From: Daly, Barbara
To: Privacy Regulations
Subject: CCPA Regulations Comment Letter
Date: Tuesday, February 25, 2020 9:23:19 PM
Attachments: CCPA Regulations Comment Letter 2-25-20.pdf

Attached please find comments regarding the California Consumer Privacy Act Regulations.

Sincerely,

Barbara Daly
Director, Government & Legislative Affairs
Transportation Corridor Agencies
125 Pacifica, Suite 100
Irvine, CA 92618
[redacted]
www.thetollroads.com

San Joaquin Hills
Transportation
Corridor Agency

Chair:
Patricia Kelley
Mission Viejo

Transportation Corridor Agencies™

Foothill/Eastern
Transportation
Corridor Agency

Chair:
Christina Shea
Irvine

February 25, 2020

Ms. Lisa Kim
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Sprint Street, First Floor
Los Angeles, CA 90013

RE: California Consumer Privacy Act Regulations

Dear Ms. Kim:

The Transportation Corridor Agencies (TCA) are two joint powers authorities formed by the California legislature to plan, finance, construct, and operate Orange County's toll roads. TCA has implemented an electronic toll connection system and uses FasTrak® along with other California toll operators to enable road users to be charged for and pay tolls for their toll road usage. While TCA is not a business subject to the California Consumer Privacy Act (CCPA), it is writing to request clarification that where it may be considered a third party governmental entity it would not be subject to section 1798.115(d) of the CCPA if it shares personal information that is used to enable toll road interoperability. W210-1

Federal law requires that "all toll facilities on the Federal-aid highways shall implement technologies or business practices that provide for the interoperability of electronic toll collection programs." See Moving Ahead for Progress in the 21st Century Act (PL 112-141), Section 1512(b) Electronic Toll Collection Interoperability Requirements. Section 1798.115 (d) of the CCPA states that "(d) A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120." Section 999.301 of the regulations define the term category of third parties to include a government entity.

We request that the Attorney General clarify that to the extent a governmental entity would be deemed a third party under the CCPA, such government entity acting as an operator of a toll road is not subject to Section 1798.115(d) if it shares personal information used to enable toll road interoperability and support the collection and enforcement of tolls.

We appreciate your consideration.

Sincerely,

Samuel Johnson

Samuel Johnson
Chief Operations Officer

125 Pacifica, Suite 100, Irvine, CA 92618-3304 • (949) 754-3400 Fax (949) 754-3467
thetollroads.com

From: Eric Rosenkoetter
To: Privacy Regulations
Subject: RMAI Comments to Modified CCPA Proposed Regulations 02-25-2020
Date: Tuesday, February 25, 2020 7:08:12 PM
Attachments: image001.png
RMAI Comments to Modified CCPA Proposed Regulations 02-25-2020 MW.pdf

---

Dear Ms. Kim,

Attached please find comments to the Modified Proposed Regulations filed on behalf of the Receivables Management Association International.

Thank you for your hard work on the proposed regulations and consideration of these comments.

Sincerely,

Eric P. Rosenkoetter
Maurice Wutscher LLP
13785 Research Blvd., Suite 125
Austin, Texas 78750
Direct: [redacted]
Mobile: [redacted]
Email: [redacted]

Admitted to practice in Texas and Missouri

MauriceWutscher

ALABAMA | CALIFORNIA | FLORIDA | GEORGIA | ILLINOIS | INDIANA | MARYLAND | MASSACHUSETTS | NEW JERSEY | NEW YORK | OHIO | PENNSYLVANIA | TEXAS | WASHINGTON, D. C.

www.MauriceWutscher.com

MauriceWutscher

Eric Rosenkoetter

Maur ce Wutscher LLP
13785 Research B vd.
Su te 125
Aust n, TX 78750

[redacted] D rect
(866) 581-9302 Fax
[redacted]
Adm tted on y n TX and MO

ANAHEIM
ATLANTA
AUSTIN
BIRMINGHAM
BOSTON
CHICAGO
CINCINNATI
CLEVELAND
DALLAS
FLEMINGTON
FORT LAUDERDALE
NEW YORK
PHILADELPHIA
WASHINGTON, DC

maur cewutscher.com

February 25, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 S. Spring Street, First Floor
Los Angeles, CA 90013

Sent via email: PrivacyRegulations@doj.ca.gov

Re: RMAI Comments on the Modified Proposed Regulations relating to the California Consumer Privacy Act of 2018

Dear Ms. Kim:

The Receivables Management Association International ("RMAI") appreciates this opportunity to submit the following comments regarding the Modified Proposed Regulations relating to the California Consumer Privacy Act of 2018 ("CCPA").

Because the "Updated Notice of Modifications to Text of Proposed Regulations" requests that comments be limited to the changes to the proposed regulations, RMAI incorporates by reference its previous comments submitted December 6, 2019.

I. BACKGROUND

RMAI is the nonprofit trade association that represents more than 550 companies that purchase or support the purchase of performing and non-performing receivables on the secondary market. The existence of the secondary market is critical to the functioning of the primary market in which credit originators extend credit to consumers. An efficient secondary market lowers the cost of credit extended to consumers and increases the availability and diversity of such credit.[1]

[1] See generally, U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities, Nonbank Financials, Fintech, and Innovation* (July 2018), at 130 (publicly available at https://tinyurl.com/y795fwey) last accessed Feb. 18, 2020 ("[D]ebt buyers are important market participants for the continued functioning of the consumer credit markets and other industries that rely on the recoveries from debt collection or the sale of delinquent debt to minimize losses."); David E. Reid, *The Value of Resale on The Receivables Secondary Market*, RMAI White Paper (April 2016) (publicly available at https://rmaintl.org/wp-content/uploads/2019/01/RMAI-Secondary-Market-White-Paper-2016-FINAL.pdf, last accessed Feb. 22, 2020);

RMAI is an international leader in promoting strong and ethical business practices within the receivables management industry. RMAI requires all its member companies who are purchasing receivables on the secondary market to become certified through RMAI's Receivables Management Certification Program ("RMCP")[2] as a requisite for membership. The RMCP is a comprehensive and uniform source of industry standards that has been recognized by the collection industry's federal regulator, the Consumer Financial Protection Bureau, as "best practices."[3]

In addition to requiring that certified companies comply with local, state, and federal laws and regulations concerning collection activity,[4] the RMCP goes above and beyond the requirements of local, state, and federal laws and regulations by requiring its member companies to comply with additional requirements not addressed by existing laws and regulations.[5] The debt buying companies certified by the RMCP hold approximately 80 percent of all purchased receivables in the country, by RMAI's estimates.

RMCP certified companies are subject to vigorous and recurring independent third-party audits to demonstrate to RMAI their compliance with the RMAI Certification Program. This audit includes an onsite inspection of the certified companies to validate full integration of RMCP standards into the company's operations. Following a company's initial certification, review audits continue to be conducted every two to three years.

RMAI's Certification Program was recognized by a resolution of the Michigan State Senate as "exceed[ing] state and federal laws and regulations through a series of stringent requirements that stress responsible consumer protection through increased transparency and operational controls…"[6]

At the state level, since 2013, RMAI has worked with legislators and regulators in California, Connecticut, Colorado, Maine, Maryland, Minnesota, New York, Oregon, Washington, and West

---

[2] RMAI, *RMAI Receivables Management Certification Program*, https://rmassociation.org/certification (last accessed Feb. 22, 2020).

[3] Consumer Financial Protection Bureau, *Small Business Review Panel for Debt Collector and Debt Buyer Rulemaking, Outline of Proposals Under Consideration*, July 28, 2016, p. 38, http://files.consumerfinance.gov/f/documents/20160727_cfpb_Outline_of_proposals.pdf (last accessed Feb. 22, 2020).

[4] The federal laws to which member companies are subject include but are not limited to the Fair Debt Collection Practices Act, Fair Credit Reporting Act, Gramm-Leach-Bliley Act, Electronic Funds Transfer Act, Telephone Consumer Protection Act, and the Health Insurance Portability and Accountability Act.

[5] See, e.g., Consumer Financial Protection Bureau, Proposed Rule (Regulation F), 84 FR 23274, 23331, n. 402 (May 21, 2019) (Observing that the RMCP includes policies concerning the sale and transfer of debt that exceed existing law).

[6] Michigan Senate Resolution 33, adopted March 26, 2015. https://www.legislature mi.gov/(S(c0l55hrzl15jmpuaxb4uv0gf))/mileg.aspx?page=getobject&objectname=2015-SR-0033&query=on (last accessed Feb. 22, 2020).

Virginia toward the enactment of enhanced laws and regulations regarding the collection of purchased consumer debts.

II. COMMENTS

A. ***The clarity previously contained in § 999.305(d) regarding a business that is not a data broker and does not collect information directly from consumers should be restored.***

Previously, § 999.305(d) simply provided: "A business that does not collect information directly from consumers does not need to provide a notice at collection."

The Modified Proposed Regulations understandably amend this provision to address the issue of data brokers, as follows:

> If a business that does not collect information directly from consumers is registered with the Attorney General as a data broker pursuant to Civil Code section 1798.99.80, *et seq.* it does not need to provide a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out.

W211-1

Unfortunately, in addressing the issue of data brokers, the modification completely, and presumably inadvertently, omits guidance for businesses that are not data brokers and do not collect information directly from consumers. The proposed regulation would arguably capture a significant number of entities that are neither data brokers nor collect information directly from consumers and require these entities send a notice at collection, a result that was avoided by the originally proposed § 999.305(d) .

Accordingly, RMAI respectfully suggests the following language for § 999.305(d) to address data brokers and non-data brokers that do not collect information directly from consumers:

> A business that does not collect information directly from consumers and is not a data broker as defined in Civil Code section 1798.99.80, subsection (d), does not need to provide a notice at collection. If a business that does not collect information directly from consumers is registered with the Attorney General as a data broker pursuant to Civil Code section 1798.99.80, *et seq.* it does not need to provide a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out.

B. ***A business that does not sell consumers' personal information should not be required to confuse consumers by informing them of an inapplicable right to opt-out.***

RMAI appreciates the additional clarity provided in the Modified Proposed Regulations that businesses that do not sell consumers' personal information need not provide the notice of right to opt-out if certain conditions are met. RMAI also applauds the removal of the requirement in § 999.306(d)(1) that businesses state they "will not" sell personal information.

However, there remains a disconnect between § 999.306(d) and § 999.308(c) that has the potential to confuse consumers. While the former subsection states that a business does not need to provide a notice of opt-out if certain conditions are met, §999.308(c) still requires the same business to inform consumers of a right to opt-out that is made inapplicable by § 999.306(d)in that situation.

W211-2

To resolve this potentially confusing conflict, RMAI suggests the following language for § 999.308(c)(3):

> Right to Opt-Out of the Sale of Personal Information
>
> a. Unless a business does not need to provide a notice of right to opt-out pursuant to section 999.306, subsection (d), ~~E~~explain that the consumer has a right to opt-out of the sale of their personal information by a business.
> b. State whether or not the business sells personal information. If the business sells personal information, include either the contents of the notice of right to opt-out or a link to it in accordance with section 999.306.

C. *Businesses should have the ability to better safeguard consumers' specific pieces of information.*

The need for a "higher bar for verification" of consumers' requests for specific pieces of information is rightfully recognized in § 999.325(c). RMAI appreciates that the Modified Proposed Regulations provide additional safeguards in § 999.326 with respect to the use of authorized agents. However, the "bar" for verification remains no higher than if the information were being requested directly by the consumer.

W211-3

RMAI respectfully suggests that the bar should be even higher when the specific pieces of information are being requested by a third party and that a business should, therefore, have the option of requiring that the consumer's signature be acknowledged before a notary public.

RMAI understands the value to consumers to have the ability to utilize an authorized agent. However, it also believes that with respect to requests for specific pieces of information by a third party, there is greater risk to consumers and greater potential liability to businesses. To be sure, we believe that with respect to non-exempt information concerning financial products and services, medical products and services and utilities, the risk of consumer harm and business

liability can be significant. Therefore, RMAI suggests the following modification to § 999.326(a):

> When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require that the consumer do the following:
>
> (1) Provide the authorized agent written and signed permission to do so, or notarized permission to do so if the request is for specific pieces of information.
>
> (2) Verify their own identity directly with the business.
>
> (3) Directly confirm with the business that they provided the authorized agent permission to submit the request.

W211-3 (cont.)

To accommodate this change, RMAI also recommends the following modification to §999.323(d):

> A business shall not require the consumer to pay a fee for the verification of their request to know or request to delete. For example, a business may not require a consumer to provide a notarized affidavit to verify their identity unless the business compensates the consumer for the cost of notarization. This subdivision shall not apply to a consumer's permission to an authorized agent pursuant to section 999.326, subdivision (a)(1), or a power of attorney provided pursuant to section 999.326, subsection (b).

W211-4

III. CONCLUSION

RMAI thanks the California Office of the Attorney General for its many thoughtful modifications to the proposed rules and for its consideration of these comments.

Please let us know if you have questions or if we can be of any assistance.

Sincerely,

Receivables Management Association International
By: Maurice Wutscher LLP, General Counsel

Eric Rosenkoetter

From: James Harrison
To: Privacy Regulations
Subject: RE: Californians for Consumer Privacy Comments Re Revised Proposed Regulations
Date: Tuesday, February 25, 2020 5:15:00 PM
Attachments: image002.png
image003.png
CCP Comments re Proposed CCPA Regs (00403675xAEB03).pdf

Attached is a pdf version of the same letter. Thank you.

James C. Harrison
Olson | Remcho
1901 Harrison Street, Suite 1550, Oakland, CA 94612
[redacted] | [redacted]
olsonremcho.com

From: James Harrison
Sent: Tuesday, February 25, 2020 4:57 PM
To: PrivacyRegulations@doj.ca.gov
Subject: Californians for Consumer Privacy Comments Re Revised Proposed Regulations

Please find attached comments from Californians for Consumer Privacy.

James C. Harrison
Olson | Remcho
1901 Harrison Street, Suite 1550, Oakland, CA 94612
[redacted] | [redacted]
olsonremcho.com

CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication

CALIFORNIANS FOR CONSUMER PRIVACY

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

To Whom It May Concern:

Thank you for the opportunity to offer comments regarding the Attorney General's revised proposed regulations (modified on February 10, 2020) to implement the California Consumer Privacy Act ("CCPA"). We are grateful to the Attorney General's Office for the thoroughness and thoughtfulness of the proposed regulations.

Please find below our comments on and suggestions for improvements to the regulations:

'Authorized Agent' Definition (999.301(c))

We think the clarifying edit to "Authorized Agent" is excellent, as it ensures the correct level of registration of an entity without forcing them to jump through any extraneous hoops. Registration with the Secretary of State is enough and more should not be required. W212-1

'Notice at Collection' Definition (999.301(l))

We applaud the edits to the definition of 'Notice at Collection,' as we think it vital to ensure that all businesses collecting information, **must** make collection activity clear to all consumers **at or before** the point of collection. This is a very elegant and simple fix. W212-2

'Signed' Definition (999.301(u))

We think the addition of electronic signatures is appropriate; however, we would strongly recommend the Regulations ***require*** businesses to provide for electronic signature (per the Uniform Electronic Transactions Act), as we have already seen some businesses making it difficult for consumers to exercise their rights, or for authorized agents to prove they have a consumer's authorization. If businesses can make it difficult for consumers—and their agents—to exercise their rights, then businesses will 'win' and consumers will lose. W212-3

Guidance Regarding the Interpretation of CCPA Definitions (999.302)

We applaud new Section 999.302 as we think this greatly clarifies the intention of Civil Code sections 1798.100(e) and 1798.110(d)(1) and (2) with respect to what should and should not be personal information. W212-4

However, we are concerned that the current phrasing opens a major loophole in the case of a business that collects personal information but does not 'reasonably link the information to a particular

consumer or household,' and then transfers it to a third party which does so. One can imagine a business that collects personal information but is not a large data aggregator, transferring the information to one of the internet giants, which might then easily link it to a particular consumer. If the following language were added, it would ensure that to qualify for the 999.302 safe harbor, the first party could not transfer the personal information to any entity that would then use it as PI.

W212-4 (cont.)

Proposed amendment: "For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, **and does not transfer that IP address to any other person who could reasonably link the IP address with a particular consumer or household,** then the IP address would not be "personal information.""

Notice at collection: placement (999.305(a)(3))

We are strong supporters of the amended Section 999.305(a)(3)(a), which clarifies that the notice at collection should be posted on all webpages where personal information is collected, and implements the intent of Civil Code Section 1798.100(b).

We have two suggestions to improve the Notice at Collection.

The first is to name the notice, or any link thereto, something universal, such as "Your California Privacy Rights." The easier it is for consumers to find and recognize how to exercise their rights, the more effective the law will be.

W212-5

Second, we suggest amending Section 999.305(a)(3)(b) to read "When a business collects personal information through a mobile application, it may provide a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu, **provided that the link is easily available to the average consumer, and does not require the consumer to click through multiple layers or screens to find it.**"

W212-6

We have already seen businesses going to great lengths to hide any mention of CCPA, and we are concerned that if the link is only available on the download page and the settings menu of mobile apps, businesses will set up their architecture such that most consumers will never see the link in the first place. Also, the proposed wording would allow the link to be accessed five layers deep in the settings menu, which is not helpful to consumers. For example, in order to limit ad tracking, IOS currently requires a consumer to click "Settings"→"Privacy"→"Advertising"→"Limit Ad Tracking," in order to limit ad tracking, and IOS is perhaps the most privacy-friendly platform out there! Much as you did in Section 999.305(a)(4) (see comments below), we think you should tie this section to the reasonable expectations and abilities of the average consumer.

Note: there is a typo on Section 999.305(a)(3)(c) "to ~~the~~ where…"

W212-7

Consumers' reasonable expectations of collection (999.305(a)(4))

We wholeheartedly applaud Section 999.305(a)(4) as being *truly* in the best interests of consumers. Consumer legislation should protect consumers from deceptive business practices, which is what this clause does. Bravo! The only possible improvement we might suggest is to add "why" the business thinks the activity might be unexpected, or perhaps to headline this particular notice with a label

W212-8

"Information we collect that might surprise you." In this day of incessant notices, having to highlight a deceptive business practice, as opposed to burying it in a privacy notice, may shame businesses into refraining from collecting such information.

W212-8 (cont.)

Notice at Collection: Online (999.305(c))

Given the extreme steps some businesses have taken in the last 6 weeks to hide any mention of CCPA, and to make it very difficult for consumers to find where and how to exercise their rights, we have major concerns regarding the interactions between Sections 999.305(b) and (c), and think they may unintentionally countermand the requirements of Civil Code Section 1798.135(a)(1). Please see below for our thinking (emphasis to Code sections added).

- Civil Code section 1798.135(a)(1) requires "***a clear and conspicuous link*** on the business' Internet homepage, ***titled*** "Do Not Sell My Personal Information,"" for any business that sells personal information.
- Homepage is defined in Civil Code section 1798.140(l) to include "***any*** Internet Web Page where personal information is collected."
- Section 1798.185 does not specifically authorize the Attorney General to revisit this architecture. The AG's office is tasked with developing an opt-out logo or button (and so, for example, the ability to alter the wording of the notice to "Do Not Sell My Info" is clearly granted to the Attorney General), and with adopting regulations to further the purpose of the title. However, the Attorney General does not have the authority to allow a business to remove the "Do Not Sell My Information" button from any page where personal information is collected, ***if*** a business is selling information.
- Section 999.305(b)(3) allows the link titled "Do Not Sell My Personal Information" to be included in the Notice at Collection.
- Section 999.305(c) allows the Notice at Collection to be placed inside a business' privacy policy.
- We think the unintentional logical conclusion of 999.305(b) and (c), as written, is that a business that sells personal information could bury the "Do Not Sell My Information/Info" button in the privacy policy and omit it from the first page a consumer sees.
- From the very outset of our journey, we intended that the "Do Not Sell My Information" button would be omnipresent and hard not to see, for any business that sells personal information.
- If, now, a business can essentially hide this consumer call to action, in a privacy policy, then a major part of the law will be null and void, and one of the threshold achievements of CCPA will be extraordinarily weakened.
- We recognize that businesses will object to having to display this button so prominently—especially given that consumers will be much more likely to use it if they can see it—but that was *always* our intention. There should be a cost to businesses that sell consumer information, and that cost is transparency. If consumers choose to act on this knowledge, that is the cost to the businesses of collecting and monetizing consumer personal information.
- We think this is unintentional and can be easily fixed by deleting Section 999.305(b)(3), since the notice at collection applies to all businesses, whereas the Right to Opt-Out only applies

W212-9

to businesses that sell personal information. This fix would be consistent with the clear statutory language, which spells out the placement of the notice of sale in great clarity and which makes clear that it cannot be buried in a privacy policy. See also our comments regarding section 999.315.

W212-9 (cont.)

Section 999.305(d): This comment is similar to the one above, and we suggest clarifying that, in addition to including a link "…in its registration submission…", the business's home page (or any webpage which it maintains with which it conducts business in California) should include the Do Not Sell My Information button. We see this as important since we believe consumers will neither have the time nor desire to track down the myriad data brokers that have collected their information, and therefore will rely on third party privacy businesses to do it for them. Consumers and their representatives should have an easy, standard way to access the "Do Not Sell My Info" rights of CCPA.

W212-10

Our suggested amendment to section 999.305(d): "If a business that does not collect information directly from consumers is registered with the Attorney General as a data broker pursuant to Civil Code section 1798.99.80, et seq. it does not need to provide a notice at collection to the consumer if it has included in its registration submission, **its internet homepage, or any web page it maintains to conduct business in California, the** link **titled "Do Not Sell My Personal Information" in accordance with Civil Code section 1798.135(a)(1) and regulation 999.315(a),** which links to instructions on how a consumer can submit a request to opt-out."

Notice of Right to Opt-Out of Sale of Personal Information (999.306)

Section 999.306(a)(2): We are confused by this section, as we think the Notice of Right to Opt-Out ***is*** the phrase "Do Not Sell My Information," or "Do Not Sell My Info." See below:

- *1798.120 (a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out.*
  - *(b) A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information.*
- *1798.135. (a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:*
  - *(1) Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information.*
- *1798.185. (a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:…(4) Establishing rules and procedures for the following:*
  - *(A) To facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information pursuant to Section 1798.120.*
  - *(B) To govern business compliance with a consumer's opt-out request.*

W212-11

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

The above excerpts make it clear that the opt-out right ***must*** be titled "Do Not Sell My Personal Information."

Therefore we suggest the following modification:

"999.306(a)(2)(a) **Be titled "Do Not Sell My Personal Information" or "Do Not Sell My Information"** "~~Use plain, straightforward language and avoid technical or legal jargon~~.

W212-11 (cont.)

Section 999.306(b)(1): In the same vein, since the notice of right to opt-out **is** the phrase "Do Not Sell My Information/Info," we suggest this section be amended as follows:

"A business shall post the notice of right to opt-out on the **business's** Internet **homepage** ~~webpage to which the consumer is directed after clicking on the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link on the website homepage~~ or the download or landing page of a mobile application **or online service**. In addition, a business that collects personal information through a mobile application may provide ~~a link to~~ the notice within the application, such as through the application's settings menu, **provided the notice shall be easily available to the average consumer, and does not require the consumer to click through multiple layers or screens to find it**. The notice shall include the information specified in subsection (c) or link to the section of the business's privacy policy that contains the same information."

999.306(c): We are concerned that reference to "Authorized Agent" has been dropped here. In the interest of clarity, we suggest including "or their Authorized Agent" after "consumer/consumer's," in each of 999.306(c)(1), (2) and (3).

W212-12

999.306(e): We think this is a welcome addition.

W212-13

999.306(f): Given the public reaction to this button, we think it is worth reconsidering the construct, so that it is crystal clear to a consumer what the result of their action has been. We have noticed some businesses developing an architecture around the Do Not Sell My Information link which seems intentionally confusing and deliberately misleading.

We are not wedded to any one outcome here. One suggestion would be that the initial "Do Not Sell My Info" would change to "Your Info will not be sold."

W212-14

Another could be that the "Do Not Sell My Info" logo you have specified goes from the red X to a green checkmark once checked.

We think an important consideration is that If the consumer clears their cookies and the business can no longer recognize them, or the consumer logs on from a different device they have not previously opted-out from, the link should indicate their status at a glance, to remind them when the business is and is not selling their information.

<u>Notice of Financial Incentive (999.307)</u>

W212-15

Section 999.307: Given the activities of some actors online in the weeks since CCPA has gone into effect, we strongly urge you to include a definitive statement that opting-in to a financial incentive program must be a standalone action, and cannot be bundled within a Terms & Conditions or buried in some other general notice to which the consumer clicks "I agree."

For example, **999.307(a)(2)(e)** could be construed to read "If we [the business] include the notice in paragraph 129 of the privacy policy, which the consumer clicks 'I agree' to, we have fulfilled our obligation to notify the consumer. It was 'readily available;' it's their problem if they didn't read the entire privacy policy."

We suggest amending **999.307(a)(2)(e)** as follows "Be readily available where consumers will encounter it before opting into the financial incentive or price or service difference, **and is a separate and standalone notice, not bundled or combined with, or placed within, any other notice."**

We think there should be no possibility of a consumer being entered into an incentive by default, or without the overt chance to read and consider the details of the notice.

W212-15 (cont.)

Additionally, we feel that **999.307(a)(3)** is an invitation to businesses to bury the financial notice in a lengthy privacy policy which no one has the time to read. Also, we think 'immediate' timing is important, i.e. the consumer should get the notice directly upon opting-out (if the business chooses to have a financial incentive). [Note that we are fine if the notice is simply a section of a privacy policy containing the required information—this is not our point. We are not concerned with 'where the notice lives,' but we are concerned with 'how and where the consumer encounters it.']

Therefore we suggest the following revised 999.307(a)(3): "If the business offers ~~the~~ **a** financial incentive or price or service difference ~~online~~ **related to the collection, deletion, or sale of personal information,** the notice ~~may~~ **must** be given **reasonably immediately in response to a consumer's exercise of rights relating to the collection, deletion, or sale of the consumer's personal information, in the same general format as other notices, and must contain the information required in subsection (b). For example, if the consumer elects to opt-out online, then the business must provide the notice online in response to the opt-out; if the consumer opts-out in person at a business's premises, or on the telephone, then the notice must be given in person or on the telephone when the consumer opts-out." [Note this is conceptually similar to your logic in Section 999.312(c)].**

W212-16

Please note that we replaced "disclosure" with "collection" because this is the term used in Civil Code section 1798.125(b)(1).

W212-17

Privacy Policy (999.308)

Section 999.308: While the statute is not dispositive in this regard, it was written envisaging that California-specific privacy rights would be assembled in one section of any privacy policy, as evidenced by Civil Code section 1798.130(a)(5) ("Disclose [A description of a consumer's rights pursuant to Sections 1798.110, 1798.115, and 1798.125] in its online privacy policy or policies if the business has an online privacy policy or policies **and in any California-specific description of consumers' privacy rights**." Also Section 1798.135(a)(2)(B) refers to "Any California-specific description of consumers' privacy rights."

We urge you to require that the information required to be posted in 999.308 be segmented and separated from the rest of a business' privacy policy (i.e.: "Your California Privacy Rights").

W212-18

We think this is good public policy, and our fear is that as we have seen in the months since CCPA went into effect, businesses will bury different parts of important privacy information in hard-to-find areas. The impact to a California consumer of seeing all their rights enumerated in one easy-to-find section of a privacy policy is hard to overstate.

W212-18 (cont.)

Also, please note that with respect to proposed Section 999.308(c)(3)(b), we think that Civil Code section 1798.130(a)(2) requires the link to the notice of opt out, so we are concerned that the wording "contents of the notice of right to opt-out" might allow businesses to come up with misleading ways to mislabel this important right. We urge that the requirement in 999.308(c)(3)(b) be simply to have the link and label it in accordance with Civil Code section 1798.135(a)(1) and section 999.315(a): either "Do Not Sell My Info" or "Do Not Sell My Personal Information." Accordingly, our revised section would read:

W212-19

"State whether or not the business sells personal information. If the business sells personal information, include **the 'Do Not Sell My Personal Information' notice** ~~either the contents of the notice of right to opt-out or a link to it~~ in accordance with section 999.306."

As we have seen in the past few months, many businesses will use every inch of leeway to make consumers less likely to exercise their rights, and so this important right should be labeled as clearly as possible.

Responding to Requests to Know and Requests to Delete (999.313)

Section 999.313(b): With the addition of the proposed new language, this would give businesses a blanket 'out' if a business cannot verify a consumer request. To that end, we urge that the additional wording around the business' ability to deny a request to know or delete be amended as follows: "If the business, **acting reasonably and using a similar level of diligence and technology it uses to collect consumer information**, cannot verify the consumer within the 45-day time period, the business may deny the request."

W212-20

Section 999.313(c)(3)(c): We applaud the clarity around this entire section. However, we have one question: A business is not required to search for personal information if it does not sell it or use it for a commercial purpose, but presumably a business would not collect the information in the first place it if it did not have a commercial purpose – how would this paragraph apply under these circumstances? Also, even if it is retaining the information for a legal or compliance purpose in 999.313(c)(3)(b), that also is presumably a commercial purpose in that it "advances [the business's] commercial or economic interests," by keeping the business a going concern.

W212-21

We suggest a very minor amendment to say "…and does not use it for any **further** commercial purpose **after initial collection...**"

We do not feel strongly about this modification but think it would serve the purpose of clarity.

