place of the notices.

Under § 999.307, businesses would need to give notice of financial incentives for the purpose of explaining to the consumer "each financial incentive or price or service difference a business may offer in exchange for the retention or sale of a consumer's personal information so that the consumer may make an informed decision on whether to participate."⁴ The notice would have to include a "good faith estimate

² "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations." August 2019.

http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf

³ As defined by § 999.301, an "authorized agent" is "a natural person or a business entity registered with the Secretary of State that a consumer has authorized to act on their behalf subject to the requirements set forth in section 999.326."

⁴ § 999.307. "Notice of Financial Incentive (a) Purpose and General Principles (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 retention or sale of a consumer's personal information so that the consumer may make an informed decision on whether to participate. (2) The notice of financial incentive shall be designed and presented to the consumer 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 draws the consumer's attention to the notice and makes the notice 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

of the value of the consumer's data that forms the basis for offering the financial incentive." Section 999.337 spells out eight different methods for calculating that value.⁵

The regulations requiring notice of financial incentives seem primarily designed to deal with situations where companies offer some discount or free service in return for the sharing or sale of the consumer's personal information. Such situations often involve passive data collection under terms that are not entirely transparent.

Financial incentives in marketing research are different.

Marketing research requires robust participation and representation to be effective. IA members frequently achieve this by offering financial incentives to research participants (also known as respondents). For example, a doctor may be offered an honorarium to complete a survey about various pharmaceuticals, or an individual may be offered a gift card to participate in a half-day focus group about important public policy issues in their community.

In these and other similar cases, research respondents often participate for a variety of non-monetary reasons, including a desire to share opinions that will help improve product/service quality or simply on subject matter that a respondent may be passionate about. People care about the issues our members ask about, and like giving their opinions. Nevertheless, because of the costs sometimes associated with fielding a research study, insights professionals cannot afford to take participation for granted. Financial incentives of various kinds help complete research as quickly and effectively as possible.

Many exchanges between businesses and consumers involving personal information (such as those between researcher and respondent) are complicated interactions motivated by a variety of reasons. Often, there is no simple *quid pro quo* involving money for information.

on how a consumer with a disability may access the notice in an alternative format. e. Be available online or other physical location where consumers will see it before opting into the financial incentive or price or service difference. (3) If the business offers the financial incentive or price of service difference online, the notice may be given by providing a link to the section of a business's privacy policy that contains the information required in subsection (b). (b) A business shall include the following in its notice of financial incentive: (1) A succinct summary of the financial incentive or price or service difference offered; (2) A description of the material terms of the financial incentive or price of service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference; (3) How the consumer can opt-in to the financial incentive or price or service difference; (4) Notification of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and (5) An 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 consumer's data."

⁵ § 999.337 "(b) To estimate the value of the consumer's data, a business offering a financial incentive or price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data. The business shall use one or more of the following: (1) The marginal value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data; (2) The average value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data; (3) Revenue or profit generated by the business from separate tiers, categories, or classes of consumers or typical consumers whose data provides differing value; (4) Revenue generated by the business from sale, collection, or retention of consumers' personal information; (5) Expenses related to the sale, collection, or retention of consumers' personal information; (6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference; (7) Profit generated by the business from sale, collection, or retention of consumers' personal information; and (8) Any other practical and reliable method of calculation used in good-faith."

These exchanges are also, at least in the research context, generally entered into freely by both parties. If consumers knowingly consent to a financial incentive like those described in the marketing research scenarios described above, the CCPA's drafters likely did not intend to interfere in such a relationship.

The regulations do not appear to have been written with marketing research in mind and would inhibit research in an unintended way. Accordingly, the regulations should exempt marketing research participation from notices of financial incentives.

In the alternative, if such an exemption is not feasible, the regulations should provide an opt-in regime whereby the amount of the financial incentive (if any) will be disclosed prior to the commencement of the marketing research, and the respondent (or individual whose information is being used for marketing research purposes) will have the sole option to determine whether their personal information will be used for research or not.

3. Allow for email requests in lieu of an interactive webform.

Under Sections 999.312 and 999.315 of the draft CCPA regulations, businesses must provide two or more designated methods for submitting requests to know and opt-out, 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.

Many California businesses, including many of our members, have limited resources, both in terms of personnel and technological expertise. Requiring these businesses to launch an interactive webform imposes new burdens without furthering CCPA's purposes. As such, email correspondence would better serve CCPA's purposes by allowing consumers to state their questions and concerns directly, and to start a conversation regarding their privacy on their own terms.

4. Clarify how § 999.315 relates to existing "Do Not Track" requirements, and delay implementation of this requirement.

Under § 999.315, "[i]f 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 [opt-out] request."

IA seeks clarification on how this regulation relates to existing requirements related to "Do Not Track" signals. Under current California law, businesses are required to disclose in their privacy policies how they respond to such signals, but are not required to honor them. Would the regulations require that businesses honor "Do Not Track" signals, or would the regulations only apply to "a browser plugin or privacy setting" which more specifically communicates a consumer's desire that a business not *sell* their personal information?

A "Do Not Track" signal is not the same as a "do not sell" request. For example, a consumer may set her browser to "Do Not Track" because she does not want businesses tracking her browsing activities (and perhaps serving her with targeted ads), but it does *not* necessarily follow that the consumer would want to opt out of the sale of her information in every scenario.

Irrespective of this desired clarification, IA requests that the Attorney General's office delays implementation of any regulation related to a "browser plugin or privacy setting or other mechanism" for

an additional year. As discussed above, many of our members are smaller companies with limited technological capabilities. This concern is obviously not just limited to the marketing research and data analytics industry. We believe such smaller businesses will need additional time to work out the complicated implementation and response procedures related to this question.

5. Set the response times for requests to know or delete and opt-out requests at a uniform 45 days.

Under §999.313 of the draft CCPA regulations, businesses must confirm receipt of requests to know or delete information within 10 days, and respond substantively to the requests within 45 days. Under § 999.315, businesses must “act upon [an opt-out] request as soon as feasibly possible, but no later than 15 days from the date the business receives the request.”

These deadlines are unnecessarily complicated. The timeframe to respond to all requests should be set at a uniform 45 days.

However, the extension to 90 days under § 999.313 (“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”) and the requirement under § 999.315 that third parties be notified of opt-out requests within 90 days should both remain unchanged.

6. Issue further guidance on how CCPA applies to personal information collection via telephone.

Finally, the CCPA applies to the collection of all personal information, by whatever means, but does not give any guidance on unique compliance issues with different modes of collection.

In particular, the current draft regulations do not efficiently address information collection via telephone. For example, in a marketing research phone call where a financial incentive is involved, the caller would have to verbally read out the contents of three different notices: the notice at collection, notice of the opt-out right, and the notice of financial incentive. Such a three-part notice, delivered at the outset of the call, would be unduly cumbersome and likely result in significantly fewer respondents ever completing a research interaction via telephone (current response rates for U.S. telephone surveys rarely break 10 percent already). Such an outcome would not further the purposes of the CCPA.

As an alternative, the finalized regulations could require instead that, where information is collected via telephone, listeners may be directed to a URL where the required notices are posted, or callers may read out a short-form version of the notices.

Conclusion

The Insights Association hopes that the above comments will be useful to you and your staff.

We look forward to answering any questions you or your staff may have about the marketing research and data analytics industry, and working with you and your office in furtherance of consumer privacy in California.

Sincerely,

Howard Fienberg
Vice President, Advocacy
Insights Association

Stuart L. Pardau
Outside General Counsel
Insights Association (and Ponemon Institute Fellow)

Message

From: Donald Sherrill [REDACTED]
Sent: 12/7/2019 12:49:47 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments on CCPA from California Creditors Bar Association
Attachments: CCBA comments to AG.pdf

Attached please find comments regarding the CCPA from the California Creditors Bar Association.

Thank You,
Donald Sherrill
Managing Attorney
Hunt & Henriques
151 Bernal Rd, Suite 8
San Jose CA 95119-1306
[REDACTED]

This firm is a debt collector.

Confidentiality Notice: This e-mail message including attachments, if any, is intended only 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. If you are the intended recipient, but do not wish to receive communications through this medium, please so advise the sender immediately.



December 6, 2019

Re: Comment to the California Attorney General (AG) Regarding Implementation of the California Consumer Privacy Act (CCPA)

California Creditors Bar Association (CCBA) thanks the AG and his staff for their hard work and supports rules which interpret the CCPA. CCBA appreciates that the AG wants to move the industry into the 21st century by providing guidance around the private information of consumers.

CCBA is the only creditors bar association in California, and represents creditors rights attorneys. CCBA member firms practice law in a manner consistent with their responsibilities as officers of the court and must adhere to applicable state and federal laws, rules of state civil procedure, state bar association licensing, certification requirements, and the California rules of professional conduct of the state. CCBA's values are: Professional, Ethical, Responsible.

Attorneys, like lenders and consumers, are a necessary part of the "credit economy." Almost all CCBA members represent small businesses including local retail establishments, small or regional banks, credit unions, and small medical providers. These are long-term attorney-client relationships that have existed for years. These small business clients do not have vast legal departments or even in-house attorneys, and they rely on their local attorneys to ensure that outstanding receivables are paid so that their businesses can continue to operate. CCBA is comprised of law firms whose attorneys serve the needs of their local community. Attorneys who are members of CCBA law firms understand that they are officers of the court and work diligently to ensure that consumers, especially those that appear pro se in court, are treated fairly and with dignity and respect. Although our legal system is adversarial, CCBA attorneys make every effort to work with consumers throughout the legal process, including efforts to help resolve their debts in a reasonable manner.

COMMENTS OF THE CALIFORNIA CREDITORS BAR ASSOCIATION

We strongly support the goal of protecting the privacy of consumers and their data, and we are committed to vigorous compliance in furtherance of this pursuit.

The current landscape for compliance in the area of data privacy for the accounts receivable industry is robust, including complex state and federal regulations. There are multiple federal laws our members are already complying with in this area including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Fair Credit Reporting Act (FCRA), the Fair Debt Collection Practices Act (FDCPA), the Gramm Leach Bliley Act, and the Family Educational Rights and Privacy Act of 1974. Notably, the industry is already very restricted in what information and how information can be communicated to consumers under the FDCPA.