Responding to Requests to Know (999.313)

Section 999.313(c)(4): As with our submission in December, we beseech you to consider that this regulation could be a huge step backwards for privacy. Currently, it is ***not*** a settled matter in law as to whether a California consumer could go to many businesses and demand to see all the information

W212-22

those businesses had collected about the consumer. Certainly there is nothing in law saying the business would NOT have to turn over that information to a consumer.

This regulation would suddenly remove a vast category of information from any consumer's reach—**and with the addition now of biometric data**, this regulation would vastly increase the scope of this exception. The pregnancy app collecting someone's menstrual cycles? A woman wouldn't have access to that data, nor to any inferences the app had made about her. Your wearable device? All that information would suddenly be off-limits to a consumer.

We objected to this regulation in December, on the grounds that it might be important for a consumer to be able to know whether a business was a vector for selling her social security number (if a business doesn't have to disclose that information, how do you track its flow from business to business?); or for example to assist consumers dealing with identity theft (does a business have the right account number for them?).

To now exempt **all biometric data** from the Right to Know—whether a company is tracking me because of my gait or how I open the door; because it recognizes my face (or thinks it does); my voice patterns—would be simply a staggering give to industry. We urge that at the very minimum, this new addition with respect to biometric data be struck. It would be a massive hole in the heart of CCPA.

W212-22 (cont.)

Section 999.313(c)(5): typo in 'doing,' currently reads 'doings.'

W212-23

Right to Delete (999.313)

Section 999.313(d)(1): We applaud the new language, but we suggest clarifying when it is must be followed. Is the intention that *only* consumers whose request to delete information has been denied by the business because of the business' inability to verify the consumer's identity, be asked whether they would like to opt out?

We suggest that this insert be a standalone new subparagraph under **999.313(d)(1)**, and be a required response to ***any*** deletion request, whether honored or not.

The reason for this is simple: if a consumer goes to Personal.Info.Co and says "delete my information," and Personal.Info.Co complies—that still doesn't prevent Personal.Info.Co from collecting information about that consumer in the next minute, from the next site the consumer visits after deleting their information. In this instance we think Personal.Info.Co should be required to offer the opt-out (and we think this is your intention, though the wording allows for some ambiguity).

W212-24

Section 999.313(d)(2)(b): We again oppose simply deidentifying information versus deleting it, as we think consumers will want to ensure that the data can never be reused (and if a business can deidentify a consumer's information, why can't they delete it?).

Section 999.313(d)(2)(c): Equally, we oppose 'aggregating' the information as we think this too, like the point above, would not satisfy consumers' expectations regarding their request. Additionally, we think there is a grammatical mistake in this clause, since Civil Code section 1798.140(a) defines "Aggregate consumer information," and this clause refers to "Aggregating ***the*** consumer information."

W212-25

"Consumer information" is not a defined term under CCPA or the proposed Regulations, and we think (if you decide to keep the 'aggregate' concept) the phrase should read something like "Transforming the personal information into aggregate consumer information."

To conclude this part, however, we think the deletion requirement set forth in 999.313(d)(2)(a) is concise and clear and urge you to keep that and that alone as the standard for businesses to meet for deletion.

W212-25 (cont.)

We think the clarification in section 999.313(d)(3) is well-worded. This eliminates non-deletion of a consumer's information if the archive system is used for *other* consumers' information, so helps to minimize the ability of businesses to game the system.

W212-26

Section 999.313(d)(7): We propose the following amendment to this section to alleviate concerns that businesses will try to game deletion requests to make it difficult for consumers to exercise their rights:

"In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information only if a global option to delete all personal information is also offered, and more prominently presented than the other choices, **and the choice is not designed to coerce consumers into deleting only a portion of their information.**"

W212-27

Service Providers (999.314)

Section 999.314(a): This regulation is one that has improved in some respects from the initial draft, but is also still fundamentally highly problematic, and in our opinion would represent a *massive* weakening of CCPA's reach.

It is improved in its use of 'business' vs. 'person,' which was previously confusing.

W212-28

While CCPA was never intended to regulate government entities themselves, it was ***always*** intended to cover businesses that ***processed*** government data—as that presented the only way to get a glimpse into what governments are doing in so many of these areas, FOIA notwithstanding. Hard to make a FOIA request to Palantir

Just look at headlines from recent weeks, showing our own government buying surveillance data from commercial providers—no warrant required.

In combination with Section 999.314(e), 999.314(a) would with one stroke remove all data processed by businesses on behalf of governments and government agencies from being accessible to consumers, and would eliminate consumers' ability to delete it.

W212-29

So much for figuring out if the local police department is using a surveillance company to monitor me, or whether ICE has been surveilling my phone and my location to see if I'm spending time with suspected undocumented immigrants.

To the extent that the Attorney General is concerned about national security and law enforcement, then clearly any surveillance conducted pursuant to a warrant, court order, or a law enforcement agency-approved investigation with an active case number, could be exempted from the requirement that Service Providers to persons or organizations that are not businesses respond to access and deletion requests.

With all due respect, this proposed regulation would have virtually the same effect as AB 1416, a bill introduced in the 2019 Legislative Session, which was the subject of a huge outcry, and did not pass the Legislature in 2019.

AB 1416 would have exempted businesses that provided services to governments and government agencies, from complying with CCPA—so a consumer would not have been able to access or delete their information from such a business.

This proposed regulation would do almost exactly the same thing—consumers would no longer be able to access or delete personal information processed by service providers on behalf of governments or government agencies, and because consumers do not have the right under CCPA to make access and deletion requests ***to*** governments or government agencies, an entire sector of the personal information realm currently covered by CCPA would be erased from CCPA's purview in one stroke.

We think the Attorney General would be well-advised to review AB 1416's legislative history and the debate around that proposal, as this regulation would push it right back into the center of that debate.

It is worth quoting from the AB 1416 Senate Judiciary Committee Legislative Analysis, as a reminder of just how devastating new exemptions to CCPA in the vein of this proposed regulation were considered only seven months ago in the Legislature.

W212-29 (cont.)

"[AB 1416] creates several new, broad exemptions to the CCPA that would dramatically erode the rights of consumers pursuant to the nascent law and allow businesses to disregard consumers' choices to restrict the sale of their personal information or to delete it…

"So long as the business is providing data to some government entity or providing some service to some government entity, the business can effectively ignore the obligations of the CCPA. The language provides that a business is not required to delete a consumer's personal information despite a legitimate request to delete from a consumer…These loopholes fundamentally undermine the control over personal information that the CCPA currently provides consumers. Consumers that would have every right to assume their data has either been deleted or that its sale was prohibited, could have their personal information being retained…by these businesses without their knowledge…

"…Californians have a fundamental right to privacy and the CCPA provides a set of tools to effectuate that right…However, what the CCPA provides, and this bill takes away, is a person's choice. In passing the CCPA, the Legislature made a determination that Californians should be able to have more control over where their information goes and who can have access to it."

Civil Code section 1798.140(v) *clearly* defines Service Provider as entities that provide services to "**businesses**." In our negotiations prior to the passage of CCPA, we specifically and intentionally limited the definition in this fashion, precisely to avoid the outcome that the Attorney General is now proposing to effect by regulation. An organization that qualifies as a "business" under the CCPA should ***not*** escape the reach of the CCPA when it processes information on behalf of persons or organizations that are not businesses, and should be required to comply with consumer requests under the CCPA.

Section 999.314(e) is entirely appropriate in the context of service providers to *businesses,* because the consumer has a way to access and delete their information via CCPA. In the context of service providers to persons or organization that are not businesses, however, Section 999.314(a) would create an

egregiously large, anti-privacy hole right in the heart of CCPA because consumers do not have the right to make an access or deletion request to persons or organizations that are not businesses.

There is ***zero*** statutory basis for the wholesale exemption that this regulation would create, and it is inconsistent with the intent of the law, which is to enable consumers to learn what information businesses have collected about them, regardless of the source.

We understand, however, that there are substantial public policy questions that need to be resolved with respect to service providers to persons or organizations that are not businesses. A consumer should not be able to simply make non-specific requests to any large service provider (think AWS or Microsoft cloud storage services), with a query as to whether their information is processed by such a business, or to delete this information.

W212-29 (cont.)

Therefore we suggest amending Section **999.314(a)** as follows: "A business that provides services to a person or organization that is not a business (a "non-business"), and that would otherwise meet the requirements and obligations of a "service provider" under the CCPA and these regulations, shall: ~~be deemed a service provider for purposes of the CCPA and these regulations~~.

(1) Only be required to respond to access and deletion requests that identify a specific non-business on whose behalf the service provider has processed the consumer's personal information.
    a. If the non-business has agreed to be bound by the access and deletion provisions of the CCPA, then the service provider may satisfy its obligation by referring the consumer to the non-business for a response to the consumer's request.
    b. If the non-business has not agreed to be bound by the access and deletion provisions of the CCPA, then the service provider shall respond to the consumer's access or deletion request.
    c. The exceptions set forth in Civil Code sections 1798.105 and 1798.145 shall apply to this subdivision.

Section 999.314(c): This regulation is much improved, in our opinion, since the first version of the regulations. We recommend one further improvement to the phrase "A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except:"

Civil Code section 1798.140(t)(2)(C)(ii) has a different term which covers the same concept (i.e. how a service provider can use information and have it not be deemed a sale, and not be used in contravention of a consumer's expectations), except with much greater scope: "The service provider does not further **collect**, sell, or use the personal information of the consumer except as necessary to perform the business purpose."

W212-30

We suggest including the term 'collect,' so that Section 999.313(c) would read "A service provider shall not retain, **collect,** use, or disclose personal information obtained in the course of providing services except:" "Collect" has such an expansive definition that we think this change would ensure that the personal information would be useless to the Service Provider except as set forth in the rest of Section 999.313(c)(1) – (5).

Section 999.314(e): this regulation is much improved and clearer.

W212-31

<u>Requests to Opt-Out and Opt-In (999.315 & 999.316)</u>

Section 999.315(a): We suggest clarifying that this regulation *only* applies to businesses that sell personal information pursuant to Civil Code section 1798.120. Also, we think Civil Code section 1798.135(a)(1) ***requires*** the regulations to ***specify*** "internet homepage," not just a website. Given the definition of "homepage" in Civil Code section 1798.140(l), we think the statute does not permit any other language to be used in the regulations.

We suggest amending section 999.315(a) to read: "A business **that sells personal information** shall provide two or more designated methods for submitting requests to opt-out, including an interactive form 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~~ **internet homepage** or mobile application.

W212-32

Section 999.315(c): Bravo! Excellent regulation, and we think the wording is clear and unambiguous.

W212-33

Section 999.315(d): Again, bravo. The ability to set your phone to "Do Not Sell My Information" will be critical to allowing consumers to take advantage of their new rights. Section 999.315(d)(1) and (2) are also clear and thoughtful (note a typo in paragraph (1) "…that a consumer intends to ~~**the**~~ opt-out…"]

W212-34

Section 999.315(e): Given the eye-opening lengths to which some businesses have gone to make CCPA inoperative to their customers, we suggest clarifying that the choice to opt out for certain uses be contingent on a) the global opt-out **not only being** more prominent, **but *also* being displayed first**; and then b) include the concept from 999.315(c) above.

Thus, we propose an amendment to section 999.315(e): "In responding to a request to opt-out, a business may present the consumer with the choice to opt-out of sale for certain uses of personal information as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices, **and as long as the method to opt-out of sale for certain uses does not burden a consumer's ability to opt-out of the sale of all uses or any part of their personal information."**

W212-35

Section 999.315(f): This proposed regulation has gotten better in some respects, and worse in others.

It has gotten better in that the uncertainty around the 90-day threshold has been removed, which will put an end to those who suggested this meant that all CCPA covered was the last 90 days of a consumer's personal information.

However, it has also now extended the time to comply with an opt-out request from 15 calendar days to 15 *business* days, or two thirds of a month!

The intent of Civil Code Section 1798.135(a)(4) is clear: "For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer." The language does not say "wait three weeks and then refrain from selling the information." So now the regulations are using the fact that there is not a specified statutory period to complete the opt-out of sale to put a huge distance between a consumer's instruction, and that instruction taking effect. If you surveyed most consumers, and said a new California law would give them the right to opt-out of the sale of their personal information, do you think most consumers would expect it would take a business three weeks to stop doing that?

W212-36

With all due respect, this proposed regulation is a huge win for the ad-tech industry, since by far the largest value in tracking consumers and selling their movements, browsing history and search terms, is in doing so immediately.

This proposed regulation would gut a hugely important component of the law entirely. Your visits to a cancer center or dialysis clinic, abortion provider or car dealership; your searches for whether you or your niece suffer from depression; the fact that your phone is in proximity to a political activist, politician or police personnel: all of these would now be legally for sale to ad tech and thousands of other businesses of which consumers have never heard for **three weeks.** Three weeks?

Imagine, every time a consumer clears their cookies, and the business can't immediately re-identify them, they are a new consumer (essentially) to the business (though of course once the business figures out who they are, their information will continue to be added to the previously-assembled record)—and the clock will begin ticking again, with another 15 business days' worth of data for sale.

A consumer's decision to opt out should take effect immediately—if businesses can continue to sell the information, they can also *cease* selling it—all talk of how it's difficult for them to comply immediately, is revealed for the deception it is, because the businesses continue to *sell* the information. If a business is monetizing information and can bill for that monetization, they can cease monetizing it—would they give it away for free during this time period, with *nothing* received in return?

W212-36 (cont.)

We suggest amending Section **999.315(f)** to "A business shall comply with a request to opt-out as soon as feasibly possible, but no later than ~~15 business days~~ **or one business day** from the date the business receives the request."

Section 999.315(g): We think these clarifications are excellent.

W212-37

Section 999.315(h): We suggest that the consumer response should include the exact measures a consumer must take to convince the business that the request is not fraudulent, so our proposed amendment would read: "A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent, **together with steps the requestor can take to prove that the request is not fraudulent."**

W212-38

Section 999.316(b): Given the actions of some businesses since CCPA has gone into effect, we think it necessary to plan for businesses using any loophole to deny privacy rights to consumers. Therefore we recommend the following edit to this section: "If a consumer who has opted-out of the sale of their personal information initiates a transaction or attempts to use a product or service that requires the sale of their personal information, a business may inform the consumer that the transaction, product, or service requires the sale of their personal information**, together with a detailed explanation of how and why the transaction, product or service requires the sale of their personal information,** and provide instructions on how the consumer can opt in."

W212-39

Household Information (999.318)

Section 999.318(a): Typo in this paragraph, "…or a request to delete~~d~~ household personal information…"

W212-40

Verification (999.323)

Section 999.323(d): Hallelujah. And Amen. Our only suggestion is to remind industry that Authorized Agents are also able to submit requests, and should not be charged, either. Therefore, we suggest amending to "A business shall not require the consumer **or their Authorized Agents** to pay a fee…" W212-41

Verification for Non-Accountholders (999.325)

Section 999.325(e): We applaud the clarity in this section, especially in (e)(2). W212-42

Section 999.325(f): While we applaud and agree with what we believe to be the intent of this clause, we are concerned that its binary nature sends the wrong message, and provides a perverse incentive for businesses *not* to be able to verify, and therefore not have to respond to access or deletion requests.

We suggest amending as follows: "A business shall deny a request to know specific pieces of personal information if **having used commercially reasonable efforts to verify the consumer's identity,** it cannot verify the identity of the requestor pursuant to these regulations. W212-43

Authorized Agents (999.326)

Section 999.326(a)(1): Given that the regulations define "signed" as a "***written*** attestation, declaration or permission," we think this clause would read better as "written ~~and~~ **or** signed…," or simply "signed." The duplication seems unnecessary. W212-44

Section 999.326(a)(3): While we are as concerned as anyone that CCPA not become a vector to increase deceptive activities by facilitating fraudulent requests, we are also concerned that this section will allow businesses to essentially eviscerate the law's intention behind allowing third parties to assist consumers in making access and deletion requests.

We suggest including a standard taken from the statute in Civil Code section 1798.185(a)(7), in our proposed amendment to section 999.326(a)(3) : "When a consumer uses an authorized agent to submit a request to know or a request to delete, ~~the~~ a business may require that the consumer do the following:…Directly confirm with the business that they provided the authorized agent permission to submit the request, **provided such confirmation process should not create undue administrative burdens on the consumer to prove their permission**." W212-45

Section 999.326(e): We applaud this addition and think it is excellent. W212-46

Minors Under 13 Years of Age (999.330)

Section 999.330(a)(2)(a): As noted above, "signed" is defined in the regulations as either a physical signature or an electronic one, so we think this addition is unnecessary. W212-47

Section 999.330(b): Upon reflection, we are concerned this clause's wording could allow businesses to circumvent its intention, given the inclusion of "at a later date."

In the interests of clarity we suggest the following: "When a business receives an affirmative authorization pursuant to subsection (a) of this section, the business shall inform the parent or guardian of the right to opt-out ~~at a later date~~ and of the process for doing so on behalf of their child pursuant to section 999.315, subdivision (a) through (f)." W212-48

Discriminatory Practices (999.336)

Section 999.336(b): This addition is excellent and will achieve some of CCPA's most important goals of protecting consumers. W212-49

Section 999.336(d)(3): We suggest expanding Example 3, as follows:

"Example 3: … This practice is discriminatory unless the grocery store can demonstrate that the value of the coupons and special discounts are reasonably related to the value **to the business** of **selling** the consumer's data ~~to the business~~." W212-50

We think this addition would clarify that the operative function in this example is, self-evidently, the value to the business from ***selling*** the consumer's data; and we think it useful to clarify to businesses that that is the calculation they must be prepared to support in this example.

Section 999.337(b): We think this addition is fine, but we think it is **vital** to clarify that this should refer to all **US residents**. We suggest amending as follows: "For the purpose of calculating the value of consumer data, a business may consider the value of the data of all natural **United States residents** ~~persons~~ to the business and not just consumers." We are concerned that absent this change, this clause will allow multinationals to vastly understate how much they earn selling consumers' information, as the value of a consumer in India, Indonesia or Nigeria is vastly different than one in the United States, yet many of the internet giants have billions of customers in those countries. W212-51

Now, a privacy proponent could argue that having a lower number here is better, in that the amount a business may charge a consumer to opt-out of the sale of their information, would be lower.

However, we have always believed that one of the best aspects of CCPA is the chilling effect it will have on the practice of selling personal information, from requiring businesses to publicly state how much money they are earning from selling their own customers' information. We think many customers will recoil at the knowledge that a business they use, is turning around and making $X from selling their information.

Thank you for your consideration of our comments.

Yours sincerely,

/s/ Alastair Mactaggart, Chair

Californians for Consumer Privacy

From: Brent Blackaby
To: Privacy Regulations
Cc: Crid Yu
Subject: Written comment on revised CCPA regulations
Date: Tuesday, February 25, 2020 5:04:38 PM
Attachments: 20200225 CCPA revised comment.pdf

Attached please find written comments on the revised CCPA regulations from Brent Blackaby and Crid Yu at Confidently.com.

Please email or call us at [redacted] with any questions or concerns.

Thank you,

Brent Blackaby
Confidently.com

CCPA public comment

Submitted by:
Brent Blackaby & Crid Yu
Confidently.com

February 25, 2020

We appreciate the thoroughness and thoughtfulness with which the Attorney General and his staff considered public comments on the CCPA's draft implementation regulations. Thank you for the opportunity to have provided both oral and written comments in December.

Now, upon reading the revised regulations, we have additional comments to offer.

We are submitting these comments as two California residents who deeply care about our own online privacy, as well as co-founders of Confidently.com, a new company building products and services to help consumers take full advantage of the new privacy rights they've been granted here in California. Our aim is for consumers to fully realize their rights to their privacy, so our comments are all offered in that spirit.

There are three main areas where we offer feedback:

- **999.323** -- We suggest creating a new option that if agents use third-party verification services to verify their customers, before passing requests on to businesses, that those customers & their requests should be treated as verified upon receipt by the business. This would both help businesses – by reducing the verification load they have to bear – as well as make it possible for consumers to exercise their rights in more places. It's duplicative work that could be streamlined if the agent takes on the responsibility for third party verification. W213-1
- **999.324** -- We suggest that agents should be able to make access/delete requests on behalf of their customers without having to go through logged in customer accounts/dashboards if using a third party verification service above. This would make it much easier for consumers to exercise their privacy rights in more places, while still ensuring requests are authorized by consumers via their agents and verified before being processed by businesses. W213-2
- **999.326** -- We don't think that consumers should be asked to re-verify their identity with a business if an agent has already submitted verification materials to the business on the consumer's behalf. Similarly, we don't think consumers should be required to confirm with a business that they authorized the agent, if an agent submits a signed authorization form from the consumer along with the initial request. Both of these seem duplicative and onerous to the consumer, and would inhibit consumers from making privacy requests to every business they want to contact. W213-3

Thank you for considering these comments. We look forward to working with you on behalf of all California consumers to make sure they can fully exercise their new privacy rights under the CCPA!

Sincerely,

Brent Blackaby & Crid Yu
Co-Founders
Confidently.com, Inc.

From: Abrahamson, Reed C.F.
To: Privacy Regulations
Cc: Blenkinsop, Peter
Subject: Comments from IPMPC on CCPA Rulemaking
Date: Tuesday, February 25, 2020 5:00:00 PM
Attachments: Final IPMPC Comments - Revised CCPA Regulations 02252020.PDF
ATT00001.htm

To Whom it May Concern:

Please find the IPMPC's written comments on the revised draft CCPA regulations attached. The IPMPC appreciates the opportunity to provide comments.

Please don't hesitate to reach out if there's any difficulty opening or reviewing the attached. We would appreciate confirmation of receipt.

Best,

Reed Abrahamson
Associate
[redacted]
[redacted] direct / +1 202 842 8465 fax

Faegre Drinker Biddle & Reath LLP
1500 K Street NW, Suite 1100
Washington, DC 20005, USA
<!--[if !supportLineBreakNewLine]-->
<!--[endif]-->

February 25, 2020

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: Revised CCPA Proposed Regulations

Dear Attorney General Becerra,

The International Pharmaceutical & Medical Device Privacy Consortium ("IPMPC") welcomes the opportunity to provide comments on the revised 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]

[1] IPMPC members may also operate related businesses, including in vitro diagnostics manufacturing and 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.

1500 K Street, NW, Washington, DC 20005 USA
Tel: +1.202.230.5619
www.ipmpc.org

The IPMPC appreciates the revisions made by the Attorney General to the first draft of the CCPA regulations. The changes in the second draft provide needed clarity. However, the IPMPC believes that, in some areas, the new requirements may create consumer confusion—including by requiring businesses to implement ambiguous consumer-facing notices and icons. The IPMPC also believes that the revised regulations create new requirements that are not called for by the CCPA and have little benefit to consumers.

§ _.301(c) The IPMPC appreciates the additional clarity about the requirements for an "authorized agent," and requests that the Attorney General make it clear that, when someone other than the consumer submits a request on a consumer's behalf, and that person does not meet the definition of "authorized agent," a business is permitted to deny the request. W214-1

§ _.302 The IPMPC believes the guidance provided by the Attorney General offers needed clarity about the standard to be applied when determining whether data held by a business is "personal information." In many cases, IPMPC members collect data for medical or scientific research that includes information that member companies do not and could not link with a specific person. Clarification about the impact of the CCPA on these important research functions will allow IPMPC members to proceed with greater certainty about the regulatory requirements applicable to research designed to improve patient health, increase access to medicines, and identify important treatments. W214-2

Although the additional interpretative note clarifies the applicable standard, the IPMPC believes that a further statement about what information should be considered either deidentified or not personal information would be helpful. In particular, the IPMPC urges the Attorney General to make it clear that information which has been deidentified using a process described in federal regulations (like the HIPAA deidentification standards) will be considered deidentified for the purposes of the CCPA.

§ _.305(a)(3) The IPMPC appreciates the Attorney General's inclusion of additional examples, and requests that the Attorney General clarify § 999.305(a)(3)(d) to make it clear that, when a business collects information over the telephone or in person, in addition to the option of providing notice orally, a business also has the option of directing consumers to "where the notice can be found online," as described in § 999.305(a)(3)(c). W214-3

The IPMPC also requests clarification of the term "download page" in § 999.305(a)(3)(b). Most applications are downloaded from an application store—is the regulation intended to require posting of the privacy notice within the application store where the application is available for download? W214-4

§ _.306(e) The IPMPC requests that the Attorney General clarify the scope of this new section, and make it clear that the prohibition on selling data applies only to information collected after the CCPA's effective date. W214-5

§ _.306(f) The IPMPC requests that the Attorney General consider alternative designs for the opt-out button. The current proposed design of the button looks like switches that consumers are used to encountering in mobile devices or applications. However, the required functionality of the button is to serve as a link to the webpage or online location where the consumer can provide their information to accomplish the opt-out. Consumers may be misled or frustrated when this occurs, since—based on their previous experiences with switches—they will likely expect to be able to click the button and have it "turn off." To discover that, instead, they are being routed (as required by the law and these regulations) to a new page where they can provide the information required to implement the opt-out may be a surprise. Consumers may come to believe that such pages are non-compliant, even though they in fact follow the letter of the law and regulations. W214-6

Instead, the IPMPC urges the Attorney General to adopt a button that clearly implies to consumers that clicking the button will take them to a new page, where the consumer can provide information and opt-out. The IPMPC also requests that the Attorney General allow businesses to modify the color scheme, design, and placement of the button—provided it remains materially recognizable as the "Opt-Out" button and stays conspicuous—so that the button and accompanying link can be made consistent with and incorporated into the other design elements of a business's website. For the design of the button, the IPMPC suggests something like the below:

Finally, the IPMPC notes that not all websites contain buttons currently. Accordingly, the requirement in § 999.306(f)(2) that the button be "the same size as W214-7

other buttons on the business's website" should be made conditional, and apply only when other buttons are present. W214-7 (cont.)

§ _.313(c) The IPMPC appreciates the Attorney General's clarification about the kind of information that must be searched in response to a consumer's request to know. However, the IPMPC urges the Attorney General to restore a modified version of the deleted text that clearly establishes that businesses are not required to put other consumers at risk of harm in responding to a different consumer's request to know. When information about a consumer is being maintained for the purpose of protecting the security of the business's systems or networks, an important part of what is being protected is the personal information of *other* consumers, employees, and their dependents. W214-8

The Attorney General's previous draft aimed to strike a balance between consumer rights and the need to protect personal information. The IPMPC supports reincorporation of a slightly modified version of the deleted text, as follows: "A business is not required to provide a consumer with specific pieces of personal information if the disclosure creates an unreasonable risk to the security of that personal information, the personal information of other consumers, employees, and their dependents, the consumer's account with the business, or the security of the business's systems or networks."

The IPMPC requests that the Attorney General include a clause acknowledging that the CCPA permits non-disclosure when another exemption to CCPA applies, like in the case of a privileged communication or where disclosure would violate an applicable law. W214-9

§ _.313(d)(3) The IPMPC requests that the Attorney General clarify that deletion of information in an archived or backup system is only required when the information is restored *and* accessed or used for a sale, disclosure, or commercial purpose. Data is usually restored from archives or back-ups when an incident occurs that impacts the businesses' existing information systems. Restoring systems quickly is often vital to prevent negative consequences for the business, its customers, and employees. Requiring businesses to pause and reconcile systems with deletion records immediately upon restoration would create an unnecessary obstacle to the resumption of normal operations. Consumers would still be protected by the requirement that deletion occur before the data is used for a commercial purpose. W214-10

§ _.314(c)	The IPMPC requests that the Attorney General define the words "cleaning" and "augmenting" in § 999.314(c)(3), and reconsider these exclusions. Prohibiting service providers from using other information in their possession to correct erroneous, incomplete, or outdated records just means that erroneous, incomplete, and outdated records will remain in use by businesses until rectified by the consumer. The benefit to consumers from this exclusion seems negligible.	W214-11
§ _.314(e)	The IPMPC requests that the Attorney General note that a service provider may act on behalf of a business to respond to a consumer request only when the service provider has been authorized by the business to respond on its behalf. Otherwise, consumers may be confused about who acted on their request and what information was covered.	W214-12
§ _.317(e)	The IPMPC suggests that the Attorney General revise the restriction on sharing record-keeping information with third parties, and explicitly acknowledge that such information may be shared with service providers (including attorneys and auditors retained to assess compliance with the CCPA) and with third parties when an exception to the CCPA applies—like where required by law or in the course of defending a legal claim.	W214-13
§ _.317(g)(2)	The IPMPC asks the Attorney General to indicate that this obligation commences on July 1, 2021. Otherwise, businesses will not have time to compile the necessary records, and will not have a full year's worth of data to report.	W214-14

Finally, the IPMPC reiterates its request from our initial set of comments: We ask that the Attorney General publish examples of the various notices and responses to consumer requests that would be required under the proposed regulations. Example materials will greatly assist businesses in crafting compliance materials that meet consumer expectations under the CCPA. W214-15

We thank you for the opportunity to provide these comments.

Sincerely,

Peter A. Blenkinsop
IPMPC Secretariat

From: Paul Jurcys
To: Privacy Regulations
Cc: Markus Lampinen
Subject: Comments to CCPA Regulations | Prifina
Date: Tuesday, February 25, 2020 4:59:16 PM
Attachments: Prifina - Comments Concerning CCPA.pdf

Dear Privacy Regulations Coordinator,

Please find Prifina's Comments to the proposed Draft Privacy Regulations.

Sincerely,

Paul Jurcys

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

I. Comparative Study of CCPA Comments

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

Prifina applauds the Attorney General on its initiative with the implementation of CCPA and the desire to seek a balance between individual rights and businesses' ability to provide valuable services. We were both enthused and surprised by the attention that the CCPA public comment period received and the engagement from the industry.