The CCPA is a robust state law, which many members of the accounts receivables management industry have argued is overly complex and burdensome. Notably, it also touches many businesses outside of California if personal information of California consumers is collected, making its reach potentially much broader than California agencies. As the Attorney General moves forward in implementing the CCPA, it is critical to be diligent in ensuring legitimate businesses are not faced with insurmountable regulatory burdens surrounding data privacy laws, particularly if they stifle innovation or have a disproportional impact on small businesses. It is also critical to ensure legitimate businesses are provided crystal clear guidelines regarding compliance.

It is currently unclear how the CCPA will be harmonized with federal laws like HIPAA, the FCRA, the FDCPA, Gramm Leach Bliley Act, and the Family Educational Rights and Privacy Act of 1974. Furthermore, the General Data Protection Regulation went into effect in the European Union in May 2018 and impacts certain CAC and ACA members in the U.S., as well as international accounts receivable management agencies.

The accounts receivable industry does not collect consumers' information for any purposes other than those permitted by privacy and consumer financial protection laws. However, because of the breadth of the law and the lack of clarity surrounding exemptions certain practices of the accounts receivable management businesses could be swept under the law. Outlined below are several areas where the proposed regulations need additional clarification.

I. AREAS OF CONCERN

a. Confusion regarding consumer requests and statutory exemptions

The proposed requirement that a business respond to a consumer's request to know or a request to delete even when relying on a statutory or regulatory exception to the CCPA [999.313(c)(5), 999.313(d)(6(a), and the associated recordkeeping requirements in 999.317] undermines the statutory/regulatory exceptions of the statute.

The CCPA's statutory/regulatory exceptions apply to businesses that are already regulated and thus need not implement the CCPA to the extent it conflicts. However, to then require those same businesses to respond to a consumer request only to deny it based on a regulatory/statutory exception, forces those businesses to incur unnecessary costs and build infrastructure, which undercuts the purpose of the statutory exception. This aim could be accomplished instead by informing customers in the CCPA notice of the applicable statutory/regulatory exception.

b. Regulation Section 999.308. Privacy Policy Conflict

Regulation section 999.308(b)(1)(d) conflicts with Code of Civil Procedure (CCP) section 1798.110, which indicates information can be provided in a more general format. Regulation section 999.308(b)(1)(d) requires businesses for “each category of personal information collected” to 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 CCPA, however, does not require this information to be disclosed for “each category of personal information collected”, and thus this Regulation section 999.308 inappropriately extends the requirements of the statute.

c. Regulation Section 999.305. Notice at Collection of Personal Information

The proposed regulation is unclear as to how a third-party collection agency should handle consumer information that was involuntarily collected. Such situations could arise after a collection agency has received and complied with a cease-and-desist order from a consumer on an account but after time the consumer elects to make a payment. The consumer directly reaches out to the collection agency via phone or online to make a payment on the account without any interaction being initiated by the agency. The agency’s phone system records the incoming phone number and/or the agency’s online payment portal collects financial information relevant for the payment. The agency was not actively pursuing payment or trying to collect this information. The proposed regulations are unclear on how or if an agency would send a notice to a consumer about the intent to collect information, when the agency had no intent to do so.

d. **Regulation Section 999.313. Responding to Requests to Know and Requests to Delete**

Regulation section 999.313 requires clarification as to how third-party collection agencies handle requests for information when voice recordings are involved.

Section 999.313 sets forth requirements regarding requests to know information and requests to delete information. A consumer has the right to request all information a business has collected. CCPA section 1798.140 lists audio information and biometric information as two of the categories of personal information. Biometric information as defined by the section includes voice prints and recordings. The proposed regulations and the CCPA address covered “information,” but recordings are a tangible. It is unclear what the expectation is when handling a consumer’s request for information when an agency has recordings. Does the agency identify that it has recordings? Does the agency produce the actual recordings and in what form? Does the agency produce a transcription of the recordings?

e. **Effective Date**

The CCPA is broad in scope and complex. Many aspects of the CCPA and the proposed regulations are still unclear and will take time for businesses to gain clarity and properly comply. We respectfully request that the Attorney General ask for a later effective date and make the rules effective 1 year after the date of issuance.

II. General Questions

Our members have many questions regarding how to harmonize the requirements of the CCPA with requirements of Federal and State Law. For instance:

- 1) Are call recordings considered personal information and, if so, how would collectors handle a consumer’s request for the recording?
- 2) Section 1798.150(c) – “Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law”—so if a person commits a violation of the CCPA there would never be a private right of action under another law?

- 3) If a consumer demands that a service provider deletes information and the service provider deletes as requested, we can envision a consumer bringing an action alleging Federal Regulatory violations that we would no longer have evidence to defend because that evidence would have been deleted. Is there anything in the CCPA that protects a service provider in these circumstances?
- 4) Does the Gramm-Leach-Bliley Act exception under 1798.145(e) apply to service providers?
- 5) Is it possible to be a “business” and “service provider” as to the same information? What would the requirements be?

III. CONCLUSION

At the public hearing on December 4th in San Francisco, there seems to be a great deal of confusion for many different types of businesses. There were comments from auto manufacturers, data collectors and providers, credit unions, different types of law firms, marketing and research firms, etc. Everyone was urging the AG to delay going forward until there is clarification as to definitions and requirements.

In addition to our comments we encourage you to take into consideration the critical comments submitted by the California Chamber of Commerce which further detail the proposed regulations impact on the broader business community and the consumers they serve both inside and outside of the state of California.

CCBA appreciates the opportunity to comment on the CCPA and proposed regulations.

Submitted by:

Sincerely,



Donald Sherrill, Esq.

President

California Creditors Bar Association

Message

From: Kate Tummarello [REDACTED]
Sent: 12/6/2019 10:47:28 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Evan Engstrom [REDACTED]
Subject: Comments on CCPA implementing regulations
Attachments: Engine CCPA regulations comments.pdf

Dear Privacy Regulations Coordinator:

Attached please find the comments of Engine Advocacy regarding the implementing regulations for the California Consumer Privacy Act.

--

Kate Tummarello
Policy Director
[Engine](#)
[REDACTED]



Engine
44 Tehama St.
San Francisco, CA 94105

December 6, 2019

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

Re: Implementing Regulations for the California Consumer Privacy Act

Dear Mr. Becerra:

Engine submits the following comments in response to the Justice Department's proposed California Consumer Privacy Act (CCPA) Regulations. We appreciate the opportunity to comment.

I. Introduction

Engine is a non-profit technology policy, research, and advocacy organization that bridges the gap between policymakers and startups. Based in San Francisco, California, and Washington, D.C., Engine works with a nationwide network of startups to understand how ongoing policy debates affect new and small high-growth technology companies and how to best advocate on behalf of the ever-changing and growing startup ecosystem in the U.S. The thriving U.S. startup ecosystem is responsible for some of the most innovative products and services, as well as the vast majority of net job growth in the country. The center of that activity is undeniably in California. Creating regulatory burdens in the name of protecting users' privacy without fully understanding the actual privacy benefits and the very real threats to startups risks unnecessarily crippling one of the most important economic sectors of our state and country.

II. Unclear, changing requirements and high compliance costs will have a disproportionate impact on startups

More so than their "big tech" competitors, startups need clarity when it comes to the obligations and responsibilities associated with privacy regulations. While CCPA does attempt to minimize burdens for "small" businesses, the small business exemption in CCPA 1789.140(c)(1)(b) will

undoubtedly fail to capture many of the state's startups that will struggle to comply with the law's most onerous burdens. For instance, a website that receives 137 unique users per day will quickly hit the 50,000 "users or devices" threshold, as would an app that is accessed by 17,000 users on an average of three devices each.

According to the standardized regulatory impact assessment completed for the department by Berkeley Economic and Advising and Research, "Small firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises."¹ The assessment cites several factors for that disproportionate impact, including the fact that small companies have fewer resources to deal with compliance costs, have less flexibility to manage evolving compliance requirements as the rules are ironed out, and are less likely to already be in compliance with the European Union's General Data Protection Regulation. That assessment also found that businesses with fewer than 20 employees will incur initial compliance costs of \$50,000, and businesses with between 20 and 100 employees will incur initial compliance costs of \$100,000. While those numbers are only part of the estimated initial compliance total cost of \$55 billion for companies complying with CCPA, the \$50,000 and \$100,000 figures can be a large part of a startup or other small business's capital.²

III. Remaining concerns with the definition of "sale" in the underlying statute

We remain concerned that the overly broad definition of the word "sale"³ and the too-narrow exception for sharing data with service providers in the underlying statute will cause the CCPA implementing regulations to have unintended consequences, especially on startups and other small businesses that—unlike large companies that can build all its capabilities in-house—routinely have to rely on a network of dozens of vendors for everyday business needs, including data processing, analytics, and payment processing. While the definition of sale does include an exception for service providers using data necessary to perform a business purpose,⁴ the statute prohibits service providers from "collect[ing], sell[ing] or us[ing] personal information of the consumer

¹Berkeley Economic Advising and Research, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations*, prepared for California Attorney General's Office (Aug. 2019): http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

² The U.S. startup ecosystem is vast and diverse and spans several industries, and it's difficult to estimate the average resources of startups. According to data released in 2009 from the Kauffman Foundation (https://www.kauffman.org/-/media/kauffman_org/research-reports-and-covers/2008/11/capital_structure_decisions_new_firms.pdf), the average high-tech startup firm launches with around \$73,000 of outside capital, with company insiders providing a similar amount. The University of New Hampshire's Center for Venture Research.

(<https://www.unh.edu/unhtoday/news/release/2016/05/25/unh-center-venture-research-angel-investor-market-2015-buyers-market>) estimated that the average angel deal size in 2015 was \$345,390, though this figure included angel deals for biotech, industrial, and energy companies which tend to have higher capital needs than Internet-enabled startups.

³ 1798.140(t)

⁴ 1798.140(t)(2)(c)

except as necessary to perform the business purpose,” and the law provides an exclusive—but narrow—list of business purposes. This limitation could prevent service providers from using the data in innocuous ways.

The problematic definition of the word “sale” is, of course, not open to amendment in the department’s rulemaking process. However, several of our concerns about the proposed implementing regulations are exacerbated by what we see as an overly broad definition of the word “sale” without adequate exceptions to account for the kind of data sharing and usages that startups and their service providers regularly engage in. And, as we discuss below, we’re concerned about language in the proposed implementing regulations that further restricts the ability of small companies to share and use data, including by creating obligations not found in the underlying statutes.

IV. Specific requests for clarity or modifications in the proposed regulations

A. **999.305(a)(2)(e)**: “Notice at collection of personal information” must “be visible or accessible where consumers will see it before any personal information is collected.”

1. We ask that the department modify this language to clarify that notices are required to be visible or accessible “at the same time as or before any personal information is collected.”

B. **999.305(a)(3)**: “If the business intends to use a consumer’s personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.”

1. We are concerned that this language creates a new affirmative opt-in requirement not found in the underlying statute that will encourage companies to be overly broad in their initial disclosures about the purposes for which the personal information will be used. That will result in notices to consumers that are unnecessarily complex and difficult for consumers to navigate without meaningfully adding to consumer privacy protections.

This would be especially true for startups, which are constantly reiterating on their products and services, including using personal information to build new features and capabilities to enhance the user experience. Those new uses of personal information typically are similar to the ways personal information is already being used, as is disclosed in the initial notice to consumers. Instead of creating a new affirmative opt-in requirement, we ask that the department require companies that seek to

use personal information in new ways to notify consumers of the new ways personal information is being used, and provide them with a mechanism to opt-out of the use of their already-collected data in new ways.

- C. **999.307(a)(1), 999.307(b)(5), 999.336(b) and 999.337(b)**: “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 retention or sale of a consumer’s personal information[.] ... An explanation of why the financial incentive or price or service difference is permitted under the CCPA, including: A good-faith estimate for the value of the consumer’s data that forms the basis for offering the financial incentive or price or service difference. ... A business may offer a price or service difference if it is reasonably related to the value of the consumer’s data. ... To estimate the value of the consumer’s data, a business offering a financial incentive or price or service difference...shall use and document a reasonable and good faith method for calculating the value of the consumer’s data.”

1. We are very concerned that the financial notice and nondiscrimination language in the department’s proposed implementing regulations goes far beyond what is required by the underlying statute, and will create unnecessary burdens for businesses without providing meaningful advances in privacy protections.

The language requiring businesses to calculate and disclose the value of a consumer’s personal information incorrectly presumes each piece of personal information collected from a consumer has an inherent and fixed value to the business, which is especially untrue for startups still iterating on their products and establishing their business models. For instance, a startup website that offers a subscription service for cooking videos may offer users a discounted subscription in exchange for data on whether each user makes it to the end of the cooking video to see an ad for a cookbook. The startup website can have no way to determine a consistent, set value for the user’s personal information as it relates to the discount in the subscription price.

Forcing businesses to define and then defend the definition of the value of consumers’ personal information will create unnecessary and onerous burdens for businesses, without providing consumers meaningful information about the tradeoffs to consider when exchanging access to their personal information for financial incentives.

- D. **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”
1. We ask that the department update this language to align it with the amended CCPA,⁵ which requires businesses that operate exclusively online and have direct relationships with consumers to provide an email address for submitting requests instead of a toll-free telephone number.
- E. **999.313(b)**: “If necessary, businesses may take up to an additional 45 days to respond to the consumer’s request [to know or delete], for a maximum total of 90 days from the day the request is received”
1. We ask that the department modify this language to align it with the amended CCPA,⁶ which allows businesses to take “up to an additional 90 days where necessary,” which—in combination with the initial 45 days—gives companies a maximum of 135 days to respond to requests to know or delete personal information.
- F. **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, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.”
1. We are concerned that this language even further constrains the way service providers can use personal information provided by the client companies that correct the personal information directly from consumers. Often service providers can optimize their product—such as by improving functionality, or detecting misuse of the product that isn’t fraudulent or illegal—by comparing usage across all clients.

For instance, a service provider that organizations use to email their users might keep a list of invalid email addresses that senders have previously encountered, causing the sending organization to receive bouncebacks. Since receiving several bouncebacks can result in a sender’s emails being deprioritized, it would benefit senders to know if they’re about to email several invalid email addresses. However, to be able to flag for

⁵ 1798.130(a)(1)(A)

⁶ 1798.145(j)(1)

senders that they're about to send an email to invalid email addresses, the service provider would have "use" personal information—in this case, an invalid email address—it obtained from one client to improve its product for all of its clients.

We worry that, by barring service providers from using personal information obtained from one client to "provid[e] services to another person or entity" except in the narrow cases of security incidents and fraudulent and illegal activity, the proposed implementing regulations would prevent service providers from being able to use the data provided by one client to improve its products for all clients in ways that don't compromise individual consumers' privacy.

- G. **999.315(c)**: "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"
1. We ask that the department provide more guidance on what "user-enabled privacy controls" should be treated as opt-out of the sale of personal information. Especially with what we see as an overly broad definition of "sale" in the underlying statute, the user controls a consumer may have set on one device at one time may not reflect how they actually want their data shared in the context of an interaction with a specific website or an app. We would encourage the department to add more nuance to the ways businesses have to respond to the entire and growing universe of user-enabled privacy controls to reflect the varying willingness of consumers to share their personal information in specific contexts.
- H. **999.317(e)**: "Information maintained for record-keeping purposes shall not be used for any other purpose."
1. We ask that the department modify this language to allow businesses maintaining records of consumer requests pursuant to CCPA be allowed to use those records for security and fraud detection and prevention purposes.
- I. **999.325(b) and (c)**: "A [reasonable/reasonably high] degree of certainty may include matching at least [two data points/three pieces of personal information] provided by the consumer with [data points/personal information] maintained by the business."

1. We ask that the department clarify that being able to match two data points in the case of a reasonable degree of certainty and three pieces of personal information in the case of a reasonably high degree of certainty does not in itself constitute a businesses having a reasonable or reasonably high degree of certainty.

V. Conclusion

Startups support giving users better and more informed control over their data, and Engine supports the overall goals of CCPA and is grateful for the work the department has done to craft thoughtful and clear implementing regulations. With the CCPA implementation date looming, we hope the department continues to refine and clarify the law to ensure California's startups can innovate and compete.

Message

From: Kathleen Lu [REDACTED]
Sent: 12/6/2019 7:51:01 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments on CCPA regulations
Attachments: Mapbox CCPA Regulation Comments - final.pdf

Please find attached written comments regarding proposed sections 999.300-999.341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations (CCR) concerning the California Consumer Privacy Act (CCPA).



50 Beale Street, Ninth Floor
San Francisco, CA 94105

03 December 2019

The following comments are submitted on behalf of Mapbox, a leading provider of map and location services, in response to a call for comments by the California Department of Justice regarding rulemaking associated with the California Consumer Privacy Act of 2018 (CCPA).

Mapbox considers the responsible stewardship of the data in our possession to be among our most important duties. This responsibility prompted us to submit comments in advance of initial CCPA rulemaking. We strongly believe that a well-designed system of privacy regulation will benefit both companies and consumers.

The draft regulations represent a meaningful step toward that goal, but businesses still face several ambiguities as they undertake compliance efforts. We believe that further improvements are possible, and we offer the following comments in the hope that they will productively contribute toward this end.

§ 999.305 - Notice of collection

Subsection (3) appears to impose a consent requirement for all business uses of personal information that were not disclosed at the original time of collection, including uses that the legislature explicitly deemed not to need consent.

While CCPA allows consumers to opt out of the sale of personal information, it does not allow consumers to opt out of the use or disclosure of information for business purposes. *Compare* 1798.110 *with* 1798.120. The legislature recognized the need of businesses to use some personal information for business purposes and gave consumers only the right to know the categories of information disclosed for business purposes. The legislature even recognized that there is some information for which the business needs outweigh consumer preferences on deletion and specifically exempted businesses from needing to comply with deletion requests when these exceptions apply (*c.f.* 1798.105(d)(1)-(9)).

Business purposes can change over time as business needs change while remaining, as recognized by the legislature, legitimate business purposes. An after-the-fact consent requirement distorts the balance the legislature struck.

This deviation from statute has the potential to introduce perverse incentives. For example, businesses that receive only IP addresses, but do not collect email addresses, phone numbers, or addresses, have no way of contacting those consumers to obtain explicit consent in the future. Under this regulation, those businesses will now be incentivized to collect more information than they would have otherwise needed solely in order to have contact information with which to seek consent under this regulation.

The Attorney General's Office should remove this subsection from the regulations.

Toll-free number

Requiring businesses that only collect data through the internet to set up a toll-free number is overly burdensome and not useful for consumers. The proposed regulations impose this burden indiscriminately:

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 application¹

This regulation appears to be out of date, as the amendments to CCPA specified:

A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information **shall only be required to provide an email address** for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

The example in § 999.312(c)(1) is also confusing:

Example 1: If the business is an online retailer, at least one method by which the consumer may submit requests should be through the business's retail website.

This example illustrates the goal of matching the method of submitting requests to the usual methods by which consumers interact with the business. But it does not mention the toll-free number at all.

§ 999.312(c)(2) does not provide any further illumination:

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

¹ Here and elsewhere in this document, quoted text has been selectively bolded for added emphasis.

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.

This formulation of examples seems to suggest that that online retailers *without* a retail location do *not* need a toll-free number. This would be sensible and in line with the legislation, but contradicts the proposed regulations.

Unnecessary toll free numbers are not without cost. A vendor has advised that operating a single toll free phone number will cost \$25 per month plus 5.9c per minute, or a minimum of \$300 annual cost to each affected business, even if the number is completely unused. But as recognized by the Federal Communications Commission, toll free number fraud is a massive problem. Toll free numbers frequently receive robocalls that are designed to churn fake traffic to increase costs for the recipient and their carrier. The originating carrier receives the increased revenue and the robocaller gets a cut, with the business paying the price². Requiring toll free numbers will make every California business that seeks to comply with CCPA a sitting duck for fraud.

The costs to the state could be massive. The Department of Justice's own forecast estimated that up to 570,066 California businesses could be impacted by CCPA³. Even ignoring the effects of fraud, requiring every business complying with CCPA to have a toll free number would be projected to drain up to \$171,019,800 from the California economy every year. For businesses that interact with consumers online, the money would be completely wasted, with absolutely no benefit to consumers.

The Attorney General's Office should redraft § 999.312(a) to make clear that businesses that only collect personal information through online methods need not provide offline methods for receiving requests. As the legislature correctly realized, a consumer whose information is collected online must necessarily have internet access and thus the ability to send an email. The Attorney General's Office should also provide more than two examples so that the myriad of different types of California businesses have guidance on regulators' expectations instead of having to read between the lines.