Considering the number of the comments submitted as well as the sophistication of insights provided therein, Ptifina saw this as an opportunity to harness that information into a more structured, industry representative format. Therefore, Prifina undertook the effort to categorize and organize the CCPA comment submitted by various stakeholders into a more comprehensive format.

In this comment letter, we will briefly explain our methodology for aggregating the public comments, provide a brief overview of our findings and offer some suggestions of how the Office of Attorney General should move forward.

The data set, methodology and related findings, as well as further updates, will be made publicly available.

Methodology

During the first comment period, the Office of the Attorney General received hundreds of written and oral comments regarding the proposed text of the CCPA Regulations.[1] The Prifina team reviewed those submitted comments and categorized them using the following taxonomy. First, eight groups of stakeholders became quite obvious:

1. Financial institutions: appr. 10%
2. Law Firms: appr. 8%
3. Consumer NGOs: appr. 6%
4. B2B compliance companies: appr. 3%
5. Consumer-rights/interest companies: appr. 3/100
6. Businesses: appr. 22%
7. Trade associations: appr. 31%
8. Individual consumers, researchers, and other non-profit associations: appr. 17%.

[1] The files are available at: https://oag.ca.gov/privacy/ccpa (last viewed on Feb. 25, 2020).

Based on the substance of the comments, it was clear that the main themes of the comments were related to the issues falling within the scope of the CCPA Regulations, namely:

Scope of CCPA Regulations

Scope of Application
Territorial Reach
Relationship with Other Statutes

Definitions

Personal Information

Notices to Consumers

Notice at the Collection of PI
Notice of the Right to Opt-Out of Sale of PI
Notice of Financial Incentive
Privacy Policy

Verification of Requests

Verification for Password-protected Accounts
Verification for Non-account Holders
Authorized Agents

Sales of Data

Definition of "Sales"
Opt-Out Requests
Practical Aspects of Compliance

Handling Consumer Requests

Methods for Submitting Requests to Know and Requests to Delete
Responding to Requests to Know and Requests to Delete
Service Providers
Requests to Opt-Out
Training, Record-Keeping
Requests to Access or Delete Household Information
Privacy by Design

Minors

Notices to Minors
Opting-in to the sale of PI

Non-Discrimination

Discriminatory Practices

Value of Customer Data

Methods of Assessing the Value of Customer Data

Effective Date

Statistics and Findings of the Study

The comments submitted during the first comment period were categorized by allocating the interested party to one of the eight stakeholder groups. Then, we conducted a comprehensive study by analyzing which themes were addressed by each commenting party. Our findings are illustrated in the graph below[2]:

[2] An updated graph with a more comprehensive report will be available here: www.prifina.com/research.

prifina

MAIN THEMES IN THE NEW DATA ECONOMY

Authors: Dr. Paul Jurcys, Markus Lampinen. Designer: Daniel Ali

A study on the public comments on the California Consumer Protection Act (CCPA) and the key themes that are raised by different interests groups.

COVERAGE OF THEMES:

HIGHER LOWER

The size of each dot in the map represents the aggregate emphasis given to a specific theme. The Map does not represent broader issues raised by certain stakeholders (e.g., wider economic implications, general principles such as data portability or extralegal factors that could shape the regulatory framework for data privacy in California).

Instead the themes represented in the map focus on the content of the CCPA and the Proposed Regulations:

Scope
- Scope of Application
- Territorial Reach
- Relationship with Other Statutes

Definitions
- Personal information

Notice to Consumers
- Notice at the Collection of PI
- Notice of the Right to Opt-out of Sale of PI
- Notice of Financial Incentive
- Privacy Policy

Handling Requests
- Methods for Submitting
- Requests to Know and
- Requests to Delete
- Responding to Requests to Know and Requests to Delete
- Service Providers
- Requests to Opt-out
- Training, Record-keeping
- Requests to Access or Delete Household Information
- Privacy by Design

Request Verifications
- Verification for Password-protected Accounts
- Verification for Non-account Holders
- Authorized Agents

Sales of Data
- Definition of "Sales"
- Opt-Out Requests
- Practical Aspects of Compliance

Minors
- Notices to Minors
- Opting-in to the sale of PI

Non-Discrimination
- Discriminatory Practices

Value of Consumers Data
- Methods of Assessing the Value of Customer Data

Effective Date

Updated information on findings, methodology and related research can be found at www.prifina.com/research

prifina

prifina

A comprehensive study of the submitted comments, feedback and recommendations submitted by various stakeholders revealed that different groups share similar concerns. For instance, credit unions and smaller financial institutions are mostly concerned with the fact that they are under-resourced to cope with the requirements imposed by the CCPA; fear that due to the complexity of data privacy they will not be able to timely comply with all of the requirements of the CCPA and therefore request to extend the effective date of the Regulations. Credit unions and financial institutions are navigating a complex regulatory environment and need more guidance on how their new obligations imposed by the CCPA should be aligned with the existing regulatory requirements (e.g., under the Gramm-Leach-Bliley Act, etc.). Furthermore, comments submitted by credit unions and financial institutions brought to daylight the desire from the finance industry to have template notices and privacy policies.

Although the discussion around data privacy is still nascent and the full effects of the CCPA remain to be seen, we can identify some commonalities from the themes raised by the stakeholders. We see there are three overarching themes within the comments that can be highlighted, namely: data portability, transparency around how data (explicit consent), and the balanced use of data.

The full version of Prifina's comparative study will be made available at: www.prifina.com/research.

II. Suggestions for the OAG Future Activities

Based on the fact that different sectors share different concerns, Prifina invites the Office of the Attorney General to consider four spheres in which it could cooperate with the interested parties and stakeholders.

1) Facilitate an Environment for Bottom-Up Solutions

In order to provide support and frameworks for new regulations such as the CCPA as well as business opportunities to build upon such regulations, several new initiatives have been undertaken. These include the Data Portability Project that has been sponsored by Google and aims to provide tools for individuals to easier extract their data from data platforms like Google, Facebook and others and bring it with them to other companies and services.[3]

Prifina believes data portability is a fundamental aspect that the market should address to give individuals more control, visibility and ultimately value from their own data. However, new types of tools are necessary to ascertain that personal data is used in a balanced way that does not become a race to the bottom, where individuals have sold all rights to their data for short term utility. This is why Prifina has proposed a set of Personal Data Licenses, where individuals would be able to attach certain rights and restrictions, akin to the CCPA's 'do not sell my data' language. This framework has been released to the public and Prifina will be advocating for bringing these rights closer to the individual, where the individual has more of a say in how an individual's personal data is used. Prifina has also released related open source developer tools to build applications on top of this framework. [4] W215-1

2) Provide Authoritative Guidance

The Office of the Attorney General could provide a compliance compendium of how CCPA and Regulations are implemented in practice. Such a compendium would especially welcome by various industries where compliance with notice and request requirements are deemed to be the biggest challenge. Such a compendium would contribute to greater transparency, legal certainty and reduce CCPA-related compliance costs for businesses. Similar practices are used by, e.g., the US Copyright Office.[5]

[3] See https://datatransferproject.dev/ (last viewed on Feb. 25, 2020).
[4] See https://shorturl.at/fGHL5 (last viewed on Feb. 25, 2020).
[5] See https://www.copyright.gov/comp3/ (last viewed on Feb. 25, 2020).

3) Work Closely with Businesses

The Office of Attorney General may consider working closely with businesses in developing practical solutions towards the most efficient ways to facilitate the development of best practices in implementing the main principles and requirements under the CCPA. For instance, the Office of the Attorney General could consider collaborating with the representatives of various industries in finding the best industry-specific practices that are capable to delicately balance the consumer-facing privacy-preserving tools with the relevant capacities of businesses.

W215-1 (cont.)

4) Look Beyond Compliance

Prifina has seen that following the implementation of the General Data Protection Regulation in 2018 in Europe, many businesses and stakeholders created solutions that were not only focused on compliance with such regulation but rather how such a regulation allowed them to create more thriving businesses and consumer value. We anticipate similar development in California, where businesses will be forced to create better value for their customers based on the new regulations and will not only comply but end up delivering better service. Given the emphasis on compliance and risk-management, we believe it would be valuable to showcase and give a forum for companies creating new solutions upon this new paradigm, where new regulations can also be seen as an opportunity to drive more consumer value.

From: Aleecia M McDonald
To: Privacy Regulations
Subject: comments regarding the proposed changes, CCPA
Date: Tuesday, February 25, 2020 4:58:44 PM
Attachments: McDonald-Comments-to-AG-CCPA-Rulemaking.pdf

Comments from:
Aleecia M. McDonald
NASA Ames Research Center
Carnegie Mellon University
Building 23, Office 220
Moffett Field, CA 94035

[redacted]

February 25, 2020

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

Regarding

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)

About the Author

Aleecia M. McDonald is an Assistant Professor at Carnegie Mellon's Information Networking Institute, based in Silicon Valley. Her *Psst!* Lab focuses on researching the public policy issues of Internet privacy including user expectations, behavioral economics and mental models of privacy, and the efficacy of industry self-regulation. She co-chaired the WC3's Tracking Protection Working Group, a multi-national effort to establish international standards for a Do Not Track mechanism that users can enable to request enhanced privacy online. She presented testimony to the California Assembly including regarding the California Consumer Privacy Act, contributed to testimony before the United States Senate, and presented research results to the Federal Trade Commission.

Professor McDonald is a member of the Board of Directors for the Privacy Rights Clearinghouse, and is a member of Carnegie Mellon's CyLab. She was Director of Privacy at the Stanford Center for Internet and Society where she maintains a non-resident Fellow affiliation. She was also previously a Senior Privacy Researcher for Mozilla during the rollout of Do Not Track in the Firefox web browser. A decade of experience working in software startups adds a practical focus to her academic work. She holds a PhD in Engineering & Public Policy from Carnegie Mellon.

Affiliations are for identification and context only. These comments reflect Professor McDonald's views alone; she does not speak for any other groups, nor do they speak for her.

Summary

In this comment I urge the following courses of action:

1. Use the language from the Initial Proposed Regulations rather than the revisions to require categories of data are specified in 999.305(b), 999.308(c)(1)(d), 999.313(c)(10) — W216-1
2. Use the language from the Initial Proposed Regulations rather than the revisions in 999.313(c)(4) to continue CCPA protections for biometric data — W216-2
3. Make the opt-out button a live control on website home pages, in addition to linking to additional controls and information — W216-3
    - Fully test the opt-out button before deployment, with a short timeframe to do so
4. Require companies honor user choices via header signals like Do Not Track — W216-4
    - Update header signal approaches in light of CCPA, with a short timeframe to do so
    - Add a short comment period specifically tailored to implementation details

Table of Contents

Topic 1: Information Required for Enacting Privacy Choices

Thank you for the opportunity to comment on the proposed rulemaking around the California Consumer Privacy Act (CCPA.) I have studied and contributed to work around enacting users' privacy preferences for what is now approaching two decades. CCPA holds great promise as a mechanism to help Californians make and enact privacy choices for themselves. Prior lighter-touch attempts from the FTC, industry self-regulation groups, privacy enhancing technologies, and standards bodies have failed to provide meaningful and actionable privacy controls. On June 27, 2018, I testified before the California Assembly Committee on Privacy and Consumer Protection in favor of CCPA as a good step forward along the path of citizen empowerment.

Notice must have details to support decision making

The process from proposition to today has not been kind to citizens' CCPA rights. Recent proposals would water down an already modest law. Weakening the detailed notice portions of CCPA (e.g. the removal of linkages between collection, purposes, and sharing in sections 999.305(b), 999.308(c)(1)(d), and 999.313(c)(10)) necessarily thwarts the ability of Californians not only to know what is collected, by whom, for which original and additional purposes, but furthermore makes it impossible for Californians to have the information they need to make decisions. Citizens' choices become either blind trust for those who collect and hold their data or saying no, even to things they would readily agree to.

W216-1 (cont.)

Currently citizens face deep *information asymmetries*. Companies have all of the information about data collection, disclosure, use, and re-use. Citizens are left with hints and clues as best they can patch

together. Privacy policies should have reduced information asymmetries to the point much of CCPA would not be necessary, but instead companies elected a different path of vague, hard-to-read text. Because CCPA's original aim would bring clarity to data collection, disclosure, use, and re-use, post-CCPA privacy policies should be clearer and more readable than they have been to date.[1]

All of the points above dovetail with the filing from Professor Scott Jordan at UC Irvine. Having read a draft of his comments, I agree with and endorse his filing.

W216-1 (cont.)

RECOMMENDED: use the language from the Initial Proposed Regulations rather than the revisions to require categories of data as specified in 999.305(b), 999.308(c)(1)(d), 999.313(c)(10)

Biometric data must be disclosed to support decision making

Section 999.313(c)(4) addresses concerns about identity theft by ensuring CCPA requests do not inadvertently provide would-be thieves with information like social security numbers or account numbers. This is information citizens may already have, and is arguably a reasonable security provision in those cases.

However, recent modifications add "unique biometric data generated from measurements or technical analysis of human characteristics" to the list of data that must not be disclosed in response to a CCPA request. This is ill-advised. Citizens have a right to know what data is held about them. Further, both that biometric data is held at all and the biometrics themselves would be opaque to most Californians, in stark contrast to known information like account numbers. From 1973 forward, privacy thinking has included the bedrock principle of "no secret databases."[2] Facial recognition, gate analysis, and genetic data should all be disclosed to Californians. Once again, without information, citizens cannot make privacy decisions.

W216-2 (cont.)

Furthermore, there are open legal questions about what counts as biometric information, with caselaw undecided on basics like: are photos biometrics? The revised text provides a carve out that is too broad and too vague to address security issues, but decidedly weakens Californians' rights.

RECOMMENDED: Use the language from the Initial Proposed Regulations rather than the revisions in 999.313(c)(4) to continue CCPA protections for biometric data.

Privacy decision making requires detailed information

In short: people cannot make privacy decisions without specific information about what is collected and how it is used. CCPA was designed to give citizens rights that let them understand what happens with their data. Curtailing these rights will put companies through the trouble of redoing their privacy policies without actionable benefit to Californians, leaving CCPA as cost to companies, yet minimal gain for citizens.

[1] If useful to your office, I am happy to create an annotated bibliography of related research regarding privacy policy readability. There is much prior work in this area.

[2] Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, *Department of Health, Education, and Welfare* (July, 1973)

Topic 2: Controls for Enacting Privacy Choices

One of the statutory responsibilities for the California Attorney General's office is to operationalize the "do not sell" controls that CCPA requires on websites. I read prior comments from Professor Cranor et. al.[3] and the California Attorney General's revised suggested text[4] with great interest.

We can measure the success of such controls against the following goal: **Californians' privacy preferences should closely match their CCPA "do not sell" settings.**

Designing clear and understandable controls is one vital step to get to that goal. Again, without information, control is impossible. Studying the comprehension of controls is a vital next step, well in progress. Finally, we must study how well controls work in practice to enact choice in a realistic on-going setting.

I propose the following three additional refinements:

1. The "do not sell" widget should be an actual control, not merely a pointer to a control on a subsequent page.
2. The "do not sell" widget should accurately reflect if the website operator has a current "do not sell" setting for this user (either via opt-out or due to age-related opt-in requirements.)
3. Test, test, test all proposals with the metric for success as above: getting the smallest discrepancy between what individual Californians prefer to have happen and what actually does happen in practice.

W216-3 (cont.)

Companies have already started to experiment with slider controls, sometimes as a response to GDPR prior to CCPA. For example, the Ann Taylor website[5] uses a OneTrust widget to offer controls for categories of cookies, with one example shown in Figure 1. This approach has some similarities to the proposals from Cranor *et. al.* and the Attorney General's draft.

[3] Cranor, Habib, Zou, Acquisti, Reidenberg, Sadeh, Schaub, Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA, February 4, 2020. Available from <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-cranor.pdf>

[4] Text of modified regulations [clean version] Title 11. Law Division 1. Attorney General Chapter 20. California Consumer Privacy Act Regulations Proposed Text of Regulations, page 8. Available from <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf>

[5] Ann Taylor Cookie Consent Manager, linked from <https://www.anntaylor.com/privacy>

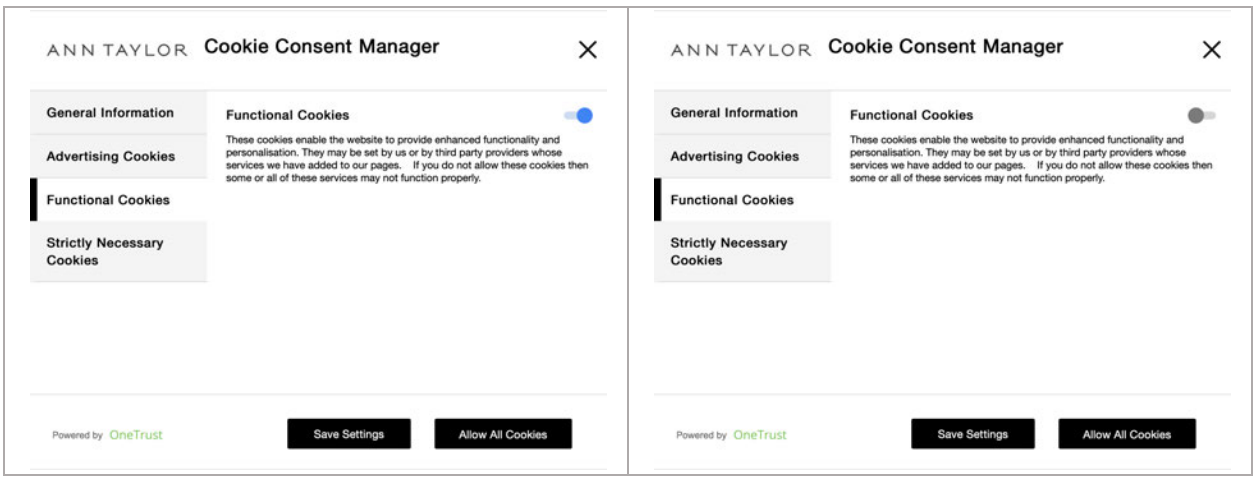


Figure 1: A slider control for cookies. Which side shows that functional cookies will be set? Elsewhere, directions include: Toggle switch is Blue when "Active" and Gray when "Inactive". *This raises new questions: does "active" mean cookies set, or cookies do not set? Can most Californians reliably understand what this means, how the widget works, and then successfully enact their personal privacy preferences accordingly?*

The good

The very good parts about the OneTrust widget are:

a) The slider responds in real-time to user interactions. That is, the toggle flips from right to left (or vice versa) and from blue to grey (or vice versa.) This provides necessary feedback that yes, something has occurred.

b) The slider reflects the website operator's understanding of privacy preferences over time. That is, if a user quits the browser and returns, the setting still shows prior choices. One easy way to do this is to instrument the widget to use locally stored cookies. Another approach is to store preference information on a server remote from the user. Both methods are well understood and reasonably easy to implement. Again this provides necessary feedback to citizens so they are informed about what companies are doing.

W216-3 (cont.)

The bad

There is room to improve upon this widget design, which was attempted (perhaps by Ann Taylor) with additional text directions on yet another screen:

> Toggle switch is Blue when "Active" and Gray when "Inactive".

This is a valiant attempt yet a bad sign when simple user interface design has to be explained. The text is still insufficient to provide clarity. Are cookies set when the toggle is blue or when it is grey? What does "Active" mean? One hopes the AG's office final design will not suffer such flaws. I expect the current proposal is very close but not quite there yet. Just a few more rounds of testing and refinement could establish greater efficacy, with benefits to Californians and companies alike.

The ugly

In order to change any settings with the OneTrust widget as implemented on the Ann Taylor website, it takes at least the following steps (there are more circuitous paths as well)

1. Scroll to the bottom of the home page
2. Click on the "Privacy Policy" link
3. Notice a smaller pop up window

4. Spot the "Manage Preferences" link (same font, same color as regular text)
5. Click "Manage Preferences"
6. On the left side, click a data category
7. On the right side of the resulting window, toggle a slider

Amazon patented "1-click" ordering because they understand how many customers they lose every time an additional step is needed to do the task the customer set out to do, which in this case is how Amazon makes money. Every time a user has to click is a time that user may give up on the task. Each of the steps listed above above is a barrier to successfully realizing privacy rights.

To fulfill the requirements of 1798.135(a)(1) the CCPA widget must also have a link "to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information." That requirement is not affected by also having the button to opt out from sale be a live button on the home page: the button simply needs an additional area to click for more rights that include opting out of sale. The Attorney General has the authority to detail how the homepage Do Not Sell works, both by 1798.135(a) and 1798.185(a) ("To facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information…")

W216-3 (cont.)

A path forward

The public policy goal of the control should neither be the most people opting out of sale, nor the lowest rate of opt outs, but rather that which reflects each Californian's individual preferences most accurately. I strongly believe that if the toggle switch currently undergoing revisions becomes an *actual* control, right there on the home page, rather than yet another step in a process, Californians will be able to enact their preferences more accurately.

It is worth the time to get the interface as usable as possible. If Californians have a bad first experience, it is very hard for them to re-learn that a new design is available and improved.

The thing about user interface design is that despite years of experience with privacy controls, I could be wrong! This is why I once again urge substantial testing of all proposals under realistic use conditions, again with the metric of matching what people actually want to happen.

RECOMMENDED: update the Modified Regulations for 999.306(f) ("Opt-Out Button") as appropriate based on the results from further user testing, and as to include the following requirements:

1. The opt-out button must reflect the website operator's current understanding of the visitor's opt-out status
2. The opt-out button must be a one-click control on the website, as well as containing a link to additional CCPA information and controls

Topic 3: Do Not Track and the California Consumer Privacy Act

The prior section addresses privacy choices for one website, with implications for any additional businesses to whom they send data. Asking Californians to enact their preferences on each website they visit, plus third parties, plus data brokers, plus apps, plus offline parties is a substantial user

W216-4 (cont.)

burden. Unmanaged, the problem of scale can obliterate effective user choice. If the bar is too high, CCPA becomes moot in practice.

As one example of the problem of scale, I teach a class in CyberSecurity Risks and Threats. In understanding what CCPA compliance might look like, I assigned homework to exercise any CCPA right. The results were painful to read and grade: pages of back-and-forth with companies to request basic CCPA rights. Now imagine this at scale. In my case, it was homework from 50 students, but this could just as easily be the experience of one person trying to get copies of information, delete information, and/or stop the sale of information with 50 companies – or more. It would take days.

As a second example, a journalist recently did exactly that.[6] With good website controls as mentioned in the prior section, the time for opting out of sale could reduce considerably. Perhaps in the future citizens will not have as much additional follow up time as my students and the *Washington Post* journalist faced. However, there remains the daunting task of learning which companies one might opt out from. For the Californians who want to opt out of all data collection and use possible, even with databases of hundreds of known data brokers available,[7] establishing a list of which parties to contact is daunting. Then there is the task of finding out how to opt out for each one, and then actually doing so. More vexing, due to the dynamic data marketplace, relevant parties are different over time. It is not enough to spend a few days opting out one time; privacy preserving citizens must continue the "never-ending project."[8]

W216-4 (cont.)

This brings us to one reason why a Do Not Track signal can help Californians realize their CCPA rights: **Do Not Track operates at web scale.** Comments in the docket and reply comments encourage leveraging Do Not Track (or similar header signals) to support CCPA rights, as authored by Californians for Consumer Privacy,[9] the Electronic Frontier Foundation,[10] the Digital Privacy Alliance,[11] and Consumer Reports.[12] Some, but not all, of these authors were participants in the W3C

[6] Geoffrey Fowler, Don't sell my data! We finally have a law for that, *The Washington Post* (February 12, 2020.) Available from <https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq>

[7] For example, 232 listed as of March 24, 2010 in: Data Brokers, *Privacy Rights Clearinghouse.* Available from <https://privacyrights.org/data-brokers>

[8] Geoffrey Fowler, IBID.

[9] "Opt-Out Through Global Setting: Section 999.315(a) allows consumers to opt-out of the sale of their personal information through a minimum of two or more methods, including a browser plugin or privacy setting as specified in 1798.BS(c) and further defined in 1798.185(a)(4)1, but the regulation should clarify that this includes a global device or browser setting. This is an incredibly important component of the law and critical to its function in the marketplace. Businesses should not be able to preclude consumers from exercising their right to opt-out through a global setting, as authorized by Civil Code section 1798.BS(c), by limiting consumers to two, less convenient, opt-out methods. […] Finally, the Attorney General should consider certifying existing privacy or device settings, such as the Do Not Track preference expression as defined by the W3C, as adequate for the purpose of indicating a consumer's intent to opt-out of sale of the consumer's personal information. This would ensure that a global setting is available to consumers when the law goes into effect in 2020."

[10] "EFF proposes that the AG require any business that interacts with consumers directly over the Internet using HTTP or HTTPS to treat an HTTP request with a DNT header set to 1 as a binding request to opt-out of data collection. There should be different DNT rules depending on whether the user is logged-in or otherwise verified as the controller of an account with the business. If so, the business should be required to consider the DNT header as an affirmative request to opt-out of all sales of the consumer's data until the consumer decides to opt back in. If not, the business should consider it a request to opt-out only from the sale of data collected in the current session."

[11] To ensure the effectiveness of these proposed rules, the coalition requests the addition of the following sentence to the end of both Section 315(a) and 315(c): A business shall treat a "do not track" browsing header as such a choice.

[12] "The AG should clarify that companies need to comply with platform-level opt-outs similar to IoS Limit Ad Tracking and Do Not Track if offered.

Tracking Protection Working Group and they have a strong understanding of the technical advantages conferred by a Do Not Track (or similar) signal. Not all of these four groups are requesting the same use of Do Not Track. Yet the appeal seems to stem from common concerns. For example, Californians for Consumer Privacy and Consumer Reports specifically point out that Do Not Track is useful at the scale of an entire platform. This avoids the whack-a-mole task of opting out party-by-party described above.

Due to the technical details of how HTTP cookies and header signals work:

- HTTP cookies can only send an opt-out or opt-in preference back to the initial party that set the cookie. They are a one-to-one mechanism.
- Header signals like Do Not Track automatically go out to every party loading data from a website. They are a one-to-many mechanism.

If a header signal becomes a required part of CCPA regulatory compliance, Californians will no longer face the daunting burden of first discovering which parties are involved in order to be able to use their CCPA rights. For example, with a header signal Californians can elect either to opt-out (adults) or consent to opt-in (children) very few times[13] rather than literally hundreds of times.

W216-4 (cont.)

Perhaps more crucially, the technical characteristics of header signals also mean website operators also do not need to know which parties are involved with their own websites. For example, say a Californian visits the fictitious website myNews.com. The myNews corporation sells ad space on their website via real-time ad auctions, and myNews cannot know in advance (a) which party will win the auction, (b) which parties are even part of the full universe of those bidding to win the ad auction at any given time. The composition of parties bidding will change over time, dynamically. If myNews.com wanted to tell all business partners "this is an under 16-year-old California visitor without consent to data collection," there is currently no practical way to do so. However, by using a header signal instead of storing opt-out status in HTTP cookies one per party, all parties would get an opt-out signal from the user, directly, *with no coordination needed between parties.*

The advantages here are both to the companies implementing CCPA compliance solutions at what might be lower cost and with less complexity, as well as usability advantages to Californians enacting their CCPA rights. Details of how a system might work are described below, but first I want to address a few misunderstandings in prior reply comments in the docket.

Reply comment misunderstandings of Do Not Track

I have tried to group comments by theme where possible to avoid duplication. Comments included below are from the California Cable & Telecommunications Association, California Chamber of

---

Companies should be required to honor global, platform-level requests to opt out of the sale of consumer data. Currently, browsers including Internet Explorer and Chrome give consumers the option to indicate their tracking preferences. Do Not Track signals from a California IP address could be interpreted as an opt out, or browsers could offer new signals to publishers to convey CCPA opt-out requests to all publishers."

[13] This could be as few times as once per device if set at the operating system level, as Windows and some mobile platforms do, or it could be once per web browser or other user agent if not set in the operating system. As the Internet of Things expands, one imagines set a household setting for all devices that connect to a "smart home" hub, with settings for the TV, refrigerator, coffee maker, etc. in one place. For this reason, it is best not to think exclusively as Do Not Track or other header systems as web browser-based. Rather, regulatory guidance for header signals should apply to everything using the HTTP protocol or similar (e.g. SPDY, which is an HTTP performance refinement.)

Commerce, California Retailers Association, CompTIA & TechNet, Interactive Advertising Bureau *et. al.*, Internet Association, and National Advertising Initiative.

My replies stem from knowledge gained by (1) working for Mozilla while Do Not Track was introduced into the Firefox web browser, which was the first large-scale deployment, (2) writing the Firefox help files that communicated what Do Not Track did and did not do, (3) co-chairing the W3C Tracking Protection Working Group, chartered to standardize Do Not Track, (4) early and continued academic research regarding Do Not Track in particular and privacy controls generally.

Comment area 1: Do Not Track and Do Not Sell are different but not incompatible

Of all objections, the one I find to have the most merit is that Do Not Track and Do Not Sell are different. This is correct. Do Not Track was created to allow users to have control around *data collection* rather than merely *data use*. Indeed, EFF's comment in support of connecting Do Not Track to CCPA reflects this history by calling for DNT:1 to be a "binding request to opt-out of data collection." Of possible data uses, sale is then only one of several data uses for which Do Not Track offers greater control.

Of course, data *not collected* is also necessarily data that *cannot be sold*. Where many commenters miss the mark is that while there are indeed differences between Do Not Track and Do Not Sell, selling is necessarily a subset of not collecting data. No data, no sale.

W216-4 (cont.)

Do Not Track entails a whole variety of limits on collection and use that are not covered by the narrow CCPA Do Not Sell. In other words, Do Not Sell is an incomplete subset of Do Not Track. It weakens Do Not Track to treat it as a *de facto* Do Not Sell. This does not harm Californians provided Do Not Sell is a floor, not a ceiling, for Do Not Track. It could be problematic if DNT:1 were taken to mean exactly and only CCPA Do Not Sell, not as a problem for CCPA implementations but rather for the (admittedly few) Do Not Track implementations in use today, as well as future Do Not Track uses regarding GDPR compliance. There are ways to address these concerns, but it will take some time and care to do so.

Treating a DNT:1 signal as a CCPA opt out of data sale (or a signal of being under age and not consenting to data sale) is fully aligned with users' expressed privacy interests, again because sale is a subset of Do Not Track, with collection a necessary precondition for sale. Therefore, comments like these are incorrect and/or miss the point:

- "Existing browser signals are not "opt-out of sale" signals." (California Chamber of Commerce)
- "It is problematic to treat tracking and selling as interchangeable terms because it weakens consumer control over personal information. … To require that user privacy controls be interpreted as Do Not Sell opt out requests takes that choice away from the consumer." (California Retailers Association)
- "A `Do Not Track' signal is not the same as a `do not sell' request." (Internet Association)
- "…`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." (National Advertising Initiative)

Early academic work on Do Not Track[14] found 79% of study participants expected Do Not Track to limit data collection. Of particular relevance, we asked about data use before and after clicking a fictitious Do Not Track button.

- 88% of participants believed data could not be shared with partners/affiliates even without Do Not Track
- 29% of participants believed data could not be shared with partners/affiliates with Do Not Track

Of note, the 29% who expected Do Not Track would fail to limit data sharing were not necessarily supportive of that outcome. 10% of participants independently raised issues in a free-form text box with concerns that companies' promises on the web are not trustworthy. Issues of cynicism and lack of trust aside, the majority of study participants expected Do Not Track would prohibit data sharing. Tying a CCPA opt out of sale to Do Not Track will not 100% meet users' expectations, but it is congruent with them, and there is no violation of user expectations to do so. To the contrary, Californians may be quite pleased to have their oft-ignored Do Not Track signals do more for them.

A user with a DNT:1 setting has requested an opt out of data collection. It necessarily follows that the user is opting out of data sale, since data not collected cannot be sold.

W216-4 (cont.)

Comment area 2: <u>Do Not Track is useful because it is device-specific, not user-specific</u>

One of the serious barriers for Californians using their Shine the Light law rights is that in many cases data collected about Californians is tied to unique identifiers in cookies, device identifiers, or browser fingerprinting techniques, none of which Californians have a practical way to extract. This is PII, but has no name attached (at least before it is "enriched" with other databases.) When Californians want to know what data a company has about them, they do not know how to form a request that gives companies the technical information needed to be able to properly identify what data is held. Californians do not even which technical techniques companies use to reidentify them. CCPA suffers the same challenges as Shine the Light in all of these regards.

Where Do Not Track excels is that users do not need to find a way to figure out how to describe their devices to the companies they contact. Whatever technology the companies already use for identification, that is fine. The DNT signal goes along with the company's choice, from cookies to device identifiers to fingerprinting or new approaches that might be used in the future. This way a company with, say, a broad set of information collected about a Californian's medical history for sale to insurance companies cannot say "sorry, we do not have names attached to our database, so we cannot respond to your CCPA opt-out." No names are required. The DNT signal is all that is needed. Companies can likewise respond to consumers without names or addresses – as one example, they already do so to show ads. Therefore, comments like these are incorrect and/or miss the point:

- "Under the Regulations as drafted, a business will not know how to reconcile a consumer's use of user-enabled privacy controls with a consumer's action or inaction vis-a-vis a `Do Not Sell' button. Further, a business has no way to contact a consumer in this scenario to

[14] McDonald, A. M., and Peha, J. M. Track Gap: Policy Implications of User Expectations for the 'Do Not Track' Internet Privacy Feature. *39th Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference)* September 25, 2011.

confirm that it contacted all third parties to which it sold data in the previous 90 days." (California Retailers Association)

- "…the business very well may not even know that the consumer exercised the opt-out, the identity of the consumer, or have any way of contacting him, as this is a browser-based control that may not be tied to any personally identifying information." (California Cable & Telecommunications Association)

Comment area 3: Rather than a header signal *OR* other opt outs, a header signal *AND* other opt outs

It is sometimes the case, as the California Cable & Telecommunications Association phrased it, that "…the business would be unable to implement an opt-out for the sale of the consumer's other personal information across other channels." Exactly. Do Not Track signals allow Californians to opt out of sales of data that are PII yet are not tied to their names *at that point in time*, which turns out to be a great deal of information. Meanwhile, opt outs via channels like phone, email, or physical mail necessarily do not have information about browser fingerprints. These channels can be responsive for cases where the company already has the Californian's name, address, or other information that the Californian actually knows.

W216-4 (cont.)

In order to have the ability to opt out of data sales, Californians need both sorts of mechanisms: those that identify devices, and those that identify people. Unfortunately, as we see in the next comments, several authors suggested making this "or" rather than "and."

- "We ask the OAG to eliminate the requirement to honor browser plugins or privacy settings or mechanisms, or, alternatively, revise the draft rules so that businesses have the option of honoring such settings or providing a "Do Not Sell My Personal Information" link along with another method for consumers to opt out of the sale of personal information by the business." (Interactive Advertising Bureau)
- "A business should be able to accept the browser-enabled method or provide the 'Opt-Out Button'…" (California Chamber of Commerce)

An either/or approach necessarily means Californians will have CCPA rights to opt out of data sale, but no mechanism with which to opt out. The Attorney General's office should adopt a requirement for (a) a method to opt out of data sale that identifies people (e.g. via phone, email, mail) AND (b) a method to opt out of data sale that identifies devices (e.g. a header signal.)

Choices should be in the hands of Californians: to opt to let parties sell their data or not. It is not reasonable to let companies choose which opt outs to ignore. To decide to allow companies to effectively ignore EITHER requests to opt out of sale of data that identifies people OR to ignore opt out of sale of data that identifies devices is to erode the very rights CCPA was authored to protect. An either/or approach here would necessarily leave Californian's data very much for sale with no path to opt out of sales, and therefore cannot be the Attorney General's decision.

RECOMMENDED: section 999.315(a) should end as "Other acceptable methods for submitting these requests include… a form submitted in person, **or** a form submitted through the mail."

A new section to follow of 999.315(b) should then have a **requirement** to respond to user-enabled global privacy controls. The content of that requirement may be improved, with further discussion in the subsequent section. At present, it may be most useful to add the requirement as well as a timeline for future work.

Comment area 4: Do Not Track is useful because it communicates broadly
Comment area 5: Do Not Track is not necessarily all or nothing

These two comment areas are intertwined. In brief, some authors were unhappy with the idea of a signal that reaches all parties who collect data. Header signals are a powerful tool for user empowerment while expressing opt outs to multiple parties. This is a positive feature, not a problem, despite comments like:

> "…browser-based signals or plugjns would broadcast a single signal to all businesses opting a consumer out from the entire data marketplace." (Interactive Advertising Bureau)

W216-4 (cont.)

Authors also misrepresent that Do Not Track is monolithic, e.g.

- "Indeed, it becomes an all-or-nothing approach." (California Retailers Association)
- "It is not possible through these settings for a consumer to make discrete choices among businesses allowing the consumer to restrict certain businesses while permitting other businesses to transfer data to benefit the consumer." (Interactive Advertising Bureau)

On the contrary, Do Not Track was designed with mechanisms for users to grant specific permissions (either to consent or withdraw consent) that override a global setting. Current CCPA proposals do not include these protocols. I believe they should, but with an eye to simplification from the W3C texts. There may also need to be adjustments due to CCPA being a law, not a standard. This will take a short additional time to accomplish.

Comment area 6: CCPA is not a voluntary standard

Do Not Track was designed for voluntary adoption by companies. It was not a legislative requirement to facilitate privacy rights, as is CCPA. As one consequence of this difference, many decisions that were flatly bad for user privacy were accepted as compromises in Do Not Track standards. This makes sense: voluntary industry adoption would not happen otherwise. What surprises me is to see such areas of negotiation in W3C reappear in the CCPA context as if they were somehow decisions the Attorney General's Office must follow – or even take notice of. There is no need for the AG's office to wade into the morass of trying to understand when a header signal is set directly by a user, or set indirectly because the user chose to use the software that sent the signal, and then whether that makes the signal less or even more valid.[15]

[15] If the AG's office has the authority to tell user agents how they may structure their header signal consent process in order to have a valid CCPA signal, surely the AG's office also has the authority – and the responsibility – to compel all user agents have the readily-usable capacity to send opt out header signals for California customers. Professor Eric Goldman's comments calling for a certification process, presumably from the AGO not the DOJ, could have merit

Some authors appear to think the very notion of user choices for privacy opt outs are also up for negotiation, as if CCPA were a standard to thwart, not a law to uphold. For example, from CompTIA and TechNet:

> "…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."

In their text CompTIA and TechNet envision a user's own choice to opt-out, yet propose it still will not count, and they want the Attorney General to require Californians' privacy choices be ignored. How many times must a Californian opt out in order to actually opt out? Ignoring user choices is not a reasonable regulatory approach.

A path forward

All of this said, there are other elements of the transition from voluntary standard to law that give me pause. One does not simply hook up CCPA to DNT:1 without some unintended consequences. For this reason, I suggest a **brief extension prior to header signal regulations**. I suggest first settling the details of the button and other regulations, then turning to Do Not Track after. An additional two months should be adequate for design and drafting, with a brief comment and response period after, with comments limited just to the topic of how best to implement a required header signal. The goal is to improve outcomes, not continually delay.

W216-4 (cont.)

Where Do Not Track struggled was with what CCPA decided: details of compliance. What Do Not Track accomplished is a great deal of technical infrastructure work already well thought out. For example, CCPA could benefit not just from companies accepting an incoming Do Not Track signal, but also from the Do Not Track protocols for companies to send back an acknowledgement. CCPA could leverage this prior work very well. Thus far, the proposals for a header with CCPA do not get into the level of detail needed for usable implementations, which could hinder companies (regulatory and technical uncertainty,) and Californians (maze of controls, all different,) alike. Putting these halves together to form a coherent whole is not so difficult a task, but there would be useful editing work to reflect updates based upon CCPA details.

I also suggest offering sample implementations with freely available source code in order to reduce compliance burden on small companies. While companies have the latitude to implement as meets CCPA requirements, in many cases a custom solution is not necessary. Having an AG-approved sample code offering would be a great way to support fast implementations.

Work to align a header signal with GDPR is ongoing.[16] It is possible to extend DNT to apply to regulatory frameworks in different countries, even with differing opt-in and opt-out approaches. One of the reasons for spending a little more time to think through the fine details is because a step forward for California privacy rights could inadvertently harm European privacy rights. It is viable

provided such controls are required offerings from user agents including web browsers and others, covering all technologies that send HTTP or similar requests (e.g. HTTPS, SPDY, etc.) from Californians.

[16] One example: Zuiderveen Borgesius, F. J., and McDonald, A. M. (2015). Do Not Track for Europe. *43rd Research Conference on Communication, Information and Internet Policy (Telecommunications Policy Research Conference)* September 26, 2015.

to support both approaches in tandem, without requiring a high burden on companies to maintain two entirely different technical implementations, but it does take some careful thought.

W216-4 (cont.)

Topic 4: Implementation details

In this comment I have recommended ways to support Californians' abilities to use their new CCPA rights in practice. Not all of these recommendations are best suited for regulations, and not all of them are best suited to move forward today. While there is great latitude established in 1798.185(a)(4)(A) ("…the Attorney General shall… establish rules and procedures… to facilitate and govern the submission of a request by a consumer to opt-out of the sale…") there may be instances where it is initially better to issue Safe Harbor examples or best practices, especially while working out the details for edge cases.

Please do not mistake this as a suggestion to delay broad enforcement. Californians have waited a long time for privacy rights, as guaranteed by our California Constitution. The tension is that for user-facing elements, there is one chance for a first impression. If privacy controls go out with usability flaws, CCPA may not be given a second chance. This is why I again repeat my call for usability testing in advance for privacy controls, as has been required in other privacy domains.[17]

Similarly, I suggest a round of feedback on using a header signal like Do Not Track with CCPA, specifically to uncover any novel implementation issues. The header signal should be adopted; I encourage that as a regulatory decision now. Certain types of CCPA-protected information will not be able to be addressed and citizens will not be able to out of sale of some of their data without a header signal or similar technical approach. However, the details of how best to adopt header signals legitimately do benefit from broader industry discussion. Small differences in technological implementations can mean big differences for user privacy, and can be substantially easier or harder for companies to implement. While Attorney General's legislatively-required priority is necessarily to enact a privacy law that allows citizens to make privacy choices in effective ways, reducing cost and implementation complexity for organizations in ways that do not impinge privacy rights is also a very worthy goal.

Neither of these suggestions imagines a long time horizon. These tasks can be done in weeks to months, not years. Much work is already done in both cases. I look forward to your upcoming decisions and additional future discussions.

[17] An example is the "Schumer box" for financial disclosures, which was sadly found to be incomprehensible only after it was widely deployed. It has since been redesigned and tested with greater success. However, redesign was so late that citizens may well ignore the information due to prior bad experiences.

From: Halpert, Jim
To: Privacy Regulations
Cc: Hurley, Megan
Subject: 2nd Round Comments of the State Privacy & Security Coalition
Date: Tuesday, February 25, 2020 4:47:39 PM
Attachments: StatePrivacy&SecurityCoalitionCCPARegs2comments.docx

Thank you very much for this opportunity to comment and for considering these comments.

Sincerely – Jim Halpert

Jim Halpert
Partner, co-Chair Global Data Protection, Privacy and Security Practice

T [redacted]
F +1 202.799.5441
M [redacted]
E [redacted]

DLA PIPER

DLA Piper LLP (US)
500 Eighth Street, NW
Washington, DC 20004
United States
www.dlapiper.com [dlapiper.com]

State Privacy and Security Coalition, Inc.

COMMENTS TO THE ATTORNEY GENERAL

February 25, 2020

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 Revised Proposed Text of Regulations

I. Introduction

The State Privacy & Security Coalition is a coalition of 30 companies and 8 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 other 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 appreciate that the revised draft Regulations address and resolve a number of the outstanding confusing features of the law. We focus these comments only on clarifications to new proposals in the revised proposed rules, with the exception of the "do not sell" signal component, which we urge the Attorney General's Office to suspend pending resolution of the California Privacy Rights Act Initiative ("CPRA"), No. 19-0021, filed Nov. 13, 2019. W217-1

As we noted in our opening comments, the CCPA has already been amended and changed twice. The rules will change CCPA requirements *a third time* (after two drafts).

If approved by the voters in 2020 (as appears likely), 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. We urge your office to give weight to this concern as it finalizes its CCPA rules.

500 8th Street, NW
Washington, DC 20004
202.799.4000 Tel
202.799.5000 Fax

II. AG's Office should not issue rules, such as the Do Not Sell Signals Rules, that differ from both the statute and CPRA

By way of example, the proposed "do not sell" signal or browser or device settings are mentioned nowhere in the CCPA, including in Civ. Code § 1798.185(a)(4), which authorizes an AG rulemaking on the do not sell icon, but not on a technical setting expressing a do not sell request.

But leaving aside the question of whether the Attorney General's Office has the statutory authority on this issue, moving forward *at this juncture* with a rule on this question is unwise public policy because the CPRA would address the issue very specifically. If the CPRA is approved, it would establish different requirements regarding providing consumers with the ability to opt out of selling or sharing personal information. Honoring an opt-out preference is one of the options provided, and including the required hyperlink to limit sharing of personal information and secondary use of sensitive personal information is another compliance option. What is more, websites would be able to present on a landing page reasons why the Internet user should agree to a CCPA data "sale." CPRA, § 1798.135(b)(2). The 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. This is a more nuanced approach than the one in the proposed rule, and one that is arguably more narrowly tailored for purposes of a challenge in a 1st Amendment action that may be brought by smaller Internet advertising firms that lose access to personal information under a "do not sell" technical settings system in which individuals are not making case-by-case choices about use of their personal information.

W217-1 (cont.)

The AG's Office will know in a matter of months whether the CPRA Initiative has enough valid signatures to appear on the November 2020 ballot, and in November 2020, whether the CPRA has been approved by the voters. It would be far more sensible to defer consideration of this aspect of the proposed rules until after the outcome of the CPRA is known.

It would be needlessly confusing to issue a do not sell rule that would change significantly three years later. This aspect of the proposed rules would serve no purpose because the new agency is called upon to issue these rules in 2023. The proposed rule contains no process at all for clarifying the system and how it would be implemented technically. Because there is no such signal today, these questions are very important. The CPRA requires two further rulemakings to develop real rules on this issue, then time for the development of a technical standard, and then deployment of technology to make the privacy control effective. Because it would take time for the technical signal mentioned in the proposed rule to be implemented, there is no interest in rushing to finalize this aspect of the proposed rules. The far wiser course is to hold this aspect of the rule in abeyance until November 2020, once the outcome of the CPRA Initiative is known.

500 8th Street, NW
Washington, DC 20004
202.799.4000 Tel
202.799.5000 Fax

III. The Final Rules Should Restore the Risk Exception in § 999.313(c)(3) from Disclosing Specific Pieces of Personal Information where there is "a Substantial, Articulable, and Unreasonable Risk to the Security of that Personal Information"

The latest version of the proposed rules would strike a critical fraud exception in the previous version of § 999.313(c)(3) against disclosing specific pieces of personal information where there is a substantial, articulable and unreasonable risk to the security of that personal information. This exception should be restored in the final rules.

W217-2

The exception was tightly drafted and addressed the very real risk of "pretexting" requests for personal information. This risk is heightened because other parts of the proposed rules would allow third party authorized agents to obtain access to and delete personal information of individuals. In this environment, fraudsters and even foreign intelligence services may attempt to abuse the CCPA access right to obtain personal information about California residents. If they are sophisticated, they may well be able to phish or otherwise obtain the requisite number of verifying data elements and falsify an authorization request.

For these reasons, it is very important that this exception be restored in order to avoid undermining the privacy of Californians' personal information in ways that can be very damaging.

IV. The Clarification in § 999.302 Regarding the Status of IP Addresses Is Helpful But Should Be Clarified Further to Address the Status of Deidentified Data and Aggregate Data

The guidance inserted in new § 999.302 regarding the status of IP addresses is generally helpful, but is incomplete and not yet accurate because it does not account for IP addresses that are de-identified or aggregated and thereby fall outside the definition of "personal information."

W217-3

The Civ. Code § 1798.140(o)(2) was amended in 2019 to clarify that: "'Personal information' does not include consumer information that is deidentified or aggregate consumer information." This clarification should be reflected in § 999.302 by inserting the following text in revision marks:

> (a) Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "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," in aggregate form, or in de-identified form with safeguards so that "they cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer." For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, ~~and could not reasonably link the~~

500 8th Street, NW
Washington, DC 20004
202.799.4000 Tel
202.799.5000 Fax

~~IP address with a particular consumer or household,~~ then the IP address would not be "personal information."

These revisions would accurately reflect the de-identification and aggregate data definitions and avoid needless confusion.

W217-3 (cont.)

V. The Proposal in § 999.305(a)(3)(a) to require links to "at or before collection" notices "on all webpages where personal information is collected" Should be Revised

This subparagraph changes from an "or" to an "and" the requirements to provide a conspicuous link to the "at collection" notice "on the introductory page of the business's website *and* on all webpages where personal information is collected notice." This language is inconsistent with the statute, which requires notice "at *or* before collection", not "at *and* before."

W217-4

It is true that, in a drafting error, the definition of "homepage" includes "any Internet web page where personal information is collected." § 1798.140(l). However, this is highly counter-intuitive and contradicts the statutory obligation to provide notice either at or before the point of collection. For this reason, as in the previous version of this proposed rule, the final rules should state that link may be placed on the home page *or* at each point of collection.

This change would both align with common understanding of the term "home page" and would be less likely to make consumers tune out by seeing the same link on every web page.

VI. The Clarifications to Service Provider Uses of Personal Data in § 999.314(c) Align the Provision with Statute, But the Reference to "Cleaning and Augmenting Data" Does Not and Is Unclear

The CCPA expressly allows service providers to use personal data "for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title." § 1798.140(v). This text fully supports the changes to § 999.314(c).

W217-5

However, the reference to "cleaning" and augmenting other data is undefined and unclear and should be either removed or clarified by adding at the end "unless performed as part the services specified in the written contract". This clarification is important to avoid confusion as to whether service providers do not lose their status as service providers if they are engaged to and perform analytics functions while acting in a service provider role.

VII. The Requirement in § 999.305(a)(5) to Obtain Opt-in Consent for Specific Data Uses Is Inconsistent with the Statute.

W217-6

500 8th Street, NW
Washington, DC 20004
202.799.4000 Tel
202.799.5000 Fax

We appreciate that the explicit consent requirement in this section has been cabined somewhat through a "materially different" standard. However, the requirement that an entity must "directly notify" and "obtain explicit consent" from consumers in order to use a consumer's personal information for a purpose materially different than what was disclosed in the notice at the time of collection goes beyond the scope of what the underlying statute provides. Civ. Code §1798.100 (b) clearly states that use of collected personal information for additional purposes should be subject to further *notice* requirements only.

W217-6 (cont.)

The drafters of the CCPA required the further step of obtaining explicit consent from a consumer only for the sale of a minor consumer's personal information,[1] participation in an entity's financial incentive program,[2] and retention of a consumer's personal information for the purposes of peer-reviewed scientific, historical, or statistical research in the public interest.[3]

Requiring explicit consent beyond these well-defined and clearly cabined use cases in the statute is contrary to the text of the CCPA.

VIII. The New Requirement in § 999.323(d) Preventing Businesses from Charging Consumers for Identity Verification Should be Clarified.

The new requirement in § 999.323(d) that businesses not charge consumers for proper identity verification should be clarified to make clear that *authorized agents* can be charged for identity verification, including powers of attorney, which are specifically envisioned by § 999.326(b) and require notarization. Experience thus far with CCPA requests suggests that entities are building for-profit authorized agent businesses. They can afford identity verification. At the same time, there is risk that fraudsters may pose as authorized agents and obtain access to specific pieces of personal information or delete accounts. It makes sense as a matter of public policy to require that authorized agents verify the identity and legitimacy of their business, as well as their authority to act on behalf of the consumers they are purporting to represent. At least as to access to specific pieces of personal information and data deletion, § 999.323(d) should be clarified specifically to allow this in order to reduce potential risk to Californians' privacy.

W217-7

The same risk applies to fraudsters who pose as a California consumer. In this context, the final rules should also clarify that while a business should not require that consumers pay for a new power of attorney, it may require consumers that already have a power of attorney submit it.

Respectfully submitted,

Alan F. Hoyt

[1] § 1798.120(d).
[2] § 1798.125(b)(3).
[3] § 1798.105(d)(6).

500 8th Street, NW
Washington, DC 20004
202.799.4000 Tel
202.799.5000 Fax

Jim Halpert, Counsel
State Privacy & Security Coalition

500 8th Street, NW
Washington, DC 20004
202.799.4000 Tel
202.799.5000 Fax

From: John Kabateck
To: Privacy Regulations
Subject: Public Comment Letter re: CCPA - Small Business Data Privacy Committee
Date: Tuesday, February 25, 2020 4:46:53 PM
Attachments: SB_Data_Privacy_Comments_AG.docx

ATTN: Lisa B. Kim, Privacy Regulations Coordinator, California Office of the Attorney General

Attached please find the public comment letter submitted on behalf of the Small Business Data Privacy Committee, submitted as follow-up to the original public comment letter submitted by this Committee on December 6, 2019, concerning the draft California Consumer Privacy Act (CCPA) regulations issued by the California Office of the Attorney General. This letter is signed by seven of the leading small and small ethnic business organizations from across California.

Thank you and the Attorney General for your consideration of these comments during your process of evaluating these regulations. If you should have any questions feel free to contact me at [redacted] or at [redacted]

John Kabateck
California State Director
National Federation of Independent Business

--

John Kabateck
President, Kabateck Strategies
[redacted]
www.kabstrat.com
[redacted]

February 25, 2020

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

To Whom It May Concern:

On behalf of the Small Business Data Privacy Committee, we appreciate the progress made in the Revised Proposed Regulations for the California Consumer Privacy Act (CCPA). We request that you address our continuing concerns regarding the cost of compliance, confusion about definitions and requirements, and the expansive reach of the proposed regulations. We support the effort to protect consumer privacy, however, that goal cannot be achieved if the rules and regulations are too complex to understand and too hard to implement. With the law in effect and enforcement fewer than six months away, business owners are still struggling to appropriately allocate resources and establish efficient processes to ensure compliance. We join other business organizations in requesting that you delay enforcement until January 1, 2021.

At a time when small business is struggling to absorb minimum wage cost increases, changes in the independent contractor laws, and increased energy and business costs, we strongly reiterate our concern about the CCPA compliance costs. The economic impact assessment of the CCPA prepared for your office estimates an initial compliance cost of $55 billion dollars, with an estimated cost of $50,000 for small business. This is much more than many small and medium size businesses can reasonably afford. Small business does not have the resources to hire law firms and consultants and to invest in new technology systems.

In our initial comments, we raised concerns that the regulations require business to comply with requirements that were not authorized in the CCPA. While some of those concerns have been resolved in the Revised Regulations, the California Chamber of Commerce has provided a detailed summary of issues that have not been resolved. In addition, we are particularly concerned about the following issues:

- The Revised Regulations require business to calculate the value of consumer data. We are unclear how we would value data in order to respond to consumers nor do we have the resources to invest in the process of determining the value of data. W218-1
- The Revised Regulations failed to provide enough direction around the establishment of an opt-out policy. Small and medium-size businesses subject to the CCPA need more clarification of the opt-out and opt-in requirements in order to present consumers with a legally sufficient and effective means of establishing their privacy preference. W218-2
- The Revised Regulations fail to ensure that digital advertising will remain a means of reaching small business customers. Small and medium-size businesses are not interested in accumulating personal information, but we need a functioning internet to compete with larger businesses.

We respectfully recommend that your office consider the complexity of this area and the fact that the CCPA is a major new government program that will require small business to invest time and resources into compliance. As your office finalizes the regulations, please consider the need to make these regulations affordable to implement, easy to understand, and measured in scope.

Sincerely,

Coalition members:

California Asian Pacific Chamber of Commerce
California Hispanic Chambers of Commerce
California Small Business Association
National Federation of Independent Business, CA
Valley Industry & Commerce Association
Los Angeles County Business Federation (BizFed)
Latin Business Association

15-DAY COMMENT
W219

From: Maureen Mahoney
To: Privacy Regulations
Subject: CR Comments on Updated Proposed CCPA Rules
Date: Tuesday, February 25, 2020 4:37:14 PM
Attachments: CR CCPA Comments 2.25.20 FINAL.pdf

Dear Ms. Kim,

Attached, please see Consumer Reports' comments on the updated proposed rules to implement the California Consumer Privacy Act.

Please let me know if you have any questions.

Best,
Maureen

--
Maureen Mahoney
Policy Analyst
o [redacted]

CR.org CR.org/advocacy

February 25, 2020

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

Re: Modified Proposed Rules Implementing the California Consumer Privacy Act (CCPA)

Consumer Reports[1] thanks the California Attorney General's office (AG) for the opportunity to comment on its proposed changes to rules implementing the California Consumer Privacy Act (CCPA).[2] The landmark CCPA gives California consumers, for the first time, the ability to access, delete, and stop the sale of their personal information. Californians finally have a real opportunity to exercise their constitutional right to privacy. But tech companies have been able to avoid meaningful regulations for decades, and their behavior suggests that they're not going to let the CCPA get in the way of their sale of consumers' personal information.

It's up to the AG to hold companies accountable, especially as many of them have willfully ignored the CCPA since it went into effect in January.[3] Making matters worse, several of the changes to the draft rules proposed by the AG take a significant step back from the draft released in October. Most concerning, the updated rules exempt IP addresses from the definition of personal information—an unacceptable change that would dramatically weaken the existing statute. To protect consumers, we urge the AG to:

[1] Consumer Reports is an expert, independent, non-profit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. Consumers Reports works for pro-consumer policies in the areas of financial services and marketplace practices, antitrust and competition policy, privacy and data security, food and product safety, telecommunications and technology, travel, and other consumer issues, in Washington, DC, in the states, and in the marketplace. Consumer Reports is the world's largest independent product-testing organization, using its dozens of labs, auto test center, and survey research department to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

[2] California Attorney General, California Consumer Privacy Act Regulations, Text of Modified Regulations (Feb. 10, 2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-redline-020720.pdf [hereinafter CCPA Modified Regulations].

[3] Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs to Act* (Jan. 9, 2020), https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb.