² <https://www.fastcompany.com/90304830/why-800-numbers-are-getting-their-own-robocalls>,
<https://ecfsapi.fcc.gov/file/06080397520310/FCC-18-76A1.pdf>

³

http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf

Webforms

Requiring businesses to set up webforms to receive requests is overly burdensome. The text of CCPA itself states that an email address is an acceptable manner of receiving requests from consumers. Almost every business that has an online presence will already have at least one email address. A CCPA-specific webform is another matter.

While setting up a webform is not a debilitating barrier, it does take some hours of work to set up properly and test. This work is of a technical nature that the average person does not have skills in. Smaller businesses with only a handful of employees may not have the technical skills and may need to hire someone to make such a form, paying significant out of pocket costs. This is the case even if that business never receives a single request from a consumer through the form.

A webform is simply a format for consumers to submit requests. It has no impact on a consumer's substantive rights under the law, nor does it aid the consumer in asserting her rights.

While webforms can no doubt assist many businesses in managing requests and responses, the state should allow businesses to determine for themselves whether a webform would assist them in organizing and responding to requests. Those businesses that anticipate significant volume in requests or have easy access to the necessary technical capabilities will voluntarily set up such forms. Those businesses that anticipate limited requests or would need to hire help can determine, after receiving some requests, whether a webform would aid in efficiency or not.

The legislature did not intend to impose an unnecessary and expensive burden on California businesses with no commensurate benefit to California consumers. In fact, the legislature specifically anticipated that businesses could receive requests via email: "A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information **shall only be required to provide an email address for submitting requests** for information required to be disclosed pursuant to Sections 1798.110 and 1798.115".

The Attorney General's office should redraft § 999.312 to remove all references to webforms from the proposed regulations or to list them only as optional alternatives to email addresses.

Definition of "sale"

A number of commentators have opined that the definition of "sale" under CCPA is so broad as to include whenever a business uses free services that involve data. For example, suppose a business wishes to count how many visitors it receives to each of its webpages. It does so by counting unique IP addresses. It of course discloses this in its privacy policy. It uses online analytics software to compare the pages and look for trends. *Did a new announcement get a lot*

of attention? Did updated graphics draw in more viewers? The business is using the data about its website visitors for its own business purposes. It receives no compensation from the analytics software provider.

But commentators have nonetheless suggested that this is a “sale” of data because the analytics software is free to use. The logic does not follow. Trial or entry versions of software are often free for many reasons, including to entice potential customers to try out the software in the hopes that they will like the features and become familiar with the platform enough to become a paying customer in the future.

While it is reasonable for the legislature to regulate the sale of data for something other than cash, such as two data brokers exchanging databases, the regulations should make clear that “sale” still means something that looks like a sale, not merely accepting free services from another business.

Definition of “disclose”

Based on public discussions, there is confusion as to which entity takes action to “collect” or “disclose” personal information in some commonplace online scenarios. It would be helpful for the regulations to shed light on this issue.

For example, if a retail business embeds a video hosted by another business on its website, the user’s browser receives certain information, such as metadata about the video, from the video hosting business when the webpage loads. It is necessary for the video hosting business to collect some personal information about the user, such as IP address, because it must know the user’s IP address in order to send information about the video to the user. This information reaches the video hosting business directly and does not pass through the retail business.

Some commentators have suggested that in this scenario, the retail business is disclosing or even selling information about the user to the video hosting business. However, the retail business never has custody of the information that goes to the video hosting business (the retail business may itself collect information such as IP address in order to deliver its own content, but that is a separate set of information). Instead, the retail business’s website refers the user’s browser to the video hosting business, and the video hosting business receives information such as IP address directly from the user’s browser. The video hosting business should of course have its own Privacy Policy detailing how it collects data from users and whether it sells that data, as should the retailer for the data it collects. However, the retailer should not be deemed to be *disclosing or selling* this data to the video hosting business, as the video hosting business is the entity *collecting* it.

The Attorney General’s Office should issue regulations clarifying this point.

Definition of service provider

Section 999.314(b) appears to contain an incomplete sentence. It reads:

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.

It appears this sentence is intended to read:

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 **that person or entity** 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.

However, as currently drafted the regulations are unclear.

Technical signals indicating opt-out

§ 999.315(c) calls for businesses to recognize "user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism" as a valid way to submit opt-out requests. Additional clarity on this matter is desirable.

Based upon the context surrounding CCPA's origins, we surmise that this provision is meant to allude to the Do Not Track (DNT) HTTP header, creating an obligation to detect users whose browsers have activated the DNT header through configuration or installed plugins. This requirement should be made much clearer.

Further, technologies exist that arguably fall under the current language of § 999.315(c), but which possess far more ambiguous status as privacy controls than DNT. A web browser ad blocking plugin, for instance, might be employed by a user for privacy; or it might be employed to improve browser performance; or it might be employed to enhance their cybersecurity posture. Other plugins could be created by any developer, without centralized coordination or standardization. It is unclear at what level of adoption or standardization businesses might be responsible for recognizing and responding to such signals.

The regulations should list specific technologies that constitute valid opt-out mechanisms so that businesses can take steps to account for them, and so that upon doing so businesses will have

certainty that their compliance obligation has been met. It may be appropriate to periodically update this list to reflect changes in technology.

In closing

We welcome the Department's attention to this matter and thank you for your consideration of these comments.

Thomas Lee
Policy Lead, Mapbox
[REDACTED]

Kathleen Lu
Senior Counsel, IP and Open Data, Mapbox
[REDACTED]

Message

From: Erin Guerrero [REDACTED]
Sent: 12/7/2019 12:27:29 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments on CCPA Regulations
Attachments: AG - Privacy Regs - 12.6.19.pdf

Please see the attached letter from the California Attractions and Parks Association concerning the Attorney General's draft California Consumer Privacy Act regulations.

Thank you.

-Erin Guerrero

Erin Guerrero

Executive Director
California Attractions and Parks Association
1127 11th St., Suite 214
Sacramento, CA 95814

[REDACTED]
www.capalink.org
[REDACTED]





Sent via email to: PrivacyRegulations@doj.ca.gov

December 6, 2019

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

Re: Comments on Proposed Text of California Consumer Privacy Act Regulations

Dear Attorney General Becerra,

California Attractions and Parks Association (CAPA) representing amusement, theme, water parks and other attractions throughout the state, is deeply concerned about the proposed California Consumer Privacy Act (CCPA) regulations circulated by your office. California's parks and attractions are unique in terms of their physical locations and sizes, their access points, and their forms of interactions with guests. While we appreciate that these proposed regulations are intended to implement California's landmark privacy legislation in 2018, we find that the draft regulations far exceed the statutory authority granted by the CCPA and create time-consuming, burdensome, and in some cases, unnecessary changes to physical and digital assets without providing any measurable benefit to consumer privacy protection. Further, the draft regulations do not distinguish between online and offline collection of consumer data which can create compliance obstacles for brick-and-mortar establishments. We appreciate the opportunity to provide the following comments on the draft regulations and urge you to address these concerns in your subsequent draft.

Proposed Regulations Go Beyond the Scope of the Statute

The proposed regulations envision a broadened and more explicit applicability to offline practices than in the statute itself. The over-emphasis on in-person collection of personal information is inconsistent with the legislative focus and attention on online collection. Furthermore the impact and requirements on in-person collection are much more diffuse and onerous than to online collection.

Notice at Point of Collection

The statutory requirement for prominent notice "at or before the point of collection" is too vague and overly broad; the proposed regulations do not provide any additional clarity on how that could be accomplished, particularly in an in-person environment.

This proposed notice provision will create unnecessary and impractical compliance obligations for California parks and attractions and other brick-and-mortar businesses. For example, it would be impractical and maybe impossible to notify a customer of data and the categories of personal information being collected prior to entering the premises. While we can generally provide

CALIFORNIA ATTRACTIONS AND PARKS ASSOCIATION

1127 11th St., Suite 214 ♦ Sacramento, CA 95814 ♦ [REDACTED]

signage at business entrances, we could not fit all of the substantive notice requirements onto such signage. Even if it were feasible to do so, such signage would not provide meaningful notice to consumers or advance the policy objectives of the CCPA.

Additionally, there seems to be a disconnect between the CCPA and the proposed regulations in this section. Pursuant to the CCPA, a business is required to give a notice “at or before the point of collection.” However, proposed Section 999.305(a)(2)(e) states that the notice at collection must “[b]e visible or accessible where consumers will see it **before** any personal information is collected.” (emphasis added). By using only the term “before,” rather than “at or before,” the section of the proposed regulations narrows the CCPA’s requirement for when notice must be provided and creates significant compliance difficulties for parks and attractions, as well as other brick-and-mortar businesses.

As with the over-emphasis on offline collection in the draft regulations, having proscriptive notice requirements for in-person notices creates huge burdens on companies like CAPA members, without commensurate consumer benefits. This is a prime example of how the draft regulations do not take into account the differences between collection of consumer data in an online versus offline environment. Businesses who operate brick-and-mortar establishments should be given more flexibility in how they provide notice and privacy policies to consumers who visit the physical premises.

Process for Submitting Requests to Know, Delete, and Opt Out

For consumers to request to know and delete their information and to opt-out of collection, §999.312(c) requires that businesses offer at least one method that reflects the manner in which the business “primarily interacts” with the consumer. We find that “primarily interacts,” is a vague term, particularly in light of the fact that our parks interact with guests in a wide variety of ways.

§999.312(f) further requires that businesses 1) treat requests that are deficient as requests that are sufficient according to the business’s request submittal process, or 2) provide the consumer with directions on how to properly submit a request or fix any deficiencies of their request.

A business with both online and retail interaction with a consumer should have the flexibility to offer either an online option for submission or a paper form depending on that particular business’s operational needs. Smaller brick-and-mortar businesses with single locations may decide that a physical paper form for submission is easier while others with multiple locations and larger operations could determine that paper forms are inefficient. In addition, the use of paper forms would be decentralized, would not be secure, and could actually jeopardize consumer privacy.

For diverse organizations like theme parks, allowing consumers to make requests via any channel and not through established portals presents an operational challenge. This provision essentially deems a request made in any way as providing actual knowledge to the operational

team required to respond. This proposed obligation on California parks and other brick-and-mortar establishments will create compliance obstacles because it does not clearly provide these businesses with the ability to designate which employees should be responsible for responding to and handling consumer requests. In this manner, the proposed regulations would potentially create even more significant CCPA compliance obligations than those for online exclusive companies that were the original focus of CCPA.

The regulations should clearly provide businesses with both a physical and online presence with the option of proscribe the appropriate process for submission requests for consumers.

Responding to Requests to Know or Requests to Delete

§999.313(d) requires that when businesses cannot verify a request to delete, the business must notify the consumer of this but then treat the request as an opt-out of sale. This proposed regulatory provision would require businesses to take an action other than what the consumer requests. The statute provides consumers with rights, and businesses should not be in the position to take an alternative action that was not explicitly requested by the consumer (or provided statutorily).

The CCPA does not require that a business, beyond the specific direction from a consumer, infer intent to submit an opt-out request. Accordingly, this provision should be deleted. Additionally, we do not believe this is a good way to honor consumer preferences. For businesses who primarily collect data in an offline setting, most of the consumer data will relate to transactional history with the particular business. If we cannot verify for identity, we may not be able to even associate the requester with any information in our systems. Responding to unverified requests in the in-person environment could be very ineffective and time-consuming.

§999.313(b) requires that businesses respond to consumer requests to know and delete within 45 days, beginning on the day that the business receives the request. Requiring businesses to take action on unverified requests will result in a waste of resources. To remedy this, the response period should only begin after the verification process has completed. Inclusion of an express, reasonable verification period would provide clarity for business and consumers.

Requests to Opt-Out of Sale

Similar to submitting requests to know and delete in §999.312(c), this section requires that business offer at least one method that reflects the manner a business “primarily interacts” with the consumer. Comments for this are in alignment with §999.312(c) above.

Training

In §999.317, the proposed regulations require that all individuals responsible for handling consumer inquiries about the business’s privacy practices and CCPA compliance shall be informed of the CCPA’s requirements and how to direct consumers to exercise their rights. They

The Honorable Xavier Becerra
December 6, 2019
Page 4

also requires that businesses which meet a certain threshold establish, document and comply with a training policy that ensure all individuals are capable of the above.

In the brick-and-mortar setting, "responsible for handling" is very different than in a traditional corporate or digital setting. As noted above, at California parks and attractions, consumers may directly encounter scores of individual employees and these proposed regulations do not afford brick-and-mortar businesses the ability to determine the appropriate channels for handling consumer inquiries.

The regulations should clearly provide that brick-and-mortar establishments have the ability to affirmatively designate employees who will be charged with handling consumer requests such that businesses can have duly-trained employees equipped to handle these requests and who alone are responsible for handling the requests.

CAPA appreciates your consideration of these comments and suggestions. The Amusement Parks and Attractions Industry supports protecting consumer privacy and our comments are offered in the spirit of ensuring that the regulatory requirements provide a reasonable standard for compliance and provide actual privacy protection for consumers. We look forward to working with you to address these serious concerns.

Yours truly,



Erin Guerrero
Executive Director

Message

From: Recht, Philip R. [REDACTED]
Sent: 12/6/2019 7:27:57 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments on draft CCPA regulations
Attachments: 4069_001.pdf

Please find attached above our comments on the draft CCPA regulations. Should you have any questions, please do not hesitate to get in touch. Thanks. Phil.

Philip R. Recht
Mayer Brown LLP
350 S. Grand Avenue, 25th Floor
Los Angeles, CA 90071

[REDACTED]

This email and any files transmitted with it are intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. If you are not the named addressee you should not disseminate, distribute or copy this e-mail.

Mayer Brown is a global services provider comprising an association of legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauli & Chequer Advogados (a Brazilian partnership).

Information about how we handle personal information is available in our [Privacy Notice](#).

December 6, 2019

Philip R Recht

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

Re: Proposed regulations interpreting the California
Consumer Privacy Act

Dear To whom it may concern:

I. Introduction. Our firm represents a coalition of online companies that provide e-commerce fraud prevention, background report, and other people search services. These services are widely used and highly valued by law enforcement and other government agencies, businesses, and individuals and families alike.

Unlike businesses that collect personal information (PI) directly from consumers, these companies collect information about consumers only from public and other third party sources. The companies do not otherwise have direct relationships or accounts with the consumers whose PI they collect and make available. The vast majority of the PI collected by the companies is in the public domain (e.g., yellow and white page phone book data, non-private social media data).

We send this letter to provide comments on the draft regulations, issued October 10, 2019 by the Department of Justice (DOJ), interpreting the California Consumer Privacy Act (CCPA). This letter supplements our earlier comment letters—dated February 13, 2019 and September 30, 2019—on the same subject. A copy of the September 13, 2019 letter, which contains much analysis relevant to the issues discussed herein, is attached and incorporated herein by reference.

As discussed in detail below, three provisions of the draft regulations are legally untenable. First, and of greatest concern, is 20 CCR section 999.305(d).¹ This section unlawfully would relieve businesses that do not collect PI directly from consumers of the need to provide notice (hereinafter the “pre-collection notice”) at or before they collect consumers’ PI, notwithstanding the CCPA’s clear mandate that such notice be provided. As a substitute for the CCPA’s mandatory pre-collection notice, section 999.305(d) provides that, before such a business can sell a consumer’s PI, the business must either (a) directly contact the consumer to provide notice that the business sells PI about the consumer and of the consumer’s opt rights, or (b) obtain an attestation that the source of the PI already provided the consumers such direct notice. This substitute compliance scheme itself is unlawful since it directly conflicts with the CCPA’s clear mandate that the opt out

¹ All further section references beginning with the numbers “999” refer to 20 CCR.

The California Department of Justice
December 6, 2019
Page 2

notice (hereinafter the “pre-sale notice”) be provided by businesses on their Internet homepages. Further, the proposal would lead to harsh and unreasonable results given the unworkable and impracticable nature of both the direct notice and attestation options. For a host of reasons, including the fact that the collection and use of public domain data constitutes Constitutionally protected speech that cannot be unreasonably abridged, the regulations more appropriately should allow businesses that do not collect PI directly from consumers to provide the pre-collection notice on their Internet homepages.

Second, the requirement in section 999.315(f) that, upon receipt of a consumer’s opt out request, businesses notify all third parties to whom they have sold they consumer’s PI within the prior 90 days, instruct such third parties to not further sell the PI, and then notify the consumer when this has been completed equally finds no authority in the CCPA. Moreover, absent an initial promise by the purchasing party not to resell the PI, the proposal would unconstitutionally impair the right of contract. This proposed requirement should be eliminated.

Finally, the requirement in section 999.317(g) that businesses that handle the PI of four million or more consumers compile metrics concerning the number of consumer requests to know, delete, and opt out and the time taken to respond to such requests and then post such information on their websites or privacy policies once again finds no authority in the CCPA. At least with respect to businesses that qualify as data brokers, this requirement also is at odds with the approach of the newly created data broker registry. As such, this proposal also should be eliminated.

Beyond their lack of statutory authority and other legal flaws, these three provisions each conflict with comparable provisions of the newly introduced initiative entitled the California Privacy Rights Act of 2020 (CPRA). That new initiative was developed by the proponent of the initiative that prompted the enactment of the CCPA (Alastair MacTaggart) and the co-author of the CCPA (Sen. Robert Hertzberg) for the purpose of strengthening and expanding the consumer rights provided by the CCPA. Assuming the CPRA is enacted in November 2020, which on present facts seems likely, the three provisions of the draft regulations would conflict with yet additional statutory provisions, creating yet further illegality.

II. Section 999.305(d)’s pre-collection notice proposal.

A. The regulation’s proposed notice scheme unlawfully conflicts with the CCPA’s pre-collection and pre-sale notice requirements. The pre-collection notice requirement set forth in the CCPA is clear and unambiguous. Specifically, Civil Code section 1798.100(b)² provides 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.” (Emphasis added.) The CCPA is silent as to the manner in which such pre-collection notice is to be provided. As such, the manner of providing such notice is an appropriate topic for rulemaking. Still, there is nothing

² All further section references beginning with the numbers “1798” are to the Civil Code.

The California Department of Justice
December 6, 2019
Page 3

silent or unclear about the timing of the notice. It must be provided “at or before the point of collection.” Section 1798.100(b) is equally clear that the notice requirement applies to all covered businesses that collect PI, regardless how they collect it.

Nor is there any question as to whether this is a mandatory notice. Section 1798.100(b) provides that businesses “shall” provide the notice. It is hornbook law that “[t]he word ‘shall’ means that the act is mandatory,” not optional. *Chaney v. Netterstrom*, 21 Cal. App.5th 61, 66 (2018); *Woods v. Department of Motor Vehicles*, 211 Cal. App. 3d 1263, 1272 (1989) (“The word ‘shall’ is ordinarily used in laws, regulations, or directives to express what is mandatory.”). Section 999.301(i) of the proposed regulations seemingly acknowledges both the mandatory nature and required timing of the CCPA’s pre-collection notice requirement, defining “[n]otice at collection” as “the notice given by a business to a consumer *at or before the time a business collects [PI] from the consumer as required by Civil Code section 1798.100(b)...*” (Emphasis added.)

The CCPA’s pre-sale notice requirement is spelled out in equally clear terms. Section 1798.120(b) provides that businesses that sell PI to third parties “shall” provide notice to consumers of their right to opt out pursuant to section 1798.135. Section 1798.135(a), in turn, provides that a business “shall” provide such notice by way of a “clear and conspicuous link on the business’ Internet homepage,” as well as in “[i]ts online privacy policy” and any “California-specific description of consumers’ privacy rights.”

Notwithstanding this statutory clarity, section 999.305(d) proposes a scheme that conflicts with the CCPA’s pre-collection and pre-sale notice requirements. Specifically, subsection 999.305(d)(1) first proposes to eliminate the mandatory pre-collection notice requirement, providing that a business that does not collect PI directly from consumers “does not need to provide a notice at collection to the consumer.”

As a substitute for the pre-collection notice, subsection 999.305(d)(2) proposes that, before an affected business can sell a consumer’s PI, the business must either (1) contact the consumer directly to provide notice that the business sells the consumer’s PI and of the consumer’s right to opt out, or (2) contact the source of the PI to confirm the source provided the consumer with pre-collection notice in accordance with sections 999.305(a) and (b) (which ostensibly require direct, individualized notice), and obtain a signed attestation from the source describing how the source provided the pre-collection notice and including an example of the notice.