- **Clarify that sharing for cross-context targeted advertising falls under the definition of sale;**
- **Tighten the service provider exemption;**
- **Remove the new limits on the definition of personal information, which would create a significant loophole for targeted advertising;**
- **Make global, browser opt-outs more user-friendly;**
- **Clarify that financial incentives in markets that lack competition is an unfair and usurious practice;**
- **Require companies to forward opt-out requests to third-party recipients of data where possible; and**
- **Consider a retention limit on records of deletion.**

More information continues to become known about the extent to which consumers' personal information—collected not only online, but through their phone handsets, apps, televisions, and smart devices—is bought and sold without their knowledge,[4] and the lengths to which companies will go to avoid complying with even baseline privacy protections. The AG needs to take swift action to ensure that consumers are able to exercise their privacy rights.

The AG should clarify that sharing for cross-context targeted advertising falls under the definition of sale.

Many tech companies are doing everything they can to avoid complying with consumer's explicit requests to opt-out of the sale of their information. Even though companies had ample time to prepare to comply with the new law, they are now actively looking for loopholes, and some are ignoring the CCPA altogether. For example, the Interactive Advertising Bureau (IAB), a trade group that represents the ad tech industry, developed a framework for companies to evade the opt-out by abusing a provision in the CCPA meant to permit a company to perform certain limited services on its behalf.[5] Google announced that it will follow IAB's lead,[6] and Facebook has announced that its "like" buttons, which allow the company to track users' behavior across the web—even if they are not logged in—is outside of the consumer opt-out clause.[7] Grindr, for

[4] *Out of Control: How Consumers Are Exploited by the Online Advertising Industry*, NORWEGIAN CONSUMERS COUNCIL (Jan. 14, 2020), https://fil.forbrukerradet no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf [hereinafter OUT OF CONTROL].

[5] *IAB CCPA Compliance Framework for Publishers & Technology Companies*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2019), https://www.iab.com/wp-content/uploads/2019/12/IAB_CCPA-Compliance-Framework-for-Publishers-Technology-Companies.pdf [hereinafter *IAB Framework*].

[6] Allison Schiff, *Google Will Integrate With IAB Tech Lab's CCPA Compliance Specs By Jan. 1 Deadline*, ADEXCHANGER (Dec. 4, 2020), https://www.adexchanger.com/privacy/google-will-integrate-with-iab-tech-labs-ccpa-compliance-specs-by-jan-1-deadline/; Google, Helping Advertisers Comply with CCPA in Google Ads (last visited Feb. 23, 2020), https://support.google.com/google-ads/answer/9614122.

[7] Patience Haggin, *Facebook Won't Change Web Tracking in Response to California Privacy Law*, WALL ST. J. (Dec. 12, 2019), https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175345 [hereinafter *Facebook Won't Change Web Tracking*].

example, seeks to ignore "do not sell" instructions by claiming that consumers have assented to sale in long-form contracts they almost certainly have never read.[8]

The AG has the opportunity to provide further clarity on this issue, much of which hinges on the definition of sale and the regulations around service providers. With respect to sale, some incorrectly claim that because money isn't necessarily exchanged for data, then data transfers for targeted advertising purposes aren't a sale—therefore, consumers don't have the right to opt-out.[9] For example, retailers may send adtech platforms both money and data collected about consumers to target ads on multiple sites. But addressing targeted advertising is one of the main goals of the CCPA, which has an inclusive definition of personal information and a broad definition of sale to cover transfers of data for these purposes.[10]

To help address any potential loopholes, the AG should exercise its broad authority to issue rules to further the privacy intent of the Act,[11] and clarify that the transfer of data between unrelated companies for any commercial purpose falls under the definition of sale. This will help ensure that consumers can opt-out of cross-context targeted advertising. We suggest adding a new definition to § 999.301:

W219-1

> "Sale" means sharing, 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, or otherwise for a commercial purpose.

While we appreciate that the AG has attempted to address instances of non-compliance with the opt-out button requirement by adding a provision to limit companies to "minimal steps to allow the consumer to opt-out[,]"[12] that won't be enough to stop these companies. It is true that one of the characteristics of IAB's framework for "compliance" with the CCPA is that consumers are directed to multiple sites to opt-out (IAB purports to send consumers to existing failed self-regulatory mechanisms to exercise choices about targeted advertising).[13] But the fundamental problem is that companies argue that most commercial data transfers aren't a sale, so that they

[8] Natasha Singer and Aaron Krolik, *Grindr and OkCupid Spread Personal Details, Study Says*, N.Y. TIMES (Jan. 13, 2020), https://www nytimes.com/2020/01/13/technology/grindr-apps-dating-data-tracking.html.

[9] Tim Peterson, *'We're Not Going to Play Around': Ad Industry Grapples With California's Ambiguous Privacy Law*, DIGIDAY (Dec. 9, 2019), https://digiday.com/marketing/not-going-play-around-ad-industry-grapples-californias-ambiguous-privacy-law/.

[10] Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley—And Won*, N.Y. TIMES (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data html; Cal. Civ. Code § 1798.140(o); Cal. Civ. Code § 1798.140(t).

[11] Cal. Civ. Code § 1798.185(a).

[12] CCPA Modified Regulations, *supra* note 2, at § 999.315.

[13] *IAB Framework*, *supra* note 5, at (III)(2)(d)(ii).

don't have to put up the opt-out button or comply with consumer requests. This issue needs to be decisively addressed. W219-1 (cont.)

The AG should tighten the service provider exemption to stop inappropriate data sharing in spite of an opt-out.

To address a second loophole that the IAB has exploited, the AG should clarify that when the consumer has opted out of the sale of their information, data cannot be shared—even with a service provider—to target advertising on another site or service. The AG's new § 999.314(d), stating that "A service provider shall not sell data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business" is an improvement on the previous draft rules, which were silent on the issue. Nevertheless, the language should be tightened, especially since some incorrectly claim that the data-sharing engaged in for targeted advertising purposes is not a sale.[14] We suggest a new § 999.314(d): W219-2

> If a consumer has opted out of the sale of their data, a company shall not share personal data with a service provider for the purpose of delivering cross-context behavioral advertising. "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

Second, the AG should take action to stop companies from combining data across clients. Service providers should be working on behalf of one company at a time. Allowing companies to claim that they're just service providers for everyone swallows the rules and lets third parties amass huge, cross-site data sets. To help address this problem, the AG has appropriately removed language in § 999.314(c) of the previous draft, which held that service providers can merge data across clients. But in the absence of a specific prohibition, given its disregard for the FTC consent order, Facebook (and other companies) will likely continue to engage in this behavior. The AG needs to make clear that this is not acceptable. We suggest the following language: W219-3

> A service provider may not combine the personal information which the service provider receives from or on behalf of the business with personal information which the service provider receives from or on behalf of another person or persons, or collects from its own interaction with consumers.

[14] *IAB Framework*, *supra* note 5, at (II)(3).

Online ad tech companies—including Facebook and Google—are the modern data brokers. As Berkeley professor Chris Hoofnagle explains, Google and Facebook provide app developers privileged, valuable information—your data—in return for services that help increase engagement with their platforms.[15] The AG should refine the draft regulations in order to give consumers more control over their data with respect to these practices.

W219-3
(cont.)

A history of non-compliance

Consumers who dislike ad tracking and targeted advertising will be frustrated if sending CCPA "Do Not Sell" instructions has no practical effect. Consumers in Europe have already experienced this following widespread noncompliance with GDPR as websites force consumers through coercive consent dialogs to justify perpetuating existing data practices.[16] Complaints about tracking abuses have been filed with European regulators.[17] And the Information Commissioner's Office (ICO), which is the UK GDPR regulator, has declared industry real-time bidding (RTB) behaviors—when publishers auction off a space to advertisers, based on your past internet activity, in a fraction of a second—to be violative of GDPR.[18] So far, regulators have yet to take real enforcement action.[19] The AG shouldn't make the same mistake that European regulators have made.

Ad tech companies have a long history of evading regulation. In 2012, industry representatives committed to honoring Do Not Track instructions at a White House privacy event.[20] Over the next few years, however, as regulatory pressure and the prospect of new legislation faded, industry backed away from its commitment, with trade groups publicly announcing withdrawal from the industry standard process at the World Wide Web Consortium.[21] Instead, they set up

[15] Chris Hoofnagle, *Facebook and Google Are the New Data Brokers* (Dec. 2018), https://hoofnagle.berkeley.edu/wp-content/uploads/2018/12/hoofnagle_facebook_google_data_brokers.pdf.
[16] Kate Fazzini, *Europe's Sweeping Privacy Rule Was Supposed to Change the Internet, but So Far It's Mostly Created Frustration for Users, Companies, and Regulators*, CNBC (May 5, 2019), https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html.
[17] Steven Melendez, *How Google Is Breaking EU Privacy Law, According to a New Complaint*, FAST COMPANY (Sept. 13, 2018), (https://www.fastcompany.com/90236273/google-faces-gdpr-privacy-complaint-over-its-targeted-ads-from-brave-browser; Natasha Lomas, *Google and IAB Ad Category Lists Show 'Massive Leakage of Highly Intimate Data,' GDPR Complaint Claims* (Jan. 27, 2019), TECHCRUNCH, https://techcrunch.com/2019/01/27/google-and-iab-ad-category-lists-show-massive-leakage-of-highly-intimate-data-gdpr-complaint-claims/.
[18] Update Report Into Adtech and Real Time Bidding, INFORMATION COMMISSIONER'S OFFICE (Jun. 20, 2019), https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.
[19] Simon McDougall, *Blog: Adtech - The Reform of Real Time Bidding Has Started and Will Continue*, ICO (Jan. 17, 2020), https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-the-reform-of-real-time-bidding-has-started/.
[20] Dawn Chmieleski, *How 'Do Not Track' Ended Up Going Nowhere*, RECODE (Jan. 4, 2016), https://www.vox.com/2016/1/4/11588418/how-do-not-track-ended-up-going-nowhere; *see* Julia Angwin, *Web Firms to Adopt 'No Track' Button*, WALL ST. J. (Feb. 23, 2012), https://www.wsj.com/articles/SB10001424052970203960804577239774264364692.
[21] Kate Kaye, *Do-Not-Track on The Ropes as Ad Industry Ditches W3C*, ADAGE (Sept. 17, 2013), http://adage.com/article/privacy-and-regulation/ad-industry-ditches-track-group/244200/.

their own voluntary "Ad Choices" system to allow consumers to opt-out of interest-based advertising. But industry efforts to self-regulate have largely failed. The rules only apply to coalition members; industry opt-outs are fragile and easily overridden; industry opt-outs only address usage and do not impose meaningful collection or retention limitations; and notice and privacy interfaces were seriously flawed.[22]

Companies have also pushed back against the CCPA. Last year, the tech industry worked to remove CCPA controls over third-party targeted advertising by supporting SB 753, which would have completely exempted cross-context targeted advertising from the opt-out.[23] More recently, advertising groups have asked the AG to delay enforcement of the law—even though they've had over a year to get into compliance.[24] Other states, under pressure from the tech industry, have pursued opt-out bills with a much more limited definition of sale.[25] The AG should not let companies continue to try to evade meaningful regulation.

Impact on consumers

Over time, behavioral advertising has become increasingly invasive. Sites are able to track every move a consumer makes online, including search history and search terms.[26] Apps, too, track and sell consumers' most sensitive data. Recent research from Consumer Reports revealed that so-called health apps such as period trackers collect information not only about how often you menstruate, but whether you're trying to have a baby, and even how often you have sex. Unless Californians opt out of the sale of their information—and the companies involved honor the opt-out—that information could find its way to third parties, and could be further sold or otherwise disseminated in ways that could mean getting charged more for insurance, or even facing job discrimination.[27] This information is often widely traded as a matter of course. Another recent study found that 10 apps together sent personal information on consumers to at least 135 companies involved in advertising and behavioral profiling.[28]

---

[22] *Statement of Justin Brookman Before the U.S. Senate Comm. On Commerce, Sci., and Transp.*, CTR. FOR DEMOCRACY & TECH. (Apr. 24, 2013), https://cdt.org/files/pdfs/Brookman-DNT-Testimony.pdf.
[23] *California Consumer Privacy Act Update: Assembly Approves 12 Amendments - Changes Would Exclude Employees and Vehicle Information, Protect Loyalty Programs*, JD SUPRA (Jun. 7, 2019), https://www.jdsupra.com/legalnews/california-consumer-privacy-act-update-48943/.
[24] Andrew Blustein, Ad Industry Calls for Delayed Enforcement of CCPA, THE DRUM (Jan. 29, 2020), https://www.thedrum.com/news/2020/01/29/ad-industry-calls-delayed-enforcement-ccpa.
[25] See, e.g., Nevada SB 220 (2019), https://www.leg.state nv.us/App/NELIS/REL/80th2019/Bill/6365/Text; Arizona HB 2729 (2020), https://apps.azleg.gov/BillStatus/BillOverview/73672.
[26] Glenn Fleischman, *How The Tragic Death of Do Not Track Ruined the Web for Everyone*, FAST COMPANY (Mar. 19, 2019), https://www fastcompany.com/90308068/how-the-tragic-death-of-do-not-track-ruined-the-web-for-everyone [hereinafter *The Tragic Death of Do Not Track*].
[27] Donna Rosato, *What Your Period Tracker App Knows About You*, CONSUMER REPORTS (Jan. 28, 2020), https://www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you/.
[28] OUT OF CONTROL, *supra* note 4, at 5.

Consumers are actively engaged online, spending around six hours per a day using digital media, mostly on mobile devices.[29] While some consumers may well appreciate receiving targeted offers, in study after study, the majority of people do not wish to be tracked in order to be served with more relevant advertising.[30] In a recent Pew Research study, 86% of users reported taking some action to mask their digital footprints, but most wish they had the ability to do more.[31] Older, less tech-savvy users especially feel powerless to take responsibility for protecting their privacy.[32] Most people just don't want their personal information sold to countless strangers without their knowledge,[33] and at the very least companies should be required to honor affirmative efforts to opt out of the ad tech ecosystem.

The AG should remove the limits on the definition of personal information, which would create a significant loophole for targeted advertising.

The AG should delete the provision in § 999.302, which exempts IP addresses from the definition of personal information. While information that can't be tied to a single, identifiable person should not necessarily be subject to access or deletion requests, particularly without controls to ensure that one's search terms are being shared with another person, if companies are using that data to target ads, it's identifiable and eliminating it from the definition of personal information is contrary to the clear language of the statute.[34] Consumers should retain opt-out rights in this case. This new provision significantly weakens the privacy protections of the CCPA and is essentially a loophole for targeted advertising. W219-4

IP addresses, even though they appear to be "anonymous," allow companies to access a significant amount of data about consumers and their families. While IP addresses assigned to consumers are often *dynamic* (in that they are periodically rotated), these numbers may in

[29] Ginny Marvin, *Digital Advertising's Opportunities & Threats from Mary Meeker's Internet Trends Report*, MARKETING LAND (June 1, 2018), https://marketingland.com/digital-advertisings-opportunities-threats-from-mary-meekers-internet-trends-report-241264.
[30] Chris Jay Hoofnagle et al., *Privacy And Modern Advertising: Most US Internet Users Want 'Do Not Track' to Stop Collection Of Data About Their Online Activities*, AMSTERDAM PRIVACY CONFERENCE (Oct. 8, 2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2152135; Kristin Purcell et al., *Search Engine Use Over Time*, PEW RESEARCH CTR. (Mar. 9, 2012), http://www.pewinternet.org/2012/03/09/main-findings-11/; J. Turow et al., *Americans Reject Tailored Advertising And Three Activities That Enable It*, SSRN (2009), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.
[31] Lee Raine, *The State of Privacy In Post-Snowden America*, PEW RESEARCH CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.
[32] Fatemeh Khatibloo, *Marketers, Here's How Your Customers Feel About Privacy*, FORBES (Dec. 16, 2016), https://www.forbes.com/sites/forrester/2016/12/16/marketers-heres-how-your-customers-feel-about-privacy/#52356c0f18e4.
[33] Mary Madden and Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Research Center (May 20, 2015), https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/; Joseph Turow et al., The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation, Annenberg School for Communication, University of Pennsylvania (Jun. 2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.
[34] Cal. Civ. Code §1798.140(o)(1)(A).

practice not be changed for months at a time; and as companies migrate to IPv6 addresses, there may be no need to rotate IP addresses at all as IPv6 effectively eliminates the problem of address scarcity. It can easily be used to track user behavior over time, even without access to cookies or other identifiers.[35] Moreover, correlation of IP addresses allows companies to engage in cross-device tracking, as devices that share local networks are considerably more likely to be operated by the same persons—meaning that they're used to develop detailed profiles about consumers, across devices, and about those with whom they live and spend time, for ad targeting purposes.[36] Currently, the CCPA gives consumers the right to opt out of its sale to third parties, but removing IP address from the definition of personal information would rescind this right.

W219-4 (cont.)

This new provision goes far beyond the Attorney General's rulemaking authority. Section 1798.185 gives the AG the authority to issue rules to further the purposes of the title, which are, in turn, to further Californians' constitutional right to privacy.[37] Significantly weakening the definition of personal information would go against the AG's remit under the CCPA. IP addresses are explicitly included in the CCPA's definition of personal information,[38] and to remove them clearly subverts legislative intent. Finally, a bill to accomplish the same goals as provision § 999.302—to exempt IP addresses from the protections of the CCPA—was properly defeated in the California legislature in July.[39] It would be inappropriate for the AG to overrule the legislature by inserting this provision now.

The AG should make global opt-outs more user-friendly.

We appreciate that the AG has kept the requirement that companies must honor browser privacy signals as an opt-out of sale.[40] Forcing consumers to opt out of every company, one by one—including from data brokers, whom consumers may not even know are collecting their data—is simply not workable. However, the current draft should be adjusted to ensure that it is consumer-friendly. The AG should state that platform-level controls to limit data sharing should be interpreted as CCPA opt-outs, including Do Not Track and Limit Ad Tracking. Or at the very least, the AG should clarify how platforms can certify that new or existing privacy settings should be construed as CCPA opt-outs.

W219-5

First, the AG should make it explicit in the rules that enabling Do Not Track opts the consumer out of the sale of their information. Instead, the updated draft regulations require browser signals

[35] Dennis Hartman, *The Advantages & Disadvantages to a Static IP Address*, TECHWALLA (last visited March 7, 2019), https://www.techwalla.com/articles/the-advantages-disadvantages-to-a-static-ip-address.
[36] *Cross-Device Tracking: An FTC Staff Report*, FED. TRADE COMM'N at 3 (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.
[37] Cal. Civ. Code §1798.175.
[38] Cal. Civ. Code §1798.140(o)(1)(A).
[39] AB 873 (2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB873.
[40] § 999.315(d).

to clearly convey that it constitutes an opt-out of sale, and require consumers to actively indicate their choice to opt-out.[41] This language unduly restricts consumer agency, particularly because it would mean that signing up for Do Not Track—likely the most well-known privacy setting, at one time adopted by Safari, Internet Explorer, Chrome, and Firefox—would not opt consumers out of sale.[42] While we do not object to the requirement in the draft regulations that opt-out settings should be off by default, consumers would reasonably expect that enabling Do Not Track would opt them out of sale to third parties. Consumers shouldn't have to take an additional step to opt out of sale after they enable DNT or a similar setting. This would mean that consumers already using DNT—by one estimate, nearly a quarter of American adults—would be much less likely to benefit from the AG rule, since they would likely assume that they had already opted out of sale.[43]

W219-5 (cont.)

But DNT isn't the only platform-level privacy setting governing third-party sharing. To encourage the development and awareness of, and compliance with, privacy settings for other platforms, we urge the AG to issue rules governing: 1) how the developer of a platform may designate a particular privacy control to be deemed a valid request; 2) how the attorney general shall maintain and publish a comprehensive list of privacy controls to be deemed valid requests; and 3) the conditions under which business may request an exception to sell data notwithstanding a consumer's valid request.

Millions of consumers have signed up for Do Not Track, but there are other settings that are far less well known, in part because they're not associated with online use. For example, Apple, in 2013 introduced a mandatory "Limit Ad Tracking" setting for iPhone applications, and even improved that tool to further limit the information advertisers can receive when the setting is activated.[44] Consumers also need global opt-outs from sale when using their smart televisions and voice assistants. In order to better raise awareness of the different options on the market, to encourage the development of new tools, and to address the lack of clarity around which browser settings must be honored as opt-outs, the AG should set up a system in order to make this clear for consumers and businesses.

[41] § 999.315(d)(1).
[42] *See, The Tragic Death of Do Not Track*, *supra* note 26. While it is true that in 2012, Microsoft enabled DNT in its Internet Explorer browser by default that was discontinued in 2015 following sustained criticism.
[43] Kashmir Hill, *'Do Not Track,' the Privacy Tool Used by Millions of People, Doesn't Do Anything*, GIZMODO (Oct. 15, 2018), https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324.
[44] Lara O'Reilly, *Apple's Latest iPhone Software Update Will Make It A Lot Harder for Advertisers to Track You*, BUS. INSIDER (Sept. 10, 2016), http://www.businessinsider.com/apple-ios10-limit-ad-tracking-setting-2016-9.

The AG should clarify that financial incentives in markets that lack competition is an unfair and usurious practice.

Consumers shouldn't be forced to choose between affordable necessities and exercising their right to privacy. Unfortunately, the CCPA suggests that companies can charge higher prices to consumers who limit access to their data and can offer financial incentives to consumers for the collection and sale of their personal information.[45] This language was added to the CCPA over objections from advocates, who argued that consumers should not be penalized for exercising their privacy rights.[46] While consumers may expect to have their purchases tracked by a company to be rewarded for repeated patronage, selling that consumer data to third parties runs counter to what participating consumers would reasonably expect.

W219-6

To prevent some of the worst abuses associated with financial incentives, discriminatory treatment should be presumed where markets are consolidated and consumers lack choices. The CCPA prohibits financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.[47] And, the AG currently has the authority under the CCPA to issue rules with respect to financial incentives.[48] Thus, we urge the AG to exercise its authority to prohibit the use of financial incentives in market sectors that lack competition. ISPs, for example, should not be allowed to charge consumers for exercising their privacy rights, because customers lack the meaningful opportunity to find more affordable options elsewhere. For example, for years, AT&T charged usurious rates—about $30 per month—for not leveraging U-Verse data for ad targeting.[49] Where consumers have few choices, market forces don't impose sufficient constraints on companies from penalizing exercising privacy rights. And, there is rising concentration across many industries in the United States,[50] further highlighted by the creation of a Federal Trade Commission task force to monitor these trends.[51] The AG should exercise its authority to put reasonable limits on these programs in consolidated markets.

[45] Cal. Civ. Code §§ 1798.125(a)(2) and .125(b).
[46] Consumers Union Letter re: AB 375 (Jun. 28, 2018), https://advocacy.consumerreports.org/wp-content/uploads/2018/06/CU-Letter-AB-375-final-1.pdf.
[47] Cal. Civ. Code § 1798.125(b)(4).
[48] Cal. Civ. Code § 1798.185(a)(6).
[49] Jon Brodkin, *AT&T to End Targeted Ads Program, Give All Users Lowest Available Price*, ARS TECHNICA (Sept. 30, 2016), https://arstechnica.com/information-technology/2016/09/att-to-end-targeted-ads-program-give-all-users-lowest-available-price/.
[50] *Too Much of a Good Thing*, THE ECONOMIST (March 26, 2016), https://www.economist.com/briefing/2016/03/26/too-much-of-a-good-thing.
[51] *FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets*, FED. TRADE COMM'N (Feb. 26, 2019), https://www ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology.

The AG should require companies to forward opt-out requests to third parties to whom it has sold data, if they have the information to do so.

To make the CCPA workable for consumers, there must be some obligation on companies to facilitate opt-out requests within the data-sharing ecosystem. In the previous draft of the proposed rules, companies were required to notify all third parties to whom it had sold data, when it received an opt-out request from a consumer. Under the updated rules, companies only need notify those with whom the information was sold after opt-out request was received.[52] The new rule is too limited. Where possible, companies should be required to forward opt-out requests.

W219-7

Since companies may have sold data to any number of companies without a consumer's knowledge—including data brokers, with which consumers have no direct relationship—the updated rule significantly undermines consumers' ability to protect their privacy. Further, the CCPA doesn't require transparency about the precise third parties to which data is sold.[53] While companies may not always maintain detailed records on all of the companies with whom they have sold data, especially in adtech transactions in which data is potentially transferred with hundreds of companies in a fraction of a second, if the company knows who it has sold the data to, they should be required to forward the opt-out request.

The AG should consider placing a retention limit on records of deletion.

The draft rules have been amended to allow companies to hold onto a deletion request, to help ensure that the personal information remains deleted.[54] We suggest that the AG consider placing a retention limit on these records, since the very fact of having an account with a company—for example, Ashley Madison, Tinder, and Grindr—can reveal more about a person than they might like others to know.[55]

W219-8

Given the plethora of data breaches—Privacy Rights Clearinghouse has tracked nearly 10,000 since 2006[56]—and the fact that it's not clearly stated in the CCPA that a company can't sell the information retained about a consumer following a deletion request, companies shouldn't be able to hold onto that information indefinitely. Further, the rationale that the record of deletion needs to be retained to ensure that information stays deleted is not entirely convincing, as a deletion request is not the same as a prohibition on collection—a company could conceivably collect information about a consumer again.

[52] § 999.315(f).
[53] Cal. Civ. Code §1798.110(4).
[54] § 999.313(d)(5).
[55] Thomas Germain, *How Private Is Your Online Dating Data?* CONSUMER REPORTS (Sept. 21, 2019), https://www.consumerreports.org/privacy/how-private-is-your-online-dating-data/.
[56] Privacy Rights Clearinghouse, Data Breaches (last visited Feb. 23, 2020), https://privacyrights.org/data-breaches.

The AG draft rules appropriately address household-level access and deletion requests.

The updated rules allow companies to honor access and deletion requests of unauthenticated or household-level data, when all the members of the household have placed a request jointly, and have verification their identities.[57] While this is a high bar to meet, avoiding risk of unwanted disclosure of information is important. Transparency, data portability, and access rights are key protections, but without a high bar to verify that all members of the household are comfortable with the request, the risk of disclosure of sensitive information to a person other than the consumer is simply too great.

W219-9

In addition, while the CCPA already notes that businesses need not reidentify or link data in order to comply with access requests,[58] we have no objection to clarifying further that there is no need to collect and associate information with a real name in order to provide access. Otherwise, there is the potential that someone other than the consumer, including a spouse or roommate, could obtain sensitive information about the consumer without their authorization. Not only could this be harmful to a consumer's privacy, but also it could facilitate identity theft. Identity theft by family members is a serious problem, by one estimate totaling approximately one-third of instances of identity theft overall.[59]

Thank you for the opportunity to submit comments on the updated draft rules. We would be happy to address any questions you have.

Respectfully submitted,

Maureen Mahoney
Policy Analyst
San Francisco, CA

Justin Brookman
Director, Privacy and Technology Policy
Washington, DC

[57] § 999.318
[58] Cal. Civ. Code § 1798.110(d)(2).
[59] Bruce Kennedy, *When Identity Theft is a Family Affair,* CBS NEWS (Apr. 14, 2014), https://www.cbsnews.com/news/when-identity-theft-is-a-family-affair/.

From: Kelly C. O"Brien
To: Privacy Regulations
Cc: Lara L. DeCaro; Javier A. Bastidas
Subject: Comments to Proposed Modified Regulations Concerning the California Consumer Privacy Act ("CCPA")
Date: Tuesday, February 25, 2020 4:36:56 PM
Attachments: Comments to Proposed Modified Regulations Concerning the California Consumer Privacy Act (01548720x9C6B5).pdf

---

Dear Deputy Attorney General Kim:

Please find attached correspondence from Lara DeCaro and Javier Bastidas regarding comments to proposed modified regulations concerning the California Consumer Privacy Act ("CCPA").

Thank you.

Kelly

Kelly C. O'Brien
Legal Assistant to Lara L. DeCaro and Javier A. Bastidas
Leland, Parachini, Steinberg, Matzger & Melnick, LLP
199 Fremont Street, 21st Floor
San Francisco, CA 94105
Telephone: (415) 957-1800
Facsimile: (415) 974-1520
Email: [redacted]

LELAND PARACHINI STEINBERG MATZGER & MELNICK LLP

LARA L. DECARO
[redacted]
JAVIER A. BASTIDAS
[redacted]

February 25, 2020

Sent via electronic mail

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

Re: **Comments to Proposed Modified Regulations Concerning the California Consumer Privacy Act ("CCPA")**

Dear Deputy Attorney General Kim:

On behalf of our law firm, Leland, Parachini, Steinberg, Matzger & Melnick, LLP, we respectfully provide the following comments concerning the Proposed Modified Regulations for the California Consumer Privacy Act. We appreciate and applaud the Attorney General's efforts to clarify the originally proposed regulations. Below we propose alternative text for the limited issues we perceive as presenting concrete problems for our clients engaged in business here in California and beyond. These issues primarily and consistently revolve around the inclusion within these newly issued proposed rules of so-called "generally recognized industry standards" for on-line information accessibility.

To preface these comments, we believe it is necessary to summarize our position as to the consequences of the proposed "accessibility" language. While our firm of course supports the requirement that all website notices be "reasonably accessible to consumers with disabilities," respectfully, we believe that the Attorney General's office may have overstepped its authority by introducing language, in essence new law, concerning the use of "Web Content Accessibility Guidelines." The United States Department of Justice ("DOJ") has urged that "public accommodations have flexibility in how to comply with the ADA's general requirements of nondiscrimination and effective communication" (see letter dated September 25, 2018, from Assistant General Stephen E. Boyd[1]). Furthermore, in *Robles v. Domino's Pizza, LLC* (2019) 913 W220-1

[1] https://www.adatitleiii.com/wp-content/uploads/sites/121/2018/10/DOJ-letter-to-congress.pdf

F.3d 898, the Ninth Circuit held that the ADA was intended to give businesses "maximum flexibility" in meeting the statute's requirements.