Clearly, DOJ “may not adopt a rule which would conflict with the enabling or otherwise governing statute.” *Dept. of Alcoholic Beverage Control v. Alcoholic Beverage Control Appeals Bd.*, 71 Cal.App.4th 1518, 1520 (1999); *Agricultural Labor Relations Bd. v. Superior Court*, 16 Cal.3d 392, 427 (1976). As stated in *Harris v. Alcoholic Bev. Etc. Appeals Bd.*, 228 Cal.App.2d 1, 6 (1964):

“[An administrative agency] may not exercise its sub-legislative powers to modify, alter or enlarge the provisions of the legislative act which is being administered. Administrative

The California Department of Justice
December 6, 2019
Page 4

regulations in conflict with the Constitution or statutes are generally declared to be null or void.”

Government Code section 11342.2 equally bans regulations that are inconsistent with their underlying statutes, providing:

“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.”

Despite this clear prohibition, section 999.305(d) openly and irreconcilably conflicts with two unambiguous CCPA mandates. It proposes to (1) relieve businesses that collect PI from sources other than consumers of CCPA’s requirement, applicable to all businesses that collect PI, to provide notice of their collection activities at or prior to the time of collection, and (2) require the affected businesses instead to provide consumers with direct notice of their opt out rights, as opposed to Internet homepage notice of such rights as mandated by the CCPA.

The fact that subsection 999.305(d)(2) provides an alternative compliance option (i.e., obtaining an attestation that the original source of the PI provided the consumer direct pre-collection notice) does not save the remaining illegal portions of the regulation. The attestation option’s only purpose is to serve as a substitute for the CCPA pre-collection notice requirement from which subsection 999.305(d)(1) purports to excuse compliance. Since subsection 999.305(d)(1) is illegal, the substitute provisions found in subsection 999.305(d)(2) must necessarily be unenforceable as well. Regardless of the fate of the attestation option (and see below for a discussion as to how it is independently improper), section 999.305(d)’s proposals to eliminate the pre-collection notice and require direct, as opposed to homepage, opt out notice so directly and overtly conflict with the CCPA as to be unlawful on their face.

B. The proposed notice scheme is unworkable and unreasonable. Even if the law allowed DOJ to substitute a reasonable alternative pre-collection notice requirement for CCPA’s mandatory one (which it doesn’t), subsection 999.305(d)(2)’s proposal to instead require a business to provide direct notice of its intent to sell a consumer’s PI and the consumer’s opt out rights or, instead, obtain an attestation that the original collector of the PI provided direct notice to the consumer would still fail. As explained in our earlier comment letters, businesses without direct consumer relationships are often no more capable of providing direct notice after collection than at or before collection. In many cases, the PI collected by these businesses does not contain contact information. When it does, the contact information, not coming directly from the consumers themselves, often is outdated, incomplete, or otherwise inaccurate. As such, it cannot be counted on to provide reliable and effective direct notice. Thus, subsection 999.305(d)(2)’s direct notice option is not practicable or workable for the businesses in question.

The California Department of Justice
December 6, 2019
Page 5

The same is true of the attestation option. In the vast majority of cases, the PI collected by these businesses comes from other third party sources that themselves are unable to provide direct notice to the consumers. In those few instances where the businesses obtain PI from an original source (or somehow can identify the original source and make contact with it), those sources have little, if any, incentive to provide the businesses with signed attestations of their compliance with the CCPA's notice requirements and examples of their notices, particularly when doing so exposes those sources to new and unknown potential legal liabilities. Thus, even if DOJ lawfully could propose a reasonable alternative to section 1798.100(d)'s mandatory pre-collection notice requirement (which it cannot), the alternative proposed in subsection 999.305(d)(2) is so impracticable and unworkable as to provide the affected businesses no effective means of complying with the CCPA's pre-collection notice requirement. With no way to comply, many of those businesses—including companies like our clients that generate revenues exclusively from the sale of consumer PI—would have no choice but to go out of business or, at a minimum, cease all business involving California consumer PI.³

The law will not tolerate such harsh and unreasonable results, particularly where, as discussed below, reasonable alternatives exist; also, where the enactment of AB 1202 establishing a data broker registry so clearly indicates the legislature's intent that these businesses continue to operate in the state. *Kinney v. Vaccari*, 27 Cal.3d 348, 357 (1980) ("It is a well-settled maxim of statutory construction that a statute is to be construed in such a way as to render it reasonable, fair, ... harmonious with its manifest legislative purposes, and ... to avoid harsh results and mischievous or absurd consequences."); *Shirley v. Los Angeles County civil Service Com.*, 216 Cal. App.4th, 1, 20 ("We interpret a statute to avoid untenable distinctions and unreasonable results whenever possible.).

C. Allowing for Internet homepage notice is a reasonable alternative. The good news is that there is another approach—i.e., Internet homepage notice—that would allow businesses without direct consumer relationships to provide pre-collection notice in a practicable, effective, and lawful fashion. A detailed discussion of the reasons why homepage notice is reasonable and appropriate is contained in our incorporated September 30, 2019 comment letter and will not be repeated in full here. In summary, however, businesses without direct consumer relationships lack the practical ability to provide direct consumer notice at or before collection.⁴ Prior to collection, the businesses lack any information, contact or otherwise, concerning the consumers. At the time of collection, much of the collected PI does not contain contact information. Even when it does, the contact information typically is unusable until after sorting and manipulation into a uniform and

³ Given the size of the California market, the difficulty of separating the PI of California consumers from consumers in other states (particularly when that PI does not include location information, as it often does not), and the difficulty of knowing for certain if a consumer is a California resident (particularly in the case of consumers who reside in multiple states including California, but for whom the companies have contact information only for non-California states), the inability of these companies to comply with the CCPA genuinely poses an existential threat to their existence.

⁴ Section 999.305(d)'s proposal to relieve these businesses of the need to provide pre-collection notice inherently acknowledges this fact.

The California Department of Justice
December 6, 2019
Page 6

usable format, a process that requires days, weeks, or even months to perform.⁵ Thus, the only practicable way for these businesses to provide the pre-collection notice is on their Internet homepages.

Providing homepage notice would be consistent with the CCPA's other notice requirements and consumer expectations. Specifically, homepage notice would be consistent with the CCPA's requirement that businesses provide consumers with notice of their opt out rights (i.e., the pre-sale notice) on the businesses' Internet homepages. It also would be consistent with the manner in which consumers typically search for online company disclosures, including those concerning company privacy policies and practices. See section 1798.140(l) defining "homepage" to include an introductory page of an Internet web site, a download, page, a link within an app, an "about" or "information" page, or any other location that allows a consumer to review the opt out notice.

Homepage notice is also consistent with the new data broker registry created by AB 1202. That bill was developed and enacted by the legislature to address the same concern that assumedly underlies section 305(d)'s proposed pre-collection notice scheme—i.e., that because businesses without direct consumer relationships cannot provide direct notice, consumers might not know of these businesses' existence and thus be unable to exercise their CCPA rights. Rather than prevent these businesses from providing their valuable and popular services as the proposed regulations would do, the legislature decided to facilitate the businesses' compliance with the CCPA by creating a registry on which businesses without direct consumer relationships that collect and sell consumer PI—defined as "data brokers"—must be listed, along with their contact information and such other information about their data collection practices as the businesses wish to disclose. The registry thus provides consumers an easily accessible means to identify businesses with which they do not have direct relationships but which collect PI about them, find out what PI the businesses have collected, and opt out if they so desire. *See Senate Rules Committee Analysis*, 9/6/19, at pp. 5-6; *Senate Judiciary Committee Analysis*, 6/21/19, at p. 70). In doing so, the registry obviates any policy concerns with the Internet homepage notice option.

Homepage notice also prevents the harsh and unreasonable, indeed absurd, results that would obtain from a direct pre-collection notice requirement. Since businesses without direct consumer relationships lack the ability to provide direct consumer notice at or before they collect consumer PI,⁶ a direct notice requirement would force the businesses to shut down entirely, or at least with respect to California consumer PI.

Even if the businesses somehow could provide direct notice to the tens of millions of California consumers whose PI is collected in some measures by these businesses, the cost of doing so would be so enormous as to pose yet another existential threat to the businesses' survival.⁷ Worse yet, it

⁵ Even then, the contact information often is outdated, incomplete, or otherwise inaccurate, as noted above.

⁶ See attached correspondence dated September 30, 2019 at pp. 1-2 for a detailed explanation as to why direct pre-collection notice is impossible for these businesses.

⁷ See September 19, 2019 correspondence at p. 2 for a more detailed discussion of the cost implications of this concept.

The California Department of Justice
December 6, 2019
Page 7

would result in tens of millions of California residents receiving precisely the kind of unsolicited email, text, telephone, or mail contacts that consumers find so annoying and intrusive and that various consumer protection laws (e.g., TCPA, CAN-SPAM) are meant to prevent. Further, such blanket notice almost certainly would lead to the same kind of rampant consumer scams that plagued EU residents when GDPR first took effect and EU residents were flooded with email notices from companies with which they were not familiar. See <https://www.thesun.co.uk/tech/6375142/gdpr-email-scams-police-warning>; search “gdpr email scams” for more such articles. Such unacceptable results cannot possibly be what the legislature envisioned in enacting the CCPA, and certainly is not what the legislature intended in creating the data broker registry. And, as noted above, the law will not tolerate such unreasonable results when a reasonable alternative approach—i.e., homepage notice—is available.

Perhaps the most compelling proof of the reasonableness of homepage notice is the fact that the newly introduced CPRA initiative explicitly provides for homepage notice as the appropriate means for businesses without direct consumer relationships to meet the pre-collection notice requirement. Specifically, the CPRA would move the pre-collection notice requirement into section 1798.100(a) and then amend section 1798.100(b) to read as follows:

“A business that, acting as a third party, collects personal information about a consumer may satisfy its obligation under subdivision (a) by providing the required information prominently and conspicuously on the homepage of its Internet website. In addition, if the business, acting as a third party, collects personal information or authorizes another person to collect personal information, about a consumer while the consumer is proximate to a physical location at which the personal information is collected, then the business shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes or which the categories of personal information shall be used, and whether such personal information is sold, in a clear and conspicuous manner at such location.”

As noted above, the CPRA was developed by two of the principal movers behind the CCPA—Alastair MacTaggart and Sen. Robert Hertzberg—for the purpose of strengthening the CCPA and consumer rights, including with respect to the topics covered by the pre-collection notice. See CPRA, Sections 2.E, G, and H (declaring that California should strengthen its privacy rights, mandate laws that will allow consumers to understand more fully how their PI is being used, and provide consumers with clear explanations of the uses of their PI); Section 3.A, B (indicating purpose and intent to allow consumers to know who is collecting their PI and to require businesses to clearly inform consumers about how they collect and use PI).

To accomplish these goals, the CPRA provides that businesses without direct consumer relationships may provide the pre-collection notice on their Internet homepages. In doing so, the authors of the CPRA provide yet further, and highly compelling, evidence of the reasonableness and appropriateness of this approach.

The California Department of Justice
December 6, 2019
Page 8

Finally, homepage notice is consistent with, if not required by, the fact that the collection and dissemination of PI in the public domain constitutes Constitutionally protected speech that can only be restricted by laws or regulations that are narrowly tailored to further a compelling government interest. *United States v. Playboy Entm't Grp., Inc.*, 529 U.S. 803, 813 (2000); *The Fla. Star v. B.J.F.*, 491 U.S. 524, 541 (1989) (the truthful publication of lawfully obtained information falls within the First Amendment's ambit and may only be restricted when narrowly tailored to a state interest of the highest order.). The fact that companies receive compensation for these activities does not diminish this "strict scrutiny" level of Constitutional protection. *City of Lakewood v. Plain Dealer Publ'g Co.*, 486 U.S. 750, 756 n.5 (1988). Only when speech proposes a commercial transaction does a more intermediate level of scrutiny apply, and even then such speech cannot be infringed absent a substantial government interest and a showing that no less onerous restrictions will serve that interest. *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557, 562, 566 (1980).

The activities of our client companies and other similarly situated businesses, of which there are many,⁸ do not propose commercial transactions. As such, the strict scrutiny test applies to section 305(d)'s notice proposal, as well as any other provisions of the proposed regulations that would impair the ability of these companies to continue to engage in these activities.

But, even if the intermediate test applied, section 305(d) would not pass muster. First, it is unclear what government interest this notice requirement would address. The government cannot claim a broad interest in privacy alone. *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1235 (10th Cir. 1999). And, it is hard to see how an onerous notice requirement that effectively prevents the dissemination of non-confidential data that already is in the public domain could address the more specific interests articulated in the CCPA—i.e., protecting consumers from security breaches, financial fraud, and identity theft. Section 1798.100; *see also*, Senate Judiciary Committee Analysis, AB 375, 6/25/2018, at pp. 1-2.

Further, even if a restriction on the use of public domain data was relevant to these purposes, which it is not, the notice scheme proposed by section 305(d) is far from being narrowly tailored to further, or otherwise the least onerous means of achieving, the purposes. Internet homepage notice, which itself arguably burdens speech impermissibly, certainly is a more reasonable and, as such, Constitutionally required approach.⁹

⁸ As one indicator of the number of businesses affected section 305(d)'s notice proposal, the Vermont data broker registry, which most observers believe covers fewer businesses (because of its narrower definition of "data broker") than the newly recreated California data broker registry, has approximately 140 registered companies.

⁹ Recognizing the severe Constitutional problems in the CCPA's attempt to regulate the collection and dissemination of public domain data and the risk this legal flaw poses to the entirety of the CCPA, the CPRA extends the CCPA's exemption for "publicly available" information (currently limited to government records data) to include all public domain data as well. CPRA, section 1798.140(v)(2).

The California Department of Justice
December 6, 2019
Page 9

For the numerous reasons discussed above, section 999.305(d) should be amended to remove the currently proposed language and instead to allow for Internet homepage notice by businesses that do not collect PI directly from consumers.

III. Section 999.315(f)'s downstream opt-out notification requirement. Section 999.315(f) suffers from the same defects as section 999.305(d) and must be eliminated for similar reasons. Section 999.315(f) would require a business in receipt of a consumer's opt out request to notify all third parties to whom it has sold the consumer's PI within the 90 days prior to the consumer's opt out, instruct those third parties not to further sell the PI, and then notify the consumer when these tasks have been completed.

This provision is improper for at least two reasons. First, there are no similar provisions in the CCPA providing for downstream notice of a consumer's opt out decision, let alone requiring downstream buyers to refrain from reselling the PI. Equally, there are no similar provisions in the CPRA. At most, the CPRA, in section 1798.100(d), requires buyers and sellers of PI to enter into contracts specifying the purposes for which the PI can be used by the buyer. However, nothing in the CPRA prohibits resale of the PI or requires any downstream notice of a consumer's opt out decision. As such, section 999.315(f)'s imposition of new downstream notice, resale prohibition, and consumer notification requirements find no authority either in the statute it purports to interpret or in the likely successor to that statute. Imposing these not insignificant new requirements in the regulations constitutes precisely the type of statutory alterations and enlargements the law prohibits.

Second, nothing in the CCPA (or CPRA) prevents a buyer or other acquirer of PI from reselling the PI absent a restriction to that effect in the contract between the buyer and seller. As such, section 999.315(f)'s prohibition on the resale of an opting-out consumer's PI impairs the contractual rights of those PI buyers who did not voluntarily agree to such a resale restriction, all in violation of the federal and California constitutions. US Const., art. I, section 10, cl. 1; CA Const., art. I, section 9 ("A bill of attainder, ex post facto law, or law impairing the obligation of contracts may not be passed."); *see also Deputy Sheriffs' Assn. of San Diego County v. County of San Diego*, 233 Cal.App.4th 573, 578 (2015) ("Article 1, section 9 of the California Constitution prohibits the passage of a 'law impairing the obligation of contracts.'"); *Teachers' Retirement Bd. v. Genest*, 154 Cal.App.4th 1012, 1026 (2007) ("The contract clauses of both the federal and California Constitutions prohibit a state from passing laws impairing the obligation of contracts."); *La Costa Condominium Owners Assn. v. Seith*, 159 Cal.App.4th 563, 584-5 (2008)) ("The obligations of a contract are impaired by a law which renders them invalid, or releases or extinguishes them.").

For these various reasons, section 999.315(f) is unlawful and should be deleted.

IV. Section 999.317(g)'s requirements for large data processors. Section 999.317(g) provides that a business that annually processes (i.e., buys, receives for commercial purposes, sells, or shares for commercial purposes) the PI of four million or more consumers must compile metrics for the number of requests to know, delete, and opt out that the business received, complied with

The California Department of Justice
December 6, 2019
Page 10

in whole or part, or denied, as well as the median number of days within which the business responded to the requests, and then disclose that information in its privacy policy or post it on its website in a fashion that is accessible from a link included in its privacy policy.

Once again, nothing in the CCPA even comes close to requiring any similar data collection and publication exercise. Similarly, nothing in the CPRA contains any similar requirements. At most, the CPRA requires businesses whose processing of consumers' PI presents significant risk to consumers' privacy or security to perform annual cybersecurity audits and risk assessments. CPRA, section 1798.185((a)(15)). As such, section 999.317(g)'s proposed data collection and publication requirements lack the necessary statutory authority and are unlawful.

At least with respect to businesses that qualify as data brokers, section 999.317(g)'s mandatory data collection and publication requirements additionally conflict with AB 1202's voluntary approach to the publication of consumer data. Specifically, while section 1798.99.82(b)(2), added by AB 1202, requires data brokers to publish on the registry their name and primary physical, email, and internet website addresses, it permits (but does not require) data brokers to publish "[a]ny additional information or explanation the data broker chooses to provide concerning its data collection practices." Even assuming the phrase "data collection practices" is broad enough to cover a data broker's handling of requests to know, delete, and opt out, section 1798.99.82(b)(2), in accordance with the legislature's judgment, leaves the decision whether to collect and publish this data strictly up to the data broker. Section 999.317(g)'s contrary approach—requiring businesses to collect and publish the data—conflicts with AB 1202, adding to section 999.317(g)'s illegality with respect to data brokers.

Given its lack of statutory authority and its further conflict with AB 1202, section 999.317(g) should also be deleted.

V. Conclusion. As a seminal principle of administrative law, regulations must be properly authorized by and otherwise comport with the statute they propose to interpret. The three draft regulatory provisions discussed above demonstrably do not meet this requirement and, for this reason alone, are unlawful and unenforceable. Each of the provisions suffers from other infirmities too, but none so much as the notice provision of section 305(d) which, among other things, violates federal and state Constitutional free speech protections. Each of the provisions should be amended or deleted as suggested above.

Sincerely,



Philip R. Recht

Enclosure

September 30, 2019

Philip R. Recht

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

Re: Proposed CCPA Regulations

To whom it may concern:

Our firm represents a group of online companies that provide background report, e-commerce fraud detection, and other people search services. We send this letter to supplement our initial comment letter, dated February 13, 2019, concerning the potential content of the CCPA interpretive regulations your office is drafting.

Since our earlier comments, there have been significant legislative and related developments with respect to three of the issues addressed in the comments. Specifically, the legislature enacted AB 874, incorporating the regulatory solutions we had proposed on the topics of (1) determining what data is "capable of" constituting personal information (PI), and (2) clarifying the allowable uses of government records data. Assuming the governor signs AB 874, our proposed regulatory solutions on those issues no longer are necessary.

The legislature also enacted AB 1202, establishing a data broker registry. This development is relevant to the issue of clarifying how the pre-collection notice required under Civil Code section 1798.100(b)¹ may be provided by businesses that, like our clients, collect PI about consumers from public and other third party sources but do not have direct relationships or accounts with such consumers. As discussed below, the creation of a registry supports our suggestion that such businesses be allowed to provide pre-collection notice on their Internet homepages. It also provides an additional location—the registry itself—where businesses that are data brokers can post the notice.

Also, in recent days, the proponents of the proposed initiative that led to the enactment of the CCPA have submitted a proposed follow-up initiative called 'The California Consumer Privacy Act of 2020. This new initiative, intended by the proponents to strengthen the CCPA and consumer privacy rights, explicitly allows for the pre-collection notice to be provided on Internet homepages and, as such, equally supports our proposal on the topic.

¹ All further statutory references are to the Civil Code.

The California Department of Justice
September 30, 2019
Page 2

I. Nature of the pre-collection notice issue. The CCPA requires covered businesses to provide consumer notice in two instances—(1) at or before collection of a consumer's PI (section 1798.100(b)), and (2) before sale of a consumer's PI (section 1798.115(d)). While the CCPA specifies that a covered business must provide the pre-sale notice (i.e., an opt out link) on the business' Internet homepage and in its online privacy policy (sections 1798.120(b), 1798.135), the CCPA does not specify how a business may or must provide the pre-collection notice.