> "A desire to maintain this flexibility might explain why DOJ withdrew its [Advanced Notice of Proposed Rulemaking] related to website accessibility and 'continue[s] to assess *whether specific technical standards are necessary and appropriate* to assist covered entities with complying with the ADA'." (*Id.* at 908-909, citing 82 Fed. Reg. 60921-01 (December 26, 2017) [emphasis in original]).

In other words, the Federal government has spoken on this point. While the California legislature, if not pre-empted (see e.g. *In re People ex rel. Harris v. Delta Air Lines, Inc.* (2016) 247 Cal.App. 4 884), could perhaps create new law concerning accessibility, it did not do so when it passed the CCPA. In fact, the only mention of accessibility within the CCPA is found under Section 1798.185(a)(6), where there is no mention of the so-called "generally recognized industry standards" or the "Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium." The Attorney General's office has therefore promulgated new law in conflict with the binding precedent of the Ninth Circuit cited above. W220-1 (cont.)

The Web Content Accessibility Guidelines are also quite technical and voluminous, over 80 pages of materials. This is an incredible amount of information to absorb within a 15-day (or even a 45-day) comment period. Moreover, there is no evidence to support the proposition that Version 2.1 of these Guidelines equate with "generally recognized industry standards." In fact, both the DOJ and the Ninth Circuit hold positions, as stated above, that contradict this proposition. Furthermore, if other states were to issue different guidelines, it would be a practical impossibility for companies with a national presence to comply with every state's rules on this subject. It is therefore best to leave the decisions concerning website accessibility in the hands of the Federal government.

That said, we are grateful for the opportunity to present these comments. For each comment, we present first the proposed regulation to which we are responding, explain our specific concern(s), and recommend solutions in the form of proposed alternative text. We suggest that any mention of the Web Content Accessibility Guidelines in the proposed text be removed from the final Regulations altogether as these new provisions run counter to established law. We are available to answer any questions you may have regarding these comments and look forward to the final text.

PROPOSED TEXT:

§ 999.302. Guidance Regarding the Interpretation of CCPA Definitions

(a) Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "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." For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be "personal information."

W220-2

POSITION - SUPPORT: The above clarification is extremely helpful. In advising clients regarding the new privacy law, it has been extremely difficult to ascertain whether or not the CCPA even applies to certain businesses. The above limitation regarding IP addresses will certainly give concrete guidance to our clients.

PROPOSED TEXT:

§ 999.305. Notice at Collection of Personal Information.

d. Be reasonably accessible to consumers with disabilities. ~~At a minimum,~~ For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

W220-1 (cont.)

POSITION: SUPPORT IN PART/OPPOSE IN PART: Aside from the insertion of the word "reasonably," the other introduced language oversteps the authority of the Attorney General's office. The new language contradicts the mandate of Ninth Circuit case law (see *Robles* case cited above). Accessibility regulations are also pre-empted by the broad scope of the ADA.

PROPOSED SOLUTION: Retain "reasonably" but otherwise return to the original language of the proposed Regulations issued on October 10, 2019, so that the text reads as follows: "d. Be reasonably accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format."

PROPOSED TEXT:

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

d. Be reasonably accessible to consumers with disabilities. ~~At a minimum,~~ For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

POSITION: SUPPORT IN PART/OPPOSE IN PART: Aside from the insertion of the word "reasonably," the other introduced language oversteps the authority of the Attorney General's office. The new language contradicts the mandate of Ninth Circuit case law (see *Robles* case cited above). Accessibility regulations are also pre-empted by the broad scope of the ADA.

PROPOSED SOLUTION: Retain "reasonably" but otherwise return to the original language of the proposed Regulations issued on October 10, 2019, so that the text reads as follows: "d. Be reasonably accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format."

W220-1 (cont.)

PROPOSED TEXT:

§ 999.307. Notice of Financial Incentive

d. Be reasonably accessible to consumers with disabilities. ~~At a minimum,~~ For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

POSITION: SUPPORT IN PART/OPPOSE IN PART: Aside from the insertion of the word "reasonably," the other introduced language oversteps the authority of the Attorney General's office. The new language contradicts the mandate of Ninth Circuit case law (see *Robles* case cited above). Accessibility regulations are also pre-empted by the broad scope of the ADA.

PROPOSED SOLUTION: Retain "reasonably" but otherwise return to the original language of the proposed Regulations issued on October 10, 2019, so that the text reads as follows: "d. Be

reasonably accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format."

PROPOSED TEXT:

§ 999.308. Privacy Policy

> d. Be reasonably accessible to consumers with disabilities. ~~At a minimum,~~ For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

POSITION: SUPPORT IN PART/OPPOSE IN PART: Aside from the insertion of the word "reasonably," the other introduced language oversteps the authority of the Attorney General's office. The new language contradicts the mandate of Ninth Circuit case law (see *Robles* case cited above). Accessibility regulations are also pre-empted by the broad scope of the ADA. W220-1 (cont.)

PROPOSED SOLUTION: Retain "reasonably" but otherwise return to the original language of the proposed Regulations issued on October 10, 2019, so that the text reads as follows: "d. Be reasonably accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format."

In sum, the new accessibility language included in Sections 999.302 through 999.306 appears to encroach on the powers of the legislative branch and is therefore unconstitutional. The language clearly contradicts the flexibility that the DOJ has sought to maintain, and the new proposed law fails to abide by the Ninth Circuit's holding in *Robles*. Furthermore, the Federal government has legislated on the question of accessibility with the passage of the ADA, and at least one California Court of Appeal has held that the ADA pre-empted the California Online Privacy Protection Act. It follows that the CCPA should likewise be pre-empted by the ADA. In short, the Attorney General's office should not be making new law in this area concerning accessibility, certainly not while providing the public a mere 15-day comment period.

Thank you for your time and consideration of these comments.

Very truly yours,

Lara L. DeCaro
LELAND, PARACHINI, STEINBERG,
MATZGER & MELNICK, LLP

Javier A. Bastidas
LELAND, PARACHINI, STEINBERG,
MATZGER & MELNICK, LLP

From: Tony Ficarrotta
To: Privacy Regulations
Cc: David LeDuc; Leigh Freund
Subject: Comments from the Network Advertising Initiative (NAI)
Date: Tuesday, February 25, 2020 4:32:13 PM
Attachments: NAI Comment Letter - CCPA Modified Proposed Regulations (February 25, 2020).pdf

---

Thank you for the opportunity to submit comments regarding the modifications to the proposed regulations for the California Consumer Privacy Protection Act of 2018 (CCPA). Please find attached comments from the NAI. If you have any questions or would like to discuss these comments in greater detail, please feel free to reach out.

Thank you,

--
Tony Ficarrotta
Counsel, Compliance & Policy
Network Advertising Initiative
[redacted] | [redacted]

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

February 25, 2020

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: Modified 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 modifications to the regulations proposed for adoption[1] under the California Consumer Privacy Act of 2018 (the "CCPA").[2]

The NAI appreciates the remarkable effort the Office of the Attorney General ("OAG") has put forth to review thousands of pages of comments submitted by dozens of stakeholders in response to the initial proposed regulations. The modified proposed regulations ("MPRs") clearly represent thoughtful engagement by the OAG with those comments, and they include a number of marked improvements that will promote business compliance with the CCPA.

The NAI has, however, identified certain proposed changes in the MPRs that would benefit from further clarifications and changes, discussed below.

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.

[1] CAL. CODE REGS. tit. 11, §§ 999.300-341 (proposed Feb. 10, 2020).
[2] CAL. CIV. CODE §§ 1798.100 *et seq.*

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 the NAI's 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 Federal Trade Commission. These 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 and the MPRs. 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 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 and the MPRs 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 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. *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 MPRs should be amended to clarify when information pertains to a "particular consumer or household."

The MPRs add a new section titled "Guidance Regarding the Interpretation of CCPA Definitions."[9] This section is currently populated only with guidance on the CCPA's definition of "personal information," as follows:[10]

> *Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "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." For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be "personal information."*

W221-1

The NAI welcomes this additional guidance on the definition of "personal information" (and other definitions in the future) and believes businesses will generally benefit from such guidance. Still, this proposed guidance on the definition of "personal information" is generating confusion, because while the CCPA explicitly refers to IP address as a kind of "identifier" and as a "unique personal identifier" that may fall under the definition of "personal information,"[11] the guidance calls the classification of IP address as a form of personal information into question, that is, when it may or may not be considered personal information. Further, because IP address is defined by the CCPA as a type of "unique personal identifier," the guidance also calls into question whether other unique personal identifiers enumerated by the CCPA (such as device identifiers, cookies, beacons, pixel tags, mobile ad identifiers, and even telephone numbers)[12] may also fall outside the definition of personal information in certain circumstances.

The basic source of the confusion generated by the guidance stems from uncertainty around what it means to link an IP address (or another unique personal identifier) to a "particular consumer or household." Intuitively, a business "linking" an IP address to a "particular consumer or household" would involve associating the IP address with other identifiers known by the business to refer to a particular consumer or household. For example, if a business

[9] CAL. CODE REGS. tit. 11, § 999.302 (proposed Feb. 10, 2020).
[10] *Id.* § 999.302(a).
[11] *See* CAL. CIV. CODE §§ 1798.140(o)(1)(A) (referring to both "unique personal identifier" and "internet protocol address" as types of personal information); 1798.140(x) (referring to "an Internet Protocol address" as a type of "unique identifier" or "unique personal identifier.").
[12] *Id.* § 1798.140(x).

knows a consumer's full name (referring to a "particular" consumer) and links, or reasonably could link, an IP address with that full name, the IP address would become personal information in the hands of that business. Similarly, a business may know a residential address for a household, and if it links an IP address to the residential address, that would also cause the IP address to be personal information.

The NAI recommends clarifying the guidance on the definition of "personal information" by specifying that information such as an IP address is not personal information unless the business processing such information has linked it, or reasonably could link it, with additional pieces of information known by the business to identify a particular consumer or household, such as name or residential address.

This approach would be largely consistent with the way the NAI Code treats pseudonymous information like an IP address: such information is only considered Personally-Identified Information if it is "linked, or intended to be linked, to an identified individual[.]"[13] This approach places the focus on what a business holding the information does, or actually intends to do with it – not on what may be theoretically possible for any business to do with it. For example, if a news website operator collects IP addresses from website visitors, but does not link IP addresses to any identified individuals (and does not intend to so link them), the IP address is not considered Personally-Identified Information under the NAI Code – even if the same IP address, in the hands of another kind of business like an internet service provider, could be linked to identified individuals.

W221-1 (cont.)

Recommended Amendments to the MPRs:

Section 999.302(a)

Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "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." For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any information known by the business to identify a particular consumer or household, such as a full name or residential address, and could not reasonably link the IP address with such information ~~particular consumer or household~~, then the IP address would not be "personal information."

[13] NAI CODE OF CONDUCT, *supra* note 4, at § I.K. Note, however, that IP address is still considered Device-Identified Information and its use is therefore subject to many requirements under the NAI Code, including access to an Opt-Out Mechanism for Tailored Advertising. *See id.* §§ I.E (defining Device-Identified Information); II.C.1.a (requiring an Opt-Out Mechanism for the use of Device-Identified Information for Tailored Advertising).

Part II: Consumer Exercises of CCPA Rights and Business Responses

A. The proposed regulations should not require businesses to disclose precise geolocation information in response to certain consumer requests to know.

The MPRs add a new type of personal information that a business may not disclose in response to a consumer request to know: "unique biometric data generated from measurements or technical analysis of human characteristics."[14] The NAI recognizes that the addition of this type of biometric information by the MPRs was likely in response to the legislature's addition of the same type of biometric information to the list of personal information that, if subject to a data breach, could lead to the exercise of the CCPA's private right of action.[15] This change in the MPRs is consistent with the OAG's reasoning in the Initial Statement of Reasons ("ISORs") as to why certain types of personal information must not be disclosed in response to a request to know (*i.e.*, to "reduce the risk that a business will violate another privacy law, such as Civil Code section 1798.82, in the course of attempting to comply with the CCPA.").[16]

However, the ISORs contain an additional rationale as to why certain types of personal information may not be disclosed pursuant to a request to know, which is balancing "the consumer's right to know with the harm that can result from the inappropriate disclosure of information."[17] Therefore, the MPRs should be further amended under that rationale to include precise geolocation information[18] as a type of personal information businesses may not disclose to consumers who are not accountholders. W221-2

The improper disclosure of the precise physical location of a consumer or device over time is potentially very sensitive information. However, the risk of improper disclosure is reduced when a business maintains an account for the consumer making the request because, in that case, the business likely maintains information like an email address and a username/password it may use to securely authenticate a consumer. By contrast, in cases where a business processing precise geolocation information does *not* maintain consumer accounts – *e.g.,* as is the case with a number of NAI members who act as "third party" platforms – the information is

[14] CAL. CODE REGS. tit. 11, § 999.313(c)(4) (proposed Feb. 10, 2020).
[15] *See* CAL. CIV. CODE § 1798.81.5(d)(1)(vi) (listing "unique biometric data generated from measurements or technical analysis of human body characteristics" as a form of covered personal information); *id.* § 1798.150(a)(1) (specifying the types of personal information that, if subject to a data breach, support a private right of action).
[16] CAL. DEP'T OF JUSTICE, OFFICE OF THE ATTORNEY GEN., INITIAL STATEMENT OF REASONS (ISOR), PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS 18 (2019) [hereinafter ISORs], https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.
[17] *Id.*
[18] The NAI Code of Conduct refers to this type of information as "Precise Location Information," defined as "data that describes the precise geographic location of a device derived through any technology that is capable of determining with reasonable specificity the actual physical location of an individual or device, such as GPS-level latitude-longitude coordinates or location-based radio frequency signal triangulation." NAI CODE OF CONDUCT, *supra* note 4, at § I.L.

often held in pseudonymous form only (*e.g.*, associated only with a mobile advertising identifier). This in turn presents unique difficulties for those businesses, because they have no secure way to connect a purely pseudonymous identifier with any particular consumer. There is no way for these third parties to know whether the location information they have pertains to the person who has submitted the request, or whether either the person in possession of a device or the person requesting the information is the actual device owner. These third parties therefore cannot reasonably verify the identity of such users in a manner sufficient to justify providing access to detailed location information – and for reasons of personal privacy and even public safety, the NAI requests that the OAG makes this clear.

This is not merely a hypothetical issue. It is common for a variety of people to have or gain possession of or access to another's mobile device – partners, friends, colleagues or others, whether consensually or not. Any of those persons – whether entrusted by the owner or not – could easily obtain a device ID (from device settings) or take a screenshot of that identifier; if doing so were possible grounds for verifying a request to know, then that person could also obtain the detailed location information of a colleague, spouse, friend or acquaintance. Further, a recent study concluded that approximately one half of mobile phones were not password protected – making the possibility of such "spoofing" a very real concern.[19] Even were a consumer to physically present a mobile device to the business, the business may not be in a position to know if the device is secure (e.g., whether it had a passcode known only by its proper owner/user), or if it has been stolen or otherwise misappropriated.

W221-2 (cont.)

Moreover, because "third party" platforms (such as NAI members) studiously avoid collecting names, addresses and emails for privacy reasons, they lack those conventional ways to verify the identity of an actual device owner.

Still, consumers in this position would have access to the fact that a business maintains precise geolocation information through the exercise of their right to know the categories of personal information the business maintains,[20] and could still exercise choices with the business about that information (*e.g.*, to opt out of the sale of such information, or to delete it).[21] The exercise of opt out or deletion rights by consumers (with the attending degree of verification required by the MPRs)[22] may adversely affect a business's commercial interests, but unauthorized deletion of precise geolocation information, or opting out of its sale, do not present comparable risks of harm to the consumer as inadvertent disclosure would. Further, the utility of log-level GPS data to consumers is likely minimal (indeed, the NAI is not familiar with any legitimate consumer use cases for such data).

[19] *See* Press Release, Kapersky Lab, Kapersky Lab Finds Over Half of Consumers Don't Password-Protect their Mobile Devices (June 28, 2018), https://usa.kaspersky.com/about/press-releases/2018_kaspersky-lab-finds-over-half-of-consumers-don-t-password-protect-their-mobile-devices.
[20] *See* CAL. CODE REGS. tit. 11, § 999.313(c)(10) (proposed Feb. 10, 2020).
[21] *See id.* §§ 999.315 (pertaining to the right to opt out); 999.313(d) (pertaining to the right to delete).
[22] *See id.* § 999.325.

Due to the considerations discussed above, some businesses processing precise geolocation information only on a pseudonymous basis already believe that they cannot verify the identity of consumers to a reasonably high degree of certainty and would not release precise geolocation information pursuant to a request to know for that reason.[23] But similarly situated businesses remain uncertain of their obligations under the CCPA and the MPRs. To avoid inconsistencies as to how consumer requests to know precise geolocation information are treated, and to protect consumers from the risk of harm from improper disclosure of such information, the MPRs should add precise geolocation information as a type of personal information that businesses may not disclose to non-accountholders in response to requests to know.

W221-2 (cont.)

Recommended Amendments to the MPRs:

Section 999.313(c)(4):

A business shall not disclose in response to a request to know 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, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. If a consumer does not have or cannot access a password-protected account with the business, the business shall not disclose in response to a request to know a consumer's precise geolocation information.

B. The proposed regulations should not require businesses to interpret global privacy controls as overriding particular consumer choices.

The MPRs add new provisions that will help businesses understand how they should respond to global privacy controls.[24] In particular, the MPRs make changes ensuring that businesses are only required to treat global privacy controls as valid requests to opt out when those controls clearly communicate that a consumer intends to opt out of sales of personal information (not some other, undefined activity like tracking or advertising), and that global privacy controls represent an affirmative consumer choice, not a default setting.[25] In addition to those helpful clarifications, however, the MPRs also add a new provision requiring businesses to resolve conflicts between local (or site-specific) privacy settings and global privacy settings in favor of the global settings. This new provision does not promote consumer choice and conflicts with longstanding principles regarding how to resolve conflicts between general and specific rules.

W221-3

W221-4

Requiring businesses to honor global privacy controls instead of local controls does not promote consumer choice because it does not adequately account for existing preferences

[23] *See id.* §§ 999.325(c), (e)(2).
[24] *See id.* § 999.315.
[25] *Id.* § 999.315(d)(1).

expressed by consumers, and it will create a frustrating, confusing, and repetitive user experience. Consider, for example, the following hypothetical series of events:

1. A consumer visits Website 1, receives a notice of her right to opt out, and she consciously decides not to opt out of sales of personal information by that website in order to support the site.
2. Later, the consumer installs a new browser extension designed to signal a global preference to opt out of sales of personal information. The consumer thinks of this as a default preference, not as one that overrides prior choices.
3. Under the MPRs, a subsequent visit to Website 1 by the consumer would have to be treated by Website 1 as a request to opt the consumer out of sales (because of the presence of a global "do not sell" signal), unless the consumer confirms that she intends **not** to opt out of sales by Website 1.[26]
4. Regardless of how many times the consumer has confirmed her intent **not** to opt out of sales by Website 1, Website 1 would have to surface a confirmation request each time the site encounters that consumer in order to comply with the MPRs as currently drafted. This is because the global setting is always on and will therefore conflict with the existing local preference of the consumer each time the consumer navigates to Website 1 (or any other website where the consumer has expressed a specific preference).

W221-4 (cont.)

Bombarding consumers with repetitive notices and requests to confirm choices every time they visit known and trusted websites will lead to choice-fatigue and cause consumers to pay less attention to such notices over time. Consumers may instead simply click through without reading or considering privacy notices, a result that does not enhance consumer privacy.

Requiring businesses to override site-specific preferences in favor of global settings could also lead to inconsistent approaches due to continued uncertainty surrounding what global opt-out technologies will become available. This increases the likelihood of non-harmonized and conflicting signals and could create confusion and uncertainty for consumers and business alike. And, although the MPRs require businesses to honor only user-enabled (not default) privacy controls,[27] there are also significant issues around the reliability and authenticity of browser-based signals as well as difficulties clearly communicating which consumers are California residents. Making global settings trump local settings would only exacerbate those problems.

In addition, and irrespective of any notices that may be surfaced to consumers, requiring businesses to honor general settings over particular ones abandons the well-established maxim that if there is a conflict between a general provision and a specific provision, the specific

[26] *See id.* § 999.315(d)(2).
[27] *Id.* § 999.315(d)(1)

provision prevails.[28] This result is counterintuitive and probably does not align with consumer expectations.

Finally, requiring businesses to seek confirmation from consumers of business-specific choices will favor the few large brand advertisers who have direct relationships with consumers and have the ability to ask consumers to override browser or device-setting based opt-out requests. This is dangerous from a competition standpoint, hurting online advertisers' ability to compete as well as potentially reducing revenue for online journalism.

W221-4 (cont.)

For the reasons discussed above, global privacy settings should govern only where a user has indicated no particular preferences regarding the sales of personal information.

Recommended Amendments to the MPRs:

Section 999.315(d)(2):

If a global privacy control conflicts with a consumer's existing business-specific privacy setting or their participation in a business's financial incentive program, the business ~~shall respect the global privacy control but~~ may continue to rely on the existing business-specific privacy setting or the consumer's participation in the financial incentive program ~~notify the consumer of the conflict and give the consumer the choice to confirm the business-specific privacy setting or participation in the financial incentive program~~.

C. The regulations should not require businesses to pass consumer opt-out requests on to any other business for which a consumer has not made an opt-out request.

As the NAI discussed at length in its comments on the initial proposed regulations, the core principles of the CCPA are notice and choice – principles the initial proposed regulations would have departed from had they retained a 90-day lookback for opting out of sales by third parties.[29] Specifically, the initial proposed regulations would have required each business in receipt of a request to opt-out to notify each third party to whom the business had sold personal information within 90 days of receiving the request to opt out, and to require each third party so notified to also opt the consumer out of its sales of personal information for that consumer.[30]

W221-5

[28] *Cf.* ANTONIN SCALIA & BRYAN A. GARNER, READING LAW: THE INTERPRETATION OF LEGAL TEXTS (1st ed. 2012) (explaining that under the canon *generalia specialibus non derogant*, if there is a conflict between a general provision and a specific provision, the specific provision prevails. While the NAI recognizes that this canon applies literally only to statutory interpretation, it is also useful for inferring intent in other contexts, such as a consumer's intent when their general and specific privacy settings conflict).

[29] *See* Letter from Leigh Freund, President & CEO, Network Advert. Initiative, to Xavier Becerra, Attorney Gen., Cal. Dep't of Justice 13-15 (Dec. 6, 2019), https://www.networkadvertising.org/sites/default/files/final-nai_comment_letter_-_proposed_ccpa_regulations_dec._6_2019.pdf.

[30] *See* CAL. CODE REGS. tit. 11, § 999.315(f) (proposed Oct. 11, 2019).

The MPRs have removed the 90-day lookback found in the initial proposed regulations – a critical adjustment that the NAI strongly supports – but they have replaced it with a different (albeit more limited) lookback period. Specifically, the MPRs would extend the lookback only to the time between the consumer's submission of a request to opt-out and the time a business complies with it.[31]

The more limited scope of the lookback in the MPRs does not, however, resolve other problems with any such lookback. For example, even a more limited lookback still does not take into account the role of the new data broker registry as the primary mechanism through which consumers can exercise their CCPA rights with third parties (such as data brokers) they do not have a direct relationship with. Instead, it would still cause third parties in some circumstances to opt a consumer out of sales of personal information as a matter of law, not pursuant to any actual consumer choice. Instead of forcing third parties to comply with an opt out request a consumer never made, consumers should instead use the data broker registry to identify third parties with whom to exercise their CCPA rights.

W221-5 (cont.)

In addition, it will be difficult or impossible for businesses to operationalize the requirement to notify businesses they have sold personal information to and instruct them to stop selling that information, even with the more limited lookback to. Consumers are adequately protected by the maximum 15 business day period for complying with valid requests to opt-out.[32]

For those reasons, the MPRs should be amended to remove any lookback requirement for forwarding opt-out requests.

Recommended Amendments to the MPRs:

Section 999.315(f):

A business shall comply with a request to opt-out as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. ~~*If a business sells a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request, it shall notify those third parties that the consumer has exercised their right to opt-out and shall direct those third parties not to sell that consumer's information.*~~

[31] *See* CAL. CODE REGS. tit. 11, § 999.315(f) (proposed Feb. 10, 2020).
[32] *See id.*

Part III: Disclosure Obligations

A. The obligations of businesses that do not collect personal information directly from consumers to provide a notice at collection should be further clarified.

According to the ISORs, the purposes of Section 999.305(d) of the proposed regulations include (1) to clarify that businesses who do not collect personal information directly from consumers (such as data brokers) are not required to provide a notice at collection under certain circumstances; and (2) to provide a way for such businesses to meet their obligations under Civil Code section 1798.115(d).[33]

Reliance by the MPRs on the data broker registry to achieve those purposes represents a more practical approach compared to the one taken by the initial proposed regulations.[34] Relying on the data broker registry is also more closely aligned with the NAI's longstanding approach to consumer transparency and choice around third-party data use, as the NAI operates a central page where consumers can go to learn about Tailored Advertising, and opt out of Tailored Advertising from some or all of NAI's member companies, if they so choose.[35] That said, the language in the MPRs would benefit from further clarification that the provision is intended for businesses that "sell" personal information. W221-6

This is an issue because section 999.305(d) of the MPRs as currently drafted removed reference to "sales" by businesses that do not collect information directly from consumers that was present in the initial proposed regulations.[36] However, section 999.305(d) of the MPRs pertains to businesses that are registered as data brokers – who, by definition, sell personal information to third parties.[37] Further, the intent of section 999.305(d) as articulated by the ISORs is to implement Civil Code Section 1798.115(d) – which prohibits a third party from re-selling personal information unless consumers have received explicit notice and an opportunity to opt out.[38] Because the intent of section 999.305(d) still appears to focus on businesses that *sell* personal information, the MPRs should be amended to make it more explicit that section 999.305(d) applies to certain businesses that *sell* personal information; and that it provides a way for those businesses to satisfy their obligations under Civil Code Section 1798.115(d).

[33] *See* ISORs, *supra* note 16, at 9-10.
[34] *See* CAL. CODE REGS. tit. 11, § 999.305(d) (proposed Feb. 10, 2020) (relieving businesses of the obligation to provide a notice at collection if they (1) are registered as data brokers and (2) do not collect information directly from consumers).
[35] To opt out of Tailored Advertising or to lean more, visit https://optout.networkadvertising.org.
[36] *Compare* CAL. CODE REGS. tit. 11, § 999.305(d) (proposed Oct. 11, 2019) (referring to steps a business that does not collect information directly from consumers must take "before it can sell a consumer's personal information") *with* CAL. CODE REGS. tit. 11, § 999.305(d) (proposed Feb. 10, 2020) (making no reference to a business's sales of personal information).
[37] *See* CAL. CIV. CODE § 1798.99.80(d).
[38] *See* ISORs, *supra* note 16, at 9-10.

Recommended Amendments to the MPRs:

Section 999.305(d)

If a business that (i) does not collect information directly from consumers and (ii) sells personal information to third parties is registered with the Attorney General as a data broker pursuant to Civil Code section 1798.99.80 et seq., it does not need to provide or take steps to require that the original source of the information provided a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out. A business that satisfies the conditions in this section is deemed to satisfy the requirements of Civil Code section 1798.115(d).

W221-6 (cont.)

By adopting these recommended amendments, the MPRs will avoid creating a scenario where businesses that don't "sell" personal information are pushed to register as data brokers to meet their obligations under Civil Code Section 1798.115(d).

Part IV: Other issues

A. The proposed regulations should not at this time present a design for an opt-out button.

Under the CCPA, the Attorney General is empowered to establish rules and procedures for the "development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information."[39]

The NAI supports the concept of a uniform logo or button to promote consumer awareness, and has consistently promoted similar industry efforts through the Digital Advertising Alliance's AdChoices Icon, Political Ads Icon, and most recently, the Privacy Rights Icon designed to assist companies with CCPA compliance.[40]

W221-7

There is, however, a design feature of the button introduced by the MPRs that may cause confusion among consumers and lead to inconsistent adoption among businesses. The proposed design appears to be a toggle – *i.e.*, a privacy control that a user would toggle on or off to either allow or disallow certain activities.[41] However, the MPRs specify that when a user engages the button, it should link out to a webpage or other online location with more information about consumer opt-out rights along with the actual form or method a consumer

[39] CAL. CIV. CODE § 1798.185(a)(4)(C).
[40] *See generally* DIGITAL ADVERTISING ALLIANCE, https://digitaladvertisingalliance.org (last visited Feb. 25, 2020).
[41] *See, e.g.,* The International Association of Privacy Professionals, https://iapp.org (last visited Feb. 25, 2020) (for an example of a true toggle control, navigate to the IAPP website and click the green and white cookie icon on the bottom-left corner of the page).

can use to submit an opt-out request.[42] This creates a conflict between the toggle design of the button and its function as a link to a different location where users can actually exercise control.

This peculiar design feature also points to a potentially broader problem with any future design mandates: because user-interface design is complex, fluid, and often subjective, it is difficult to set useful prescriptive requirements. It would be an undesirable outcome to have a widely-adopted (or even required) standard that is confusing for consumers.

For those reasons, the MPRs should not at this time introduce a design for a "do not sell" button, particularly when industry groups are actively promoting alternative designs that already benefit from marketplace adoption and awareness.[43] Injecting another icon or button option that will likely compete with existing industry icons will likely lead to unnecessary confusion in the marketplace. However, the NAI is supportive of efforts by the OAG to develop a process that would promote the use of a uniform button or logo consistent with Civil Code Section 1798.185(a)(4)(C), without recommending or mandating a specific design.

W221-7 (cont.)

Recommended Amendments to the MPRs:

Section 999.306(f):

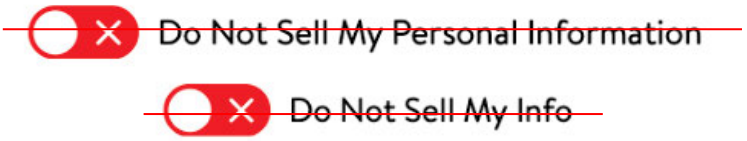
~~*(f) Opt-Out Button*~~

~~*(1) The following opt-out button may be used in addition to posting the notice of right to opt-out, but not in lieu of any posting of the notice of right to opt-out.*~~

~~*(2) When the opt-out button is used, it shall appear to the left of the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link as illustrated below, and shall be approximately the same size as other buttons on the business's webpage.*~~

[42] CAL. CODE REGS. tit. 11, § 999.306(f)(3) (proposed Feb. 10, 2020).

[43] *See, e.g.*, *Opt Out Tools,* DIG. ADVERT. ALL., www.privacyrights.info (last visited Feb. 25, 2020) (promoting the CCPA Privacy Rights Icon); IAB PRIVACY, IAB CCPA COMPLIANCE FRAMEWORK FOR PUBLISHERS & TECHNOLOGY COMPANIES VERSION 1.0 8 (2019), https://www.iab.com/wp-content/uploads/2019/12/IAB_CCPA-Compliance-Framework-for-Publishers-Technology-Companies.pdf (referring to an icon that the IAB may develop for use with its CCPA framework).



W221-7 (cont.)

~~*(3) This opt-out button shall link to a webpage or online location containing the information specified in section 999.306(c), or to the section of the business's privacy policy that contains the same information.*~~

B. The proposed regulations should further clarify permissible internal uses of personal information obtained in the course of providing services.

Section 999.314(c) of the MPRs helpfully clarifies that a service provider may in some circumstances retain, use and disclose personal information obtained in the course of providing services consistent with its status as a statutory service provider. However, this provision has also generated some confusion as businesses work to understand the scope of permitted activities for service providers.

In particular, businesses are struggling to understand which activities the MPRs intend to cover with the addition of the terms "cleaning" and "augmenting,"[44] as those terms do not have a common meaning in the digital advertising industry and are not defined by the CCPA or the MPRs. Without an established meaning in the industry or clarifying definitions in the MPRs, the introduction of these terms may lead to diverging interpretations and inconsistent application among businesses acting as service providers.

W221-8

For those reasons, the MPRs should be amended to remove reference to the terms "cleaning" and "augmenting."

Recommended Amendments to the MPRs:

Section 314(c)(3):

A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except . . . [f]or internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles~~, or cleaning or augmenting data acquired from another source~~.

[44] *See* CAL. CODE REGS. tit. 11, § 999.313(c)(3) (proposed Feb. 10, 2020).

Conclusion:

The NAI is grateful for the opportunity to comment on the MPRs. 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

From: Courtney Jensen
To: Privacy Regulations
Subject: TechNet Comment Letter Regarding Proposed CCPA Regulations
Date: Tuesday, February 25, 2020 4:31:01 PM
Attachments: TechNet AG CCPA Regulation Letter 2.25.20.pdf

Good Afternoon,

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

Please do not hesitate to reach out with any questions.

Thank you,
Courtney

Courtney Jensen
Executive Director | California and the Southwest
TechNet | The Voice of the Innovation Economy
[redacted]

TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet California and the Southwest | Telephone 916.600.3551
915 L Street, Suite 1270, Sacramento, CA 95814
www.technet.org | @TechNetUpdate

February 25, 2020

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

Dear Mr. Attorney General Becerra,

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

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic startups and the most iconic companies on the planet and represents three million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

TechNet member companies place a high priority on consumer privacy. We appreciate the aim of the CCPA to meaningfully enhance data privacy; however, the law was drafted quickly and is still in need of refinement. CCPA continues to contain unclear requirements that raise significant operational and compliance problems that do not advance privacy or data security. The Legislature has looked to the Attorney General on some issues to create cohesive rules based on a statute that in some parts is unclear. It is imperative for businesses and consumers in California that CCPA regulations move forward with the goal of providing clarity to the statute.

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

Compliance has been costly and every small change to the requirements of AB 375, via Attorney General regulations, necessitate expensive changes to platforms. Essentially, industry was required to build products without the criteria they would be graded on and now, we believe, certain portions of the draft regulations could cause further confusion and additional layers that were not clearly delineated when businesses began planning

for and implementing technologies to go live in 2020. We urge that any new requirements beyond those delineated in the statute be removed from the regulations or, at the very least, have a delayed effective date.

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

§ 999.301. Definitions

- The draft rules also define "*affirmative authorization*" as "*an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information*." Within the context of a parent or guardian acting on behalf of a child under 13, it means that the parent or guardian has provided consent to the sale of the child's personal information in accordance with the methods set forth in section § 999.330. For consumers 13 years and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in."
  - CCPA requires detailed notice concerning consumers' right to opt in to the sale of their information. This requirement coupled with consumers having to affirmatively and "clearly request to opt-in" works to ensure that consumers are making informed choices. It is therefore unclear why consumers would need to undertake an extra step concerning their affirmative and clear choice. Multiple pop-ups and other prominent notices like the separate opt-in confirmation are highly likely to be noticed, but can interrupt consumers' experiences. The more notifications presented to consumers, the less likely consumers are able to apprehend or absorb any one particular notice and make informed choices about their data. The more notices that companies display, the greater the chance of creating "click fatigue," whereby consumers skip over the words and click through to continue using the service. W222-1
  - We suggest striking the language mandating a two-step process as it can be cumbersome and disruptive for consumers and overly prescriptive for businesses. It can prevent businesses from developing innovative consent flows based on extensive User Experience (UX) and User Interface (UI) research.

§ 999.302. Guidance Regarding the Interpretation of CCPA Definitions

- We appreciate the guidance provided in § 999.302 regarding the definition of "personal information." Unfortunately, the guidance fails to appreciate that most pseudonymous or de-identified information could be linked to an individual but is not in practice. A business often maintains such information in de-identified fashion as a privacy safeguard, using technical and administrative controls such as hashing, encryption, and contractual safeguards to prevent its linkage to an individual. The European Union's General Data Protection Regulation recognizes this as a good practice.[1] W222-2
  - In order to reflect this distinction, we recommend the following revision, "*Whether information is 'personal information,' as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that 'identifies, relates to,*

[1] See, e.g., Regulation (EU) 2016/679 of the European Parliament and of the Council, Articles 25, 32.

describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.' For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, ~~and could not reasonably link the IP address with a particular consumer or household~~, then the IP address would not be "personal information."

W222-2 (cont.)

§ 999.305. Notice of Collection of Personal Information

- The draft rules in § 999.305(a)(4) include a new notice requirement regarding mobile devices. This new requirement is not tied to any specific provision of the statute and is significantly specific and prescriptive for a specific sector. This extremely prescriptive notice requirement could impact an enormous number of mobile applications and require a very specific, uniform disclosure. TechNet recommends adding flexibility in this new notice requirement for mobile devices. Granting flexibility to businesses in this notice requirement and others can help businesses find effective and innovative ways to inform consumers. At the very least, there should be flexibility on how information is provided- e.g., meaningful information about the most important types of data processing rather than a long list on a mobile device that is not actually meaningful or actionable for consumers because it is linkedly to be very long and unintelligible, and likely skipped by consumers.

W222-3

- The new requirement in § 999.305(d) is in need of clarity to confirm that it does not apply to a business whether or not it "sells" data. Clarity is needed to ensure that businesses are not inappropriately categorized as data brokers if a business is collecting information indirectly.

W222-4

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

- The draft rules in § 999.306(a)(2)(d) requires privacy notices to be "reasonably accessible to consumers with disabilities," yet standardized notification requirements like the envisioned toggle button can fail consumers with disabilities and diverse needs. Through extensive User Interface (UI) and User Experience (UX) research, businesses are in the best position to craft notices appropriately tailored to help inform consumers with specific needs and abilities and the rules should be flexible enough to allow businesses to craft the best options for consumers.

W222-5

- The draft rules in § 999.306(b) regarding the location "Do Not Sell My Personal Information" and "Do Not Sell My Info" link could be interpreted in two ways (1) a business **must** have the link on the download/landing page and the business may choose to put it in the setting menu too; or (2) If a business collects personal information through a mobile app, the business **must** have the link, but it can be on the download/landing page OR in the app, or both. TechNet believes this language is ambiguous and the proposed rules should clearly afford businesses flexibility on where to post the link, so they can select an area within their control and still helpful to consumers.

W222-6

- The draft rules in § 999.306(f) have proposed an optional "Do Not Sell My Personal Information" and "Do Not Sell My Info" toggle button. We urge the

W222-7

Attorney General to remove this toggle button as an option due to its unclear design. The toggle button omits important nuances that each business might need to convey based on its specific practices. Moreover, excessive standardization could lead to consumers ignoring notifications altogether. W222-7 (cont.)

§ 999.307. Notice of Financial Incentive

- The disclosures required in § 999.307(b)(5) in relation to financial incentives are impractical and deal with competitively sensitive information. It is challenging for any business to assign value to a single consumer's data, and data often gains value when it is aggregated. Consequently, financial incentive programs will more likely be based on a complex calculation of costs to the business and market comparisons, and they are designed to reward loyal customers rather than to serve as a value exchange. Any number that a business ultimately discloses will not be meaningful to consumers. Every business and service is different, and requiring a business to disclose its methods and calculations will likely require disclosure of competitively-sensitive information or deter businesses from offering these types of financial incentives for the benefits of consumers. The CCPA statutory language is already sufficiently protective of consumers with regard to discounts. Also, suggesting that consumer data is equal to a sum that may be bartered for goods or services also appears misaligned with the aim of the CCPA. W222-8
- As noted above, data doesn't have independent value. The perceived value of data is subjective, in flux and depends on context. Because data lacks clear, objective value, academics have come up with wildly different estimates for the value of certain services to people, and experts are likely to come up with differing values for other services as well. Concerning free, ads-based services, personalized services, people don't give up or exchange data for their experience; instead the experience is made possible by data. Data is what enables ads-based services to provide the core of the service itself, which is personalized content. The reason certain businesses can offer their services for free isn't that they're being compensated with people's data. It's that they make money by selling ads: these businesses sell advertisers the opportunity to present their messages to people. And advertisers pay the businesses based on object metrics such as the number of people who see their ads or the number of people who click on their ads.
- Specifically, § 999.307(b)(5) requires "*[a]n explanation of why the financial incentive or price or service difference is permitted under the CCPA, including: a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and a description of the method the business used to calculate the value of the consumer's data*." The rules articulate standards by which businesses can calculate the value of consumer data. We strongly recommend removing any requirements for providing an estimate of the value of consumer data.
  - The draft language should be revised to: "*[a]n explanation of why the financial incentive or price or service difference is permitted under the CCPA~~, including: a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and a description of the method the business used to calculate the value of the consumer's data~~*."

- We also propose striking § 999.337, which describes the methods in calculating the value of consumer data. This requirement to disclose the value and methodology goes beyond CCPA statutory language. We urge that this requirement be struck from the draft regulations. W222-9

§ 999.308. Privacy Policy

- The draft regulations would require that a business state in its privacy policy whether it "*has actual knowledge that it sells the personal information of minors under 16 years of age.*" 999.308(c)(1)(e)(3).
  - TechNet appreciates the addition of the "actual knowledge" standard, however we would suggest further refining this section to make clear that only a business that engages in the "sale" of personal information would be required to make such a statement. In the absence of such clarity, this requirement could result in businesses having to include in their privacy policy a statement that they do not have actual knowledge that they are selling the personal information of minors, even if they already state that they do not sell the personal information of users generally. W222-10
  - We suggest revising the language to: "*State whether ~~the~~ a business that sells personal information has actual knowledge that it sells the personal information of minors under 16 years of age.*"

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

- § 999.313(c)(1) creates risks of innapprioate disclosure of information about a consumer in request to an unverified consumer request. Creating obligations in response to unverified requests is contrary to, and inconsistent with, the stature. The CCPA contemplates that unverified requests should be discarded precisely because they are unverified: "*A business is not obligated to provide information to the consumer pursuant to Sections…1798.105…if the business cannot verify… that the consumer making the request is the consumer about whom the business has collected information…*"
  - Practically, the very reason a business should discard an unverified request is to protect the consumer- the business is unable to verify the individual's identity and therefore should not act on requests related to that ocnsumer's personal information. And the statute creates a specific mechanism for opting-out of the sale of information. Collapsing verification and opt-out procedures is contrary to the statue and creates vectors for abuse. W222-11
  - TechNet recommends striking language in (c)(1) mandating that a request that fails verification be considered for disclosure of categories of personal information as follows, "*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).~~*"

- § 999.313(c) creates substantial additional burdens on top of already-burdensome "right to know" requirements included in CCPA and GDPR, by requiring companies to produce a customized response for each consumer. No other privacy regime in the world has a requirement like this. It is hugely burdensome and expensive, provides no corresponding benefit to the consumer, and is in any event unnecessary because the consumer can simply access the actual information. W222-12
  - We suggest that any of the following could lower the burden of this provision:
    - (a) An amendment to § 999.313(c) that would clarify that a company need not additionally fulfill a request to provide categories of information collected if it is also providing specific pieces of information.
    - (b) An amendment to § 999.313(c)(10) that would not require the additional pieces of information listed (categories of sources, business purpose, categories of parties to whom disclosed/sold and why) to be broken out for each category of information collected. W222-13
    - (c) An amendment to § 999.313(c)(9) expanding the circumstances in which a company could rely on a generic articulation of categories in the privacy notice, as opposed to a customer-specific feed. For example, the regulation could be broadened to clarify that a business may refer to its privacy policy when its response would be the same for "substantially all" or "most" consumers. W222-14
- We do appreciate the clarifications in § 999.313(c)(3) that create a new exception for responding to "right to know" requests, recognizing that some personal information is not searchable or stored in a reasonably accessible format. However, this exception should also apply to personal information that is not routinely linked to an individual consumer. These considerations should also apply to deletion requests in § 999.313(d)(3). W222-15
- Unfortunately, the elimination of the previous text in § 999.313(c)(3) would require businesses to provide access to information that could place their systems at risk. The previous text allowed a business to forgo disclosure if it "*creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks*". We request the reinstatement of this deleted text. This language should be included in the final regulations to protect both consumers and businesses. W222-16
- Also, regarding § 999.313(c)(3), we suggest clarifications on the conditions under which businesses should not be required to search for personal information in response to a right to know request. As currently written, the draft rules require a four-part test for which, in practice, no information will meet all four prongs- particularly given the requirement that the information be maintained "*solely for legal or compliance purposes*." W222-17
  - The statute and draft regulations currently lack sufficient clarity regarding how far the access rights extend, and as a result, business do not have clear guidance as to whether they must build new systems to reach anything that may technically be responsive. A clear regulation is necessary

to draw outer lines around the information a business must make available. Many businesses possess data that may technically fall within the CCPA's broad definition of "personal information," but that is not used in the ordinary course of business, such as log data, is not readily accessible, or has not been "collected." This is particularly true with data that the business has derived rather than collected or which may not be readily accessible. Requiring a business to identify, compile, and then make accessible such information has the adverse effects of forcing a business to face undue burdens in an effort to create new or more robust consumer profiles. This creates privacy and security concerns for consumers by associating more data with them than otherwise would be, as businesses will be required to build systems with more detailed consumer profiles and then send those profiles outside of the business.

- A regulation drawing clearer lines regarding the scope of the right to know will have pro-privacy and pro-security ramifications and will save businesses from having to face massive burdens and legal uncertainty. The following recommendation draws a clearer line while properly taking into account the statutory limitation that the business must have "collected" the personal information, and the statutory requirements the regulations consider burden and security. W222-17 (cont.)
- Accordingly, we recommend the following revision, "*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, networks, or consumers. In responding to a request to know, a business is not required to search for personal information ~~if all~~ that meets any of the following conditions provided the business describes to the consumer the categories of records that may contain personal information that it did not provide it because it meets one of the conditions stated below ~~are met~~:*

  a. The business does not maintain the personal information in a searchable or reasonably accessible format;
  b. The business maintains the personal information solely for legal or compliance purposes;
  c. The business does not sell the personal information and does not use it for any commercial purpose;
  d. The business does not associate the personal information with a consumer in the ordinary course of business; or
  e. The personal information was not collected from the consumer or a third party, but was instead derived internally by the business.
  ~~and~~
  ~~d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.~~

- TechNet appreciates the exclusion of biometric data in § 999.313(c)(4) and believes additional data types should be excluded from subject access request productions in order to provide businesses the necessary flexibility to navigate and mitigate tensions between subject access requests and the data breach statute. W222-18

- § 999.313(d)(1) requires that for any consumer making a deletion request, if a business cannot verify the consumers identity, the business must "*ask the consumer if they would like to opt out of the sale of their personal information and shall include either the contents of, or a link to, the notice of right to opt-out in accordance with section 999.306.*" We do not believe that deletion and opt out requests are the same requests and this conflates the two issues. As companies try to automate these processes this requirement increases the costs and burden, as this requirement applies to anyone whose identity cannot be verified. We request that that this requirement be removed from the draft rules and instead require a business to point the consumer to the privacy notice that explains how to exercise their privacy rights so that they can go through the processes that have already been designed. W222-19

§ 999.315. Requests to Opt-Out

- We continue to oppose the draft language in § 999.315(a), (d) that a business treat browser plug-ins or global device settings as valid requests to opt out of the sale of personal information). The CCPA emphasizes consumer choice. It specifically defines a mechanism, the "Do Not Sell" button, that businesses must make available to consumers on their Web sites to exercise their choices. It is not consistent with the statute to create this additional mechanism, nor is it clear that consumers, who use plug-ins, intend to opt out of CCPA sales. Codifying browser-based signals could also give significant power to browsers, who could unilaterally turn on "Do Not Sell" or even do it selectively for certain companies. We support an industry-based efforts to develop consistent technical signals for "Do Not Sell" technology, an effort that has been underway for over a year.
    - Uncertainty surrounding this technology will also make these privacy controls difficult to operationalize, leading to inconsistent approaches. There are different understandings of what constitutes a browser setting or plug-in and which mechanisms reflect genuine user intent, due to significant issues around reliability and authenticity of browser-based signals. Similarly, not every browser communicates clearly and reliably which users are California residents. There is still insufficient consistency and interoperability to make this a workable standard. W222-20
    - These types of privacy controls would also harm competition by favoring a few advertisers who have direct relationships with consumers and the ability to ask consumers to override browser- or device setting based opt-out requests. If consumers make a general decision to opt-out via a single setting, they will restrict the capacity of online advertisers without a direct consumer relationship to compete in the online advertising market. The dominance of a few advertisers can easily lead to lower revenues for online journalism and higher prices for businesses who seek to reach new consumers. The result is the availability of less free content online. Consumers will not be aware of these trade-offs when they click on a global device setting.
    - We strongly recommend any provision related to user-enabled priacy controls be removed from the draft regulations. In the event this requirement is not removed, we recommend delayed implementation until there is an interoperable standard that works for business and consumers in California. The Attorney General should work with the business community

and other interested stakeholders in finding a standard that could work for all involved. W222-20 (cont.)

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

- As noted previously in regards to the definition of affirmative authorization, the draft rules continue to envision a two-step process to opt-in to the sale of data, where the consumer requests to opt in to the sale of data and then confirms the opt-in. Multiple pop-ups and other prominent notices are highly likely to be noticed but can interrupt consumers' experiences. The more notifications presented to consumers, the less likely consumers are able to apprehend or absorb any one particular notice and make informed choices about their data. The more notices that companies display, the greater the chance of creating "click fatigue," whereby consumers just skip over the words and click through to continue using the service. We therefore suggest striking the reference to a "two-step" process. W222-21

§ 999.318. Requests to Access or Delete Household Information

- TechNet encourages modification of the definition of "household" to apply more broadly to shared identifiers rather than consumers of a household affirmatively determining to be sharing a house and a device. W222-22

§ 999.337. Calculating the Value of Consumer Data

- As noted in our comments in section § 999.307, we propose striking § 999.337, which describes the methods in calculating the value of consumer data. This requirement to disclose the value and methodology goes beyond CCPA statutory language. We urge that this requirement be struck from the draft regulations. W222-9 (cont.)

Conclusion

TechNet thanks you for taking the time to consider our comments on the proposed CCPA regulations. It is imperative for businesses and consumers in California that CCPA regulations move forward with the goal of providing clarity to the statute. We urge that any new requirements beyond those delineated in the statute be removed from the regulations or, at the very least, have a delayed effective date. Regulations should help facilitate compliance on the part of California businesses, while ensuring that consumers have clear expectations about what companies are and are not allowed to do with personal information.

If you have any questions regarding this comment letter, please contact Courtney Jensen, Executive Director, at [redacted] or [redacted].

Thank you,
Courtney Jensen
Executive Director, California and the Southwest
TechNet

From: Colin Smith
To: Privacy Regulations
Cc: Derek Schwede; Todd Smithline; [redacted]
Subject: Comments to Revised CCPA Implementing Regulations
Date: Tuesday, February 25, 2020 4:20:34 PM
Attachments: Smithline Group Comments to Revised CCPA Regulations 2020 02 25.pdf

Dear Sir/Madam,

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

Very truly yours,

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

Colin Smith
Associate
[redacted]

Smithline PC
300 Montgomery Street, Ste 1000
San Francisco, CA 94104
www.smithline.com
Internet and Software Lawyers

SMITHLINE PC

300 Montgomery Street, Su te 1000 San Franc sco, Ca forn a 94104
Phone: (415) 834 1700 Fax: (415) 834 1720
www sm th ne com

February 25, 2020

By email to privacyregulations@doj.ca.gov

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

Re: Comments to Revised CCPA Regulations

We write as members of a CCPA working group composed of California and national in-house and law firm attorneys.

We applaud the Attorney General's careful consideration of the first set of public comments to the regulations (running over 1,700 pages). The revised regulations bring significant clarity and practical guidance without eroding the privacy interests the CCPA is designed to protect. As a result, the revised regulations should significantly increase compliance by giving regulated entities a clear path to follow under a complex statute.

Please find below our comments on a few final issues raised by the revisions. Thank you again for your consideration of comments from a community dedicated to understanding and complying with the CCPA.

1. *Remove Restriction on "Cleaning or Augmenting Data" (§999.314(c)(3))*

a. Issue. Section 999.314(c)(3) prohibits service providers from "cleaning or augmenting data acquired from another source" in the course of building or improving their products. Given that these terms lack an industry-standard meaning and are not used elsewhere in the CCPA, they risk confusing businesses and service providers alike. Further, to the extent "cleaning" data encompasses activities such as correcting common postal addresses, this provision could prohibit activity that directly benefits consumers, and which may even be required under data accuracy requirements of the GDPR or other data privacy regimes. (We also note this provision refers to "data" and not "personal information" as regulated by the CCPA). W223-1

b. Request. We request that the Attorney General remove the prohibition on cleaning or augmenting data. While we agree that data usage for product improvements must preserve consumer privacy, that goal is already accomplished through the new profile-related restrictions in this section.

2. *Service Providers Cannot Police Opt-Out Compliance (§999.314(d))*

a. Issue. New subsection 999.314(d) requires the service provider to honor opt-outs received by the business. This is problematic because the business is the party with direct consumer relationships, making it responsible for providing consumer notices, responding to consumer requests and receiving and complying with opt-outs. The service provider may have little or no insight into the business's relationships with consumers or third-parties. Both at contract and at law, the service provider's role is to W223-2

process personal information *as instructed by the business*, and the business is responsible for ensuring that its instructions comply with the CCPA.

> ***Example***: A service provider offers a cloud platform that helps businesses manage consumer information such as email addresses. The platform includes self-serve features allowing the business to share that data with its *other* service providers, such as for marketing services. The provider of the platform simply transmits the data as directed by the business, but has no relationship with the consumers and no method to learn of, verify or comply with the opt-outs. Only the business can assess whether this sharing is a "sale" under the CCPA and whether the business has honored any opt-outs.

W223-2 (cont.)

As this example illustrates, we do not mean to suggest that a service provider may ignore a business's instructions, including if in furtherance of an opt-out, but merely that the service provider should not have an *independent obligation* to look through those instructions with respect to opt-outs or other requirements under the CCPA.

b. Request. We request that the Attorney General remove this new subsection. This standalone opt-out obligation with direct liability for service providers would blur the CCPA's core roles, cause service providers to second-guess businesses' instructions and likely violate existing service provider contracts.

3. *Clarify Scope of Verification Security Obligations (§999.323(e))*

a. Issue. §999.323(e) states: "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." While the surrounding section clearly relates to verification of consumer requests, taken out of context, the phrase "prevent the unauthorized access or deletion of a consumer's personal information" could arguably be seen as a general-purpose security obligation for businesses – an unexpected requirement that exceeds statutory scope and authorization.

W223-3

b. Request. Revise §999.323(e) as follows: "A business shall implement reasonable security measures to detect fraudulent identity-verification activity and to prevent the unauthorized access to or deletion of a consumer's personal information *in connection with the verification process*."

4. *Missing Elements in Privacy Policy Guidance? (§999.308(c))*

a. Issue. We appreciate the removal of most of the category-by-category disclosure requirements for privacy policies. However, it appears §999.308(c) is now missing the *general* requirement for privacy policies to disclose (1) the categories of sources from which personal information is collected and (2) the business or commercial purposes of collection or sale. Since these are requirements for privacy policies in the statute (see §110(c)(2)-(3)), their absence in the regulations is likely to cause confusion for businesses seeking implementation guidance.

W223-4

b. Request. Consistent with the statute, add the following to the disclosure requirements in §999.308(c)(1), between current subsections (d) and (e).

"e. Identify the categories of sources from which the personal information is collected."

"f. Identify the business or commercial purpose for collecting or selling personal information."

Smithline PC | 300 Montgomery Street, Suite 1000 | San Francisco, CA 94104 | (415) 834-1700

Thank you for your consideration of these comments and your ongoing efforts to finalize the regulations.

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

Very truly yours,

Derek Schwede

Derek Schwede
Principal
Smithline PC

Todd Smithline

Todd Smithline
Managing Principal
Smithline PC

Anna Westfelt

Anna Westfelt
Of Counsel
Co Head Data Privacy Practice
Gunderson Dettmer Stough Villeneuve Franklin & Hachigian, LLP

Lisa Babel

Lisa Babel
General Counsel
StreamSets, Inc.

Matthew Fischer

Matthew Fischer
Chief Privacy Officer
Snowflake Inc.

Mark Kahn

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

Audrey Kittock

Audrey Kittock
Corporate Counsel
Segment.io, Inc.

Judy Krieg

Judy Krieg
Partner, Privacy, Security and Information
Fieldfisher LLP

Eric Lambert

Eric Lambert
Division Counsel
Trimble Transportation

Xavier Le Henry

Xavier Le Hericy
Chief Privacy Officer
New Relic, Inc.

Lee Matheson
Associate
Crowell & Moring LLP

David Mitchell

David Mitchell
VP Legal
Demandbase, Inc.

Diane Nahm

Diane Nahm
Head of Legal
Miro

Diana Olin

Diana Olin
Assistant General Counsel
Sumo Logic, Inc.

Jeffrey L. Poston

Jeffrey L. Poston
Partner
Crowell & Moring LLP

Gabriel M. Ramsey
Partner
Crowell & Moring LLP

Cindy Rosser

Cindy Rosser
Legal Director, Product, IP & Regulatory Affairs
DocuSign, Inc.

Brad Simon

Brad Simon
Partner
Brad Simon Law

Annie Sun

Annie Sun
In house Attorney

Ted Torous
Associate General Counsel
StreamSets, Inc.

Jarno Vanto

Jarno Vanto
Partner
Crowell & Moring LLP

Amanda Weare

Amanda Weare
Associate General Counsel
Collibra

Mark Webber

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

From: Townley, Katie
To: Privacy Regulations
Cc: Hutnik, Alysa; Myers, Lauren
Subject: QuinStreet, Inc. Comment to Revised Proposed CCPA Regulations
Date: Tuesday, February 25, 2020 4:19:12 PM
Attachments: image001.png
QuinStreet, Inc. Comment to Revised Proposed CCPA Regulations.pdf

---

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

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

Katie

KATIE TOWNLEY
Senior Associate

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

WWW.KELLEYDRYE.COM

[redacted]

February 25, 2020

Via Online Submission – PrivacyRegulations@doj.ca.gov

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

Re: Revised Proposed California Consumer Privacy Act Regulations

QuinStreet, Inc. ("QuinStreet") is pleased to submit this comment in response to the revised California Consumer Privacy Act ("CCPA") regulations released on February 10, 2020 (the "Revised Regulations").