II. Reasons why homepage notice is appropriate. There are numerous reasons why it is appropriate to allow businesses without direct consumer relationships to provide pre-collection notice on their Internet homepages. Specifically:

A. Homepage notice is the only practicable means of providing such notice. Per section 1798.100(b), the pre-collection notice, requiring a description of the categories of PI collected and the purposes for which the PI is to be used, must be provided "at or before" the PI is collected. Businesses that have direct relationships (i.e., are in direct communications) with consumers readily can (and already typically do) provide direct, individualized notice to consumers at or before collecting a consumer's PI. For example, businesses such as Amazon, Twitter, Ebay, and Facebook that collect PI directly "from" the consumers that access the businesses' sites all place links to their privacy policies on their homepages and require that the consumers acknowledge and approve the policies before allowing the consumers to provide their PI to the businesses.

While this is easy, indeed effortless, for businesses in direct communication with consumers, it is an impossible task for our clients and the hundreds, if not thousands, of other covered businesses that collect PI "about" consumers with whom the businesses are not in direct communication (i.e., do not have direct relationships).² This is certainly the case "before" the businesses collect the consumers' PI since, at that time, the businesses lack any information, contact or otherwise, about the consumers. As such, direct communication with the consumers for notice or any other reason is impossible.

Notice "at" the time of collection similarly is impossible. First, much of the PI collected by these businesses (e.g., education and employment histories, social media profiles) does not contain contact information. Without contact information, individualized communication is impossible. Even when contact information is collected, it typically is unusable at the time of collection. These businesses manage literally billions of records that are obtained from thousands of sources and that arrive at the businesses in a multitude of formats. The data must

² This letter is focused on our clients' business model of collecting public and other information about consumers with whom they do not have direct relationships. However, our clients are also e-commerce businesses that have direct relationships and communications with the consumers that use their services. This letter is not intended to suggest that our clients be excused from providing direct, individualized pre-collection notice to consumers with whom they have direct relationships. Much like the popular consumer-facing referenced on page 1 above, our clients can and will provide direct, individualized pre-collection notice to consumers with whom they have direct relationships.

The California Department of Justice
September 30, 2019
Page 3

then be sorted and manipulated into a uniform and usable format, a process that requires days, weeks, or even months to perform. The bottom line is that even when contact information is among the PI collected by these businesses, it is not usable “at” the time of collection. Thus, individualized notice is impossible then as well.³

Even when the data subsequently becomes usable, individualized notice would be impracticable and ineffectual. First, the contact information collected by these businesses from phone books, social networks, and marketing surveys—i.e., the publicly available sources typically used by these businesses—is not subject to validation requirements such as those found in the Fair Credit Reporting Act; nor does it have the accuracy of information originating from financial transactions under the Gramm-Leach-Bliley Act. As such, the contact information often is out-of-date, incomplete, or inaccurate and, as a result, cannot be counted on to result in the delivery of reliable and effective notice in numerous cases.

Second, providing direct, individualized notice to the literally tens of millions of California residents whose PI is collected in some measure by these businesses is cost-prohibitive. To send emails, texts, or postcards to this number of persons would require the businesses to engage third party services that specialize in mass communications, all at a cost of hundreds of thousands, if not millions, of dollars annually. Costs of this size would put a significant financial strain on these businesses. In some cases, it could immediately put them out of business. This would be an unjust outcome for businesses that are engaged in constitutionally-protected commercial activity involving the collection of information in the public domain and that provide services widely used and valued by law enforcement, other government agencies, businesses, and individuals and families alike.

Given all this, the best and only way that covered businesses without direct consumer relationships can provide pre-collection notice is on their Internet homepages. (As noted below, those such businesses that qualify as data brokers may additionally provide such notice on the data broker registry).⁴

B. Homepage notice is consistent with CCPA’s other notice requirement and consumer expectations. As noted, the CCPA requires that, before selling a consumer’s PI, a business provide the consumer with notice of the right to opt out of (i.e., prevent) the sale. The CCPA requires that this notice, which assumedly is equally if not more important to the

³ It has been suggested that businesses without direct consumer relationships should be allowed a period of days after the time of collection to provide individualized notice. Allowing for notice to be delayed until a later date would conflict with section 110(b)’s clear mandate for notice to be give “at or before” collection and, thus, be unlawful.

⁴ It may be possible for a business without direct consumer relationships to provide direct notice in one scenario. Specifically, to the extent a business uses technological devices such as wifi sniffers or cameras to collect PI about consumers when those consumers are at a physical location (e.g., a coffee shop), the business could provide direct (albeit not individualized) pre-collection notice to the consumers by a visible notice posted at the physical location. (We have no objection to requiring direct notice in that scenario.) However, there is no comparable scenario by which businesses that do not collect PI at physical locations could provide direct, individualized notice.

The California Department of Justice
September 30, 2019
Page 4

consumer than the pre-collection notice (which is not accompanied by any opt out right), must be provided on the business' Internet homepage. Allowing businesses without direct consumer relationships to provide pre-collection notice in the same fashion would be consistent with this approach.

It also would be consistent with the manner in which consumers typically search for online company disclosures, including those concerning company privacy policies and practices. This fact is reflected in the CCPA's broad definition of "homepage" (section 1798.140(1)), which includes an introductory page of an Internet web site, as well as a download page, a link within an app, an "about" or "information" page, or any other location that allows consumers to review the notice required by section 1798.135(a).

C. Concerns about the lack of individualized notice are mitigated by AB 1202's creation of a data broker registry. AB 1202, authored by Ass. Chau, the co-author of the CCPA, requires that businesses without direct consumer relationships that both collect and sell consumer PI—defined as "data brokers"—be listed, along with their contact information and such other information about their data collection practices as the data brokers wish to disclose, on a public registry maintained by the Attorney General. AB 1202 was intended to address the concern that, given the inability of these businesses to provide direct notice to consumers, consumers would not know of the business' existence and, thus, could not exercise their CCPA rights. As stated in committee analyses:

"Many of the CCPA's provisions require consumers to know which entities have their personal information before they can properly exercise their rights. The data brokers discussed above, by definition, do not have direct relationships with consumers and can essentially amass personal information on consumers with their permission or knowledge." (Senate Rules Committee analysis, 9/6/19, at pp. 5-6.)

"By requiring the names and contact information for these data brokers to be systematically collected and made easily accessible to consumers, the bill allows consumers to have more meaningful control over their personal information. Consumers would be able to go to this list and contact each of these data brokers to find out what information each had collected on the consumer and to demand that the data brokers cease their sales of that information if the consumer so wished." (Senate Judiciary Committee analysis, 6/21/19, at p. 7.)

AB 1202 is relevant to the pre-collection notice issue for three reasons. First, even though limited to businesses that both collect and sell PI, AB 1202 reflects the legislature's understanding, and thus confirms, that businesses without direct consumer relationships cannot feasibly provide direct, individualized notice to consumers. If direct, individualized notice was feasible by these businesses, AB 1202 and the registry it creates would be unnecessary.

Second, AB 1202 ensures that the names and contact information of these businesses will be made "easily accessible" to consumers, thus facilitating the consumers' ability to exercise their

The California Department of Justice
September 30, 2019
Page 5

various CCPA rights. In doing so, AB 1202 obviates the one and only policy concern—i.e., the potential information gap—raised with respect to allowing pre-collection notice on Internet homepages.

Third, AB 1202 permits data brokers to list on the registry any information or explanation about their data collection practices that they wish. This enables the data brokers to provide the pre-collection notice not only on their homepages but also directly on the registry itself. We would suggest that the Attorney General encourage such additional postings in its regulation.⁵

D. Requiring direct, individualized notice would be unreasonable and lead to harsh and absurd results to covered businesses and consumers alike. As noted above, and as the legislature acknowledged in its enactment of AB 1202, businesses without direct consumer relationships cannot practicably provide the pre-collection notice required under section 1798.100(b) on a direct, individualized basis. As such, requiring these businesses to do so would be unreasonable and harsh on its face.

Even if the businesses could provide such notice, requiring them to do so would result in tens of millions of California residents receiving precisely the kind of unsolicited and unwanted email, text, telephone, or mail contacts that consumers find so annoying and intrusive and that various consumer protection laws (e.g., TCPA, CAN-SPAM) are meant to prevent.⁶ Indeed, it is hard to imagine that California residents, currently beset by an onslaught of robocalls, robotexts, and spam messaging, would be pleased with yet another form of unwelcome and unnecessary communications from businesses with whom they do not have accounts or relationships, particularly in light of the creation of the data broker registry.

E. Homepage notice is consistent with the newly proposed privacy initiative, The California Consumer Privacy Act of 2020. This newly filed initiative proposal, drafted by the same persons who were the driving force behind the CCPA and intended by these persons to strengthen the CCPA and consumer privacy rights (see Sec. 2, Findings and Declarations, at E), explicitly allows for homepage notice. Specifically, the initiative would move the pre-collection notice requirement into section 1798.100(a) and then amend section 1798.100(b) to read as follows:

“A business that, acting as a third party, collects personal information about a consumer may satisfy its obligation under subdivision (a) by providing the required information prominently and conspicuously on the homepage of its Internet website. In addition, if

⁵ While we have no objections to the Attorney General requiring such posting on the registry, it would appear that such a requirement would exceed the Attorney General’s authority. As such, we suggest recommending the posting.

⁶ These businesses collect new, different, and/or updated personal information about consumers on a regular basis. Even if the businesses could provide direct, individualized notice, consumers would be annoyed, if not outraged, to receive additional notifications from the same business each time the business collects a new piece of information about the consumer.

The California Department of Justice

September 30, 2019

Page 6

the business, acting as a third party, collects personal information or authorizes another person to collect person information, about a consumer while the consumer is proximate to a physical location at which the personal information is collected, then the business 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, and whether such personal information is sold, in a clear and conspicuous manner at such location."

The inclusion of homepage notice in this new initiative is yet further, and highly compelling, evidence of the reasonableness and appropriateness of the concept.

III. Conclusion. For all these reasons, we reiterate our earlier request that the CCPA regulations make clear that businesses without direct consumer relationships may provide pre-collection notice on their Internet homepages.

Sincerely,



Philip R. Recht