One deletion, perhaps an inadvertent one, in the Revised Regulations has prompted significant concerns. **We urge the Attorney General to reinstate Section 999.313(c)(3)[1] (the "Security Risk Regulation"). Failure to do so (or to otherwise clarify the rights of consumers to data privacy and security, and how companies should meet their related obligations) puts consumers at risk of not only data theft but also physical harm.**

QuinStreet is a leading provider of "search and compare" performance marketing services (NASDAQ: QNST). With headquarters in Foster City, California, QuinStreet takes pride in the integral role it plays in the California economy, generating over $500 million in revenue annually and employing over 600 people. W224-1

An Express Risk-Based Exemption to "Right to Know" Disclosures Should be Reinstated in Section 999.313(c)(3)

The Security Risk Regulation prohibited businesses from disclosing specific pieces of personal information in response to a consumer's "verified request to know"[2] if such a disclosure created "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."[3]

---

1 As drafted in the regulations published on October 11, 2019.

2 The challenges with verification, especially for businesses that have not previously had to do it, are described further below in this comment.

3 *See* Cal. Code Regs. tit. 11, § 999.313(c)(3) (proposed Oct. 11, 2019). The Revised Regulations remove this risk-based exemption and restrict denials of a consumer's request to know to the following circumstances: (1) the requester's identity cannot be "verified"; (2) a particular subset of personal information is at issue (*e.g.*, personal information that triggers a security breach notification under Cal. Civ. Code § 1798.82); (3) the disclosure creates a legal conflict; (4) another CCPA exception applies; or (5) the business (a) does not maintain the personal information in a searchable or reasonably accessible format, (b) maintains the personal information solely for legal or compliance purposes, (c) does not sell the personal information or use it for any commercial purpose, *and* (d) describes to the consumer the categories of records that may contain this personal information. *See* Cal. Code Regs. tit. 11, § 999.313(c) (proposed Feb. 10, 2020).

We are mindful of the view of the ACLU and other consumer advocates that the Security Risk Regulation could function as an excuse for businesses to deny access requests. Based upon our actual experience with consumer data and technology over the last 20 years, that view is not only misplaced, but inadvertently places consumers at much greater risk of real harm, including domestic violence. It also misunderstands the benefits to consumers and the burdens on businesses, the latter of which will result in additional unnecessary risks.

A. The Attorney General Recognizes the Importance of Risk-Based Discretion

The initial regulations reflected the Attorney General's recognition of the disclosure risk related to consumer personal information. The Initial Statement of Reasons ("ISOR") explained that Sections 999.313(c)(3) and 999.313(c)(4) "balance the consumer's right to know, *with the harm that can result from the inappropriate disclosure of information*."[4]

W224-1 (cont.)

These risks are real; failing to mitigate them would be consequential. In 2019, approximately 1,500 security breaches were reported in the United States. Those breaches exposed over 705 million non-sensitive and 164 million sensitive records.[5]

Notably, not all security breaches begin and end with the small subset of identifiers set forth in California's security breach notification law.[6] Phishing attacks are on the rise, and fraudsters often start with seeking and accumulating personal information from some businesses to support identity theft attempts at others.[7] The number and scope of phishing attempts will increase if businesses do not have the tools necessary to combat them, which includes reasonable discretion to limit the specific pieces of information disclosed in response to a verified request due to security concerns.

Consumer privacy advocates[8] might well ask, "Why can't businesses subject to the CCPA just spend more on tools to solve the problem?" The answer is threefold: (1) math, (2) security is hard, and (3) some consumer data is different.

Math. Consumer information security risks cannot be eliminated; they can only be mitigated.[9] Business cannot simply spend their way out of the problem; there is no 100% effective solution.

---

4 Initial Statement of Reasons, Proposed Adoption of California Consumer Privacy Act Regulations, 18 (2019) (emphasis added).

5 Identity Theft Resource Center, *End-of-Year Data Breach Report* (2020), *available at* https://www.idtheftcenter.org/2019-end-of-year-data-breach-report-download/.

6 *See* Cal. Civ. Code § 1798.81.5(d).

7 *Id.* at 16 (noting that, "[a]lthough initial access may be gained to non-sensitive accounts, if the same credentials are used for other accounts both sensitive and non-sensitive, this can lead to access to a wide-variety of personal information"); *see also* Steve Ranger, *Phishing Attacks Are a Worse Security Nightmare than Ransomware or Hacking*, ZDNet (Apr. 3, 2019), *available at* https://www.zdnet.com/article/why-phishing-emails-are-still-your-biggest-security-nightmare/.

8 Which QuinStreet believes includes itself and substantially all other reputable business stewards of consumer data.

9 Risk theory is beyond the scope of this comment. *But see, e.g.*, https://en.wikipedia.org/wiki/Risk_control_strategies.

Some consumer information will inevitably end up being delivered to the wrong party; it's just math certainty.[10]

Security risks created by the European Union's General Data Protection Regulation ("GDPR") are instructive. Only a few months after GDPR took effect, Carnegie Mellon professor and tech executive Jean Yang tweeted that, after gaining access to her Spotify account, hackers were able to request access to all of the information that Spotify retained about her, including her home address, credit card information, and music streaming history.[11] Not all of this data would fit within Section 999.313(c)(4)'s[12] disclosure exemption, yet it may raise the risk of identity theft to a consumer if it allows hackers to satisfy verification requests at other businesses.

Oxford PhD student James Pavur exposed additional GDPR security vulnerabilities. He made 150 access requests to a variety of entities, from non-profits to Fortune 500 organizations, for the personal information of his fiancée.[13] Using a rudimentary attack strategy based solely on publicly available information about her, Pavur received personal information from almost three-quarters of the entities contacted.[14] **Importantly, Pavur was easily able to satisfy the verification requirements of those entities that took "verification" steps**.[15] W224-1 (cont.)

Pavur was then able to combine the information received from some entities with information received from others to access data from an additional set of entities.[16] In total, he was able to collect 60 distinct pieces of personal information about his fiancée, including her previous residential addresses, travel itineraries, hotel stays, credit card transactions, and even her full Social Security number.[17] As a result, Pavur has suggested that legislators "assur[e] businesses that rejecting a suspicious right of access request in good faith will not later result in prosecution if it turns out that the request originated from a legitimate but suspiciously-behaving data subject."[18]

---

[10] Even lay readers may be familiar with claims of "two nines availability" (*e.g.*, a system that works correctly 99% of the time). Yet a system operating year-round with 99% availability will still fail almost four full days per year. *See, e.g.*, https://en.wikipedia.org/wiki/Availability.

[11] Kashmir Hill, *Want Your Personal Data? Hand Over More Please*, N.Y. Times (Jan. 15, 2020), *available at* https://www.nytimes.com/2020/01/15/technology/data-privacy-law-access.html.

[12] This section prohibits disclosure of "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, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics."

[13] James Pavur & Casey Knerr, *GDPArrrrr: Using Privacy Laws to Steal Identities*, Blackhat USA 2019 Whitepaper, 4 (Aug. 8, 2019), *available at* https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf.

[14] *Id*. at 5.

[15] *Id*. at 5–7.

[16] *Id*. at 4.

[17] *Id*. at 7.

[18] *Id*.

We think that Pavur's concern is correct, but his recommendation rests on a reasonable but invalid assumption: that a "suspicious-looking data subject" can be easily identified.

Security Is Hard. Financial institutions, governments, and others have invested billions of dollars over decades to mitigate the risk that someone is not who they say they are. The scale of the investment relates to the type of data at risk (*e.g.*, financial or health information). Practices have evolved over time to reflect consumer preferences.[19]

The Revised Regulations, however, suddenly saddle all businesses with indeterminate verification obligations. As Pavur demonstrated and others have discussed, verification does not produce security.[20] A one-size verification method cannot fit all; research has shown that businesses employ a variety of verification methods with varying degrees of security and effectiveness.[21] Many businesses that have never before had to validate or verify a consumer will be relying new tools and solutions; ones that may be implemented incorrectly or be subject to security risks in any event.[22]

W224-1 (cont.)

Moreover, verification is not authentication; it cannot guarantee that requesting consumers are who they claim they are.[23] As recognized by the National Institute of Standards and Technology:

> Digital identity is hard. Proving someone is who they say they are – especially remotely, via a digital service – is fraught with opportunities for an attacker to successfully impersonate someone. As correctly captured by Peter Steiner in *The New Yorker*, "On the internet, nobody knows you're a dog."[24]

Some Data Is Different. As outlined above, financial institutions and others have spent billions of dollars over decades trying to mitigate consumer data disclosure risks. But, in the context of the CCPA, in the absence of the Security Risk Regulation or other guidance, all of these efforts will be sublimated to producing the requested data to the requesting consumer.

The ACLU, Privacy Rights Clearinghouse, and other consumer advocates are keenly aware of the risks posed by producing personal information to the wrong person. For example, the New York

---

[19] Five years ago, most consumers would have been puzzled by "two-factor authentication." Such practices are now taken for granted in many consumer data access situations.

[20] *See* Mariano Di Martino *et al.*, *Personal Information Leakage by Abusing the GDPR "Right of Access,"* Fifteenth Symposium on Usable Privacy and Security (2019), *available at* https://www.usenix.org/system/files/soups2019-di_martino.pdf.

[21] *Id.*

[22] *See* Annie Bai & Peter McLaughlin, *Why the CCPA's "Verified Consumer Request" Is a Business Risk*, IAPP (2019), *available at* https://iapp.org/news/a/verified-consumer-request-dont-naively-slip-into-the-crack-or-is-it-a-chasm/.

[23] *See* GAO, *Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes*, No. GAO-19-288 (May 2019), *available at* https://www.gao.gov/assets/gao-19-288.pdf.

[24] *See* Paul A. Grassi *et al.*, *Digital Identity Guidelines*, NIST Special Publication 800-63-3 (June 2017), *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

Times recently ran a series on the risks created by disclosures of geolocation data.[25] With the proposed omission of the Security Risk Regulation, the Attorney General is on the verge of creating similar risks for California consumers.

Creating this risk is unnecessary, particularly after reflecting on how consumer information is obtained, transferred, and revealed. For example, in most cases the source of consumer contact information is the consumer. This information includes name, email and physical address, and phone number (collectively, "Contact Information") and is typically provided by the consumer.

Consumers conducting "search and compare" activities online[26] also typically elect to provide relevant information. This information includes dates of travel, outstanding loan or credit card balances, etc. (collectively, User-Provided Attributes). As is the case with Contact Information, User-Provided Attributes are typically provided by the consumer.

W224-1 (cont.)

There are two categories of information that do not typically come from consumers: automatically-collected technical information (*e.g.*, IP Address, mobile phone operating system type) and third-party data (*e.g.*, credit reports, phone number validation). Technical information is not typically used to identify the consumer, and the consumer may have the ability to eliminate or obscure that information as they configure their device. Third-party data is typically only used to validate relevant information that is required to qualify the consumer to receive an offer (*e.g.*, mortgage or credit card).

We respectfully submit that providing consumers with consumer-provided information, particularly Contact Information, is silly to dangerous. What interest is served by a consumer asking "What is my name [or phone number or email or physical address]?" Presumably, that information is known to the consumer. If the applicable business maintains a directory of consumer information that needs to be correct (*e.g.*, credit reporting agencies), they will tend to have consumer verification and information update processes that are appropriately robust. But businesses not in that line of work will have no experience with verification and related techniques.

To make the resulting risks concrete, consider the following: Consumer A submits a CCPA "right to know" request. The receiving business "verifies" Consumer A via some method. The business determines it has a phone number, email address, and physical address for Consumer A.

What possible benefit is it to Consumer A to "receive" that information? Consumer A presumably knows their own phone number, email address, and physical address. **The only time that would not be the case is when Consumer A is not who they claim to be.**[27]

---

[25] *See* Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), *available at* https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

[26] For flights, hotels, financial products and services, etc.

[27] In the best case "Consumer A" would be the proverbial internet dog. We are worried about all other cases.

And the most dangerous cases are likely to be domestic violence and similar situations. As EPIC has observed:

> Many privacy problems, such as identity theft, are harms experienced by the public from general criminal behavior. But domestic violence victims are already being specifically singled out by a particular aggressor. This aggressor is able to take advantage of the general lack of protection for personal information in our society. Furthermore, this aggressor is familiar with many of the intimate details of the victim's life. An abuser can violate privacy by sharing these details, or by using them to gain more information on a victim.[28]

This is no business excuse; it is a real risk with real consequences. It is not a risk amenable to monetization. No government nor consumer advocacy organization is going to write a check to a business that, acting in good faith, inadvertently exposed a consumer to harm.[29] W224-1 (cont.)

The use of a risk-based approach is clearly necessary to establish, monitor, and revise (including over time) verification and information-sharing processes. Accordingly, we urge the Attorney General to either (1) re-institute the Security Risk Regulation, or (2) clarify that Contact Information (and, optimally, other User-Provided Attributes) can be provided to the requesting consumer as categories of information, consistent with text of the CCPA,[30] as opposed to actual data whose revelation serves no purpose for the actual consumer, but could pose the risk of someone else obtaining that data on their behalf.

B. Hindsight Is Insufficient

The Revised Regulations do not address *potential* harms. Instead, they identify issues that would only arise *after* a breach occurred (*e.g.*, defending legal claims or complying with a regulatory inquiry).[31] The existing exemptions, like many well-intentioned legal efforts, do not enable a proactive approach. In the context of physical security, they must.

Further, the types of personal information identifiers that may trigger a security breach continue to evolve. The California legislature has recognized that fraudsters continue to evolve and thus, legislators continue to update the security breach notification statute to expand the list of personal information that would trigger a reportable breach. For example, the legislature amended the

---

[28] *Domestic Violence and Privacy*, Electronic Privacy Information Center, *available at* https://epic.org/privacy/dv/.

[29] Nor should they. The mutual goal here should be to avoid the problem, versus trying to "solve" it.

[30] Per the CCPA, the legislature agreed that categories of personal information include identifiers (*i.e.*, Contact Information); categories of personal information described in Cal. Civ. Code § 1798.80(e); characteristics of protected classifications under California or federal law; commercial information; biometric information; internet or other electronic network activity information; geolocation data; audio, electronic, visual, thermal, olfactory, or similar information; professional or employment-related information; education information; and inferences drawn from any such information. *See* Cal. Civ. Code § 1798.140(o). QuinStreet believes that, in the context of providing security, it would be appropriate to respond to a consumer's request to know certain sensitive information, such as Contact Information, on a category basis. *Compare* Cal. Code Regs. tit. 11, § 999.313(c)(1) (proposed Feb. 10, 2020).

[31] *See* Cal. Civ. Code § 1798.145.

statute in 2013, to require notification for breaches involving a username or email address in combination with the password or security question and answer that would permit access to an online account. The legislature cited "the increasing frequency of" security breaches affecting consumer usernames and email addresses as the impetus for the change.[32]

As the California legislature understood, the personal identifiers that contribute to security breaches change over time. Businesses must have the ability to respond to these changes (including changes to consumer preferences) on a daily basis to detect and prevent identity theft and fraud. Providing businesses with limited-to-no discretion, and allowing denial of "verified" requests to know based upon a limited statutory list of current identifiers, will not enable continued consumer protection by those who are best positioned to provide it.

W224-1 (cont.)

The Security Risk Regulation would allow businesses (including as guided by future enforcement) to use an evolving, risk-based approach to address the potential threats associated with disclosing certain types of consumer personal information. By giving businesses the opportunity to prevent disclosures that "create[] a substantial, articulable, and unreasonable risk to the security of" a consumer's personal information, the Security Risk Regulation recognized businesses', and, importantly, a business's human staff members', role in identifying and avoiding potential threats – steps that are essential to ensuring reasonable data security.

Businesses are in the best position to know the personal information they have and the measures available to secure that information. Business capabilities and consumer preferences change daily; regulations and statutes cannot be expected to evolve in lock-step.

The Security Risk Regulation provided businesses with the requisite discretion to limit the disclosure of personal information under specific, yet serious, circumstances – *e.g.*, a substantial, articulable, and unreasonable security risk. This provision is narrowly tailored to the cognizable risks associated with disclosure. In addition, as the ISOR notes, it strikes the appropriate "balance" between data security and consumer rights. Absent such express discretion, businesses will inevitably err on the side of disclosure (whether due to "verification" failures or otherwise). The consequences may not be merely financial; they include physical harm or worse.

We do not believe that your office or the State of California intended that outcome. Section 999.313(c)(3) was an important provision, and we urge that it be reinstated.[33]

* * *

We appreciate the opportunity to submit these comments. QuinStreet recognizes that the Revised Regulations, and Sections 999.305(d) and 999.315(f) of the Revised Regulations in particular, incorporate some of the recommendations that QuinStreet and other commenters made during the

[32] *See* S. Comm. on the Judiciary, 2013–2014 Cong., S.B. 46, at 2 (2013).

[33] It is not clear that any remedy other than reinstating the Security Risk Regulation or providing discretion to businesses to respond to requests to know on a category basis is practicable. If a business does not have the requisite discretion, releases information to the wrong person, and someone is hurt or killed, will the legislature indemnify the business? We think not. Moreover, the foregoing would not be a problem that could be solved with money. We urge your office to join us in seeking to avoid such problems.

initial comment period,[34] and requests that your Office again consider the real and unfortunate effects that the Revised Regulations will have on consumers and businesses alike. Please do not hesitate to contact us if you have any questions.

Respectfully submitted,

Martin Collins

Martin Collins
Senior Vice President and General Counsel
QuinStreet, Inc.
950 Tower Lane
Foster City, CA 94404

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

[34] *See* CCPA_45DAY_01509 through CCPA_45DAY_01521.

From: [redacted]
To: Privacy Regulations
Cc: [redacted]
Subject: Proposed Changes to the California Consumer Privacy Act (OAL File No.2019-1001-05)
Date: Tuesday, February 25, 2020 4:19:12 PM
Attachments: CCPA REGULATION COMMENT.pdf

Dear California Department of Justice,

Please see the attached PDF file for our written comments on the proposed changes to the rulemaking file for the California Consumer Privacy Act (OAL File No.2019-1001-05). We appreciate the Department's review and considerations.

Warm regards,

Liv Erickson

California Department of Justice
February 25, 2020

Re: *Comment on the Proposed Changes to the California Consumer Privacy Act (OAL File No. 2019-1001-05)*

The California Consumer Privacy Act should include explicit language that accounts for the case in which an authorized agent is acting on the behalf of a consumer who has passed away. This is a situation where the authorization of a third party agent to act on behalf of a user is implicit, and should be considered a lawful situation through which a consumer's data may be handled by an authorized agent. Because the underlying legislation authorizing the CCPA does not explicitly define the cases in which an agent can be authorized, we believe that this is a valid interpretation of the text and should be included in the regulation updates.

Based on our fellowship research with the Aspen Institute at the Aspen Technology Policy Hub, we respectfully suggest the following for your consideration:

I. Rights to request or delete data by an authorized agent should be expanded to apply to court-appointed executors in the event that a consumer dies intestate, or to an explicitly-named custodian as specified through a consumer's will or trust. As written, the proposed changes to section § 999.326 would make it more difficult for court-appointed agents to act on behalf of a deceased consumer. Therefore, sections (b) and (c) should be updated to include explicit language to support CCPA requests on behalf of a consumer posthumously. W225-1

II. The newly added section (e) in § 999.326 should be updated to allow use of information to the extent that it allows an authorized agent to manage a deceased consumer's estate. As written, this section would make it difficult for an authorized agent to manage a deceased user's digital assets. Section (e) should include an explicit approval to the activities that are required of an authorized agent to manage a deceased user's property. W225-2

Extending Authorized Agent Rights to Executors of an Estate

While some consumers may grant a power of attorney to act on their behalf, in practice, this is not representative of how the general population plans for incapacitation. In practice, 56% of Americans die without a will or trust established[1] and their estate executors are court-appointed under intestate succession laws. In these instances, a power of attorney document may not have W225-1 (cont.)

[1] Gallup, 2016: https://news.gallup.com/poll/191651/majority-not.aspx

been created, but an executor of an estate should be able to file requests under CCPA in order to effectively manage the decedent's online data that is held by online companies.
The CCPA should cover a wider range of authorized agents who can act on behalf of a user. For example, an estate's executor should be able to file requests under the CCPA on behalf of the decedent they represent. The existing text of the CCPA rightfully considers the case where an authorized agent may be acting on behalf of a deceased or incapacitated consumer, as stated in § 999.326 (b).[2]

The presumed intent of this section is to facilitate access to a consumer's information when that user has authorized a fiduciary agent under a power of attorney[3] in preparation for posthumous estate management, but the current scope is insufficient. By explicitly limiting the mechanic by which a user can authorize an agent to be restricted to the scope of the power of attorney, the current text excludes the other ways that an agent could be legally authorized on a consumer's behalf.

W225-1 (cont.)

To include conservators as authorized agents within the context of the CCPA, we suggest the following changes to § 999.326 (b) and (c):

> (b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4000 to 4465 or is acting as the conservator of an estate pursuant to Probate Code sections 2400-2595.
>
> (c) A business may deny a request from an authorized agent that does not submit proof that they have been authorized ~~by the consumer~~ to act on ~~their~~ behalf of the consumer through direct authorization by the user or through a court order.

§ 999.326(e) Exemptions for Authorized Agents Managing Estates

Section (e) should be expanded to allow authorized agents to request information as required to manage a user's estate upon their death. The phrase '*to fulfill the consumer's requests*' implies that there is an understood need for agents to act on behalf of a consumer who is unable to act on a request directly, but in the event of an intestate death the consumer's request may be implicit rather than explicitly requested. Alternatively, a consumer may have granted power of attorney to an authorized agent, but not explicitly stated how their data should be managed or destroyed.

W225-2 (cont.)

[2] "*Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4000 to 4465.*" - *California Civil Code § 999.326 (b)*
[3] California Probate Code 4120 - 4130

As currently written, section (e) would prohibit a conservator of an estate from using the information to resolve an estate after a consumer has passed away if the death was intestate, but online providers increasingly hold valuable data related to a consumer's property. Section (e) should recognize this as a valid motivation of an authorized agent to request data from a consumer when the request is made posthumously. We propose the following changes to section (e):

W225-2 (cont.)

> (e) An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purpose other than to fulfill the consumer's requests, to resolve the estate of a deceased user, for verification, or for fraud prevention.

Appendix A includes two additional modifications that should be made to reflect the case where authorized agents are acting on behalf of deceased users in the event that the above changes are considered and accepted.

We appreciate the Department's time in reviewing the comments and proposal to updates to the California Consumer Privacy Act and are happy to be in further contact about our proposed changes.

Regards,

Liv Erickson
[redacted]

on behalf of:

The Digital Afterlife Project
Liv Erickson
Cecilia Donnelly Krum
Matthew Schroeder

Appendix A

Additional language changes to reflect authorized agents of deceased users

§ 999.301(c) - The definition for 'Authorized agent' should be expanded to include legal representatives acting on behalf of a deceased user in both intestate cases and when taken as part of a fiduciary duty through resolution of an estate, trust, or will of a decedent. W225-1 (cont.)

§ 999.315(g) - Authorizations should not require a signed document from the consumer if the authorized agent is authorized through a court order on behalf of a deceased consumer W225-3

From: Kevin McKinley
To: Privacy Regulations
Subject: Internet Association Comments on Modified Proposed CCPA Regulations
Date: Tuesday, February 25, 2020 4:18:11 PM
Attachments: IA Comments on Modified CCPA Regulations.pdf

Privacy Regulations Coordinator:

I have attached Internet Association comments on the modified proposed CCPA Regulations.

Thank you,

--

Kevin McKinley
Director, California Government Affairs
O [redacted]

INTERNET ASSOCIATION
1303 J Street, Suite 400, Sacramento, CA 95814

CCPA Text of Modified Proposed AG Regulations
Discussion Draft: IA Comments

Internet Association ("IA") appreciates the opportunity to review and provide the Attorney General's Office ("AGO") feedback on the Text of Modified Regulations for the California Consumer Privacy Act ("CCPA") Regulations ("Modified Regulations"). IA is the only trade association that exclusively represents leading global internet companies on matters of public policy.[1] Our mission is to foster innovation, promote economic growth, and empower people through the free and open internet. We believe the internet creates unprecedented benefits for society, and as the voice of the world's leading internet companies, IA works to ensure legislators, consumers, and other stakeholders understand these benefits.

IA members are committed to providing consumers with strong privacy protections and control over personal information, as well as to compliance with applicable laws, and advocates for a modern privacy framework in the IA Privacy Principles.[2] Internet companies believe individuals should have the ability to access, correct, delete, and download data they provide to companies both online and offline. It is essential that the U.S. enact a comprehensive, federal privacy law that provides Americans consistent protections and controls regardless of where they live, work, or travel.

This submission marks the third time IA has weighed in on the rulemaking process for CCPA. As expressed in IA's comments submitted during the initial drafting period for these regulations,[3] IA hoped that the AGO would use the regulations as an opportunity to clarify the CCPA in ways that would promote strong consumer privacy protections and businesses' ability to comply with the statute's legal requirements. IA is encouraged by the important clarifications and simplifications reflected in the Modified Regulations. However, many of IA's concerns remain about confusing and unnecessary new obligations for businesses that lack justification in the form of meaningful privacy protections for consumers.

It is critical that the final CCPA regulations create clarity regarding business obligations for compliance to fill the gaps in CCPA text, without requiring significant new actions that go beyond the Legislature's original intent for CCPA. This is particularly important now that CCPA has taken effect and enforcement will begin mere months after final regulations will be published.

---

[1] IA's full list of members is available at: https://internetassociation.org/our-members/.
[2] IA Privacy Principles for a Modern National Regulatory Framework, available at: https://internetassociation.org/files/ia_privacy-principles-for-a-modern-national-regulatory-framework_full-doc/ (last accessed November 25, 2019).
[3] IA Comments on CCPA Initial Rulemaking begin at p. 857 of the CCPA Public Comments available at: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf (last accessed November 25, 2019).

Section I. General Comments

IA would like to reiterate some of the high level concerns previously raised in our comments to the initial Proposed Regulations as the changes in the Modified Regulations do not fully address these issues:

1. **The Modified Regulations introduce new requirements after the effective date of CCPA.**

The CCPA's provisions became operative on January 1, 2020 pursuant to Cal. Civil Code Section 1798.198(a). Enforcement actions may be brought beginning on July 1, 2020.[4] The has state that it AGO may bring enforcement actions for non-compliance with CCPA for actions going back to the January 1, 2020 effective date, regardless of whether the final regulations were available at the time the violation occurred. It seems unlikely that the final regulations will be ready in a time frame that allows adequate time for compliance before the enforcement date of July 1, 2020.

On January 1, 2020, months of planning culminated in the launch of numerous new privacy notices, opt-out links, and mechanisms for accessing, downloading, or deleting data as a result of the CCPA. Implementation of CCPA, however, was uneven and inconsistent as a result of drafting issues when CCPA was passed and the lack of regulations to guide and inform implementation. Now that the implementation of CCPA has been achieved, it is time to focus on making sure it works properly and fine tune implementation. It is not the time for Modified Regulations to introduce new requirements with little warning.

As IA noted in its comments to the Proposed Regulations, putting aside the wisdom of the implementation schedule in CCPA,[5] the reality is that businesses subject to CCPA began assessing compliance needs and developing the required new tools, such as the capability to opt-out of sale, many months, if not more than a year, ago to work toward the January 1, 2020 effective date. Significant resources have already been put against understanding the legal requirements of the statute as they apply to a given business; hiring and training necessary staff across functional areas; and designing and coding a complex set of new capabilities. The implementation schedule in CCPA only makes sense to the extent that the AGO reads the requirements for regulations narrowly, as providing clarifications and detail consistent with the

[4] Cal. Civ. Code § Section 1798.185(c). The August 2018 amendments (S.B. 1121) to CCPA revised the original time frame in the statute by giving the AGO more time to prepare the regulations, at the AGO's urging, thus creating a framework where the CCPA law would become operative before the AGO would be required to deliver final regulations.

[5] Though by comparison, it is notable that the EU General Data Protection Regulation ("GDPR"), which built on the requirements of its predecessor, the EU Data Protection Directive (adopted in 1995), allowed covered entities two years from publication of the final text of the Regulation to the effective date.

existing requirement as necessary to implement the requirements of the law.[6] Such an approach would also be most consistent with the rulemaking mandate in the CCPA (as originally passed and as amended by A.B. 1355) which only allows "additional regulations as necessary to further the purposes of th[e] title"[7] and California law governing the rulemaking process.[8]

While the Modified Regulations make important improvements to the Proposed Regulations, it is still the case that they create new obligations beyond those contemplated in the text of the CCPA.[9] IA reiterates its comments challenging the legal authority to impose new requirements through the regulations[10] and whether such requirements satisfy the thresholds of California administrative law.

IA Recommendation: The AGO should take a fair and reasonable approach to regulations by only adopting rules that are provided for in CCPA's rulemaking mandate, reasonably necessary, [11] and for which CCPA has already provided businesses with fair warning of the potential requirements in order to make the current implementation schedule for CCPA as beneficial to consumers as possible. IA provides detailed recommendations and proposed changes in *Section II: Specific Provision*s of these comments.

2. **The Modified Proposed Regulations exceed the legal authority of the AGO by altering, amending, or enlarging the CCPA, and failing to meet other requirements of California administrative procedure.**

In IA's comments to the Proposed Regulations, numerous examples were given of the ways in which the Proposed Regulations introduce new requirements, beyond the scope of CCPA, for which there is no reasonable necessity, and/or fail to meet other requirements of California's statutes and regulations for administrative procedure.[12] Many of the examples cited in IA's

[6] This approach to drafting the implementing regulations for CCPA would also be most consistent with the expectations of the California Legislature which expected that the CCPA would set the deadlines and core provisions for compliance with CCPA. The Senate Judiciary Bill Analysis stated, "[t]hese provisions provide clear guidance on the basics for ensuring compliance." Senate Judiciary Committee Bill Analysis, p. 19 (June 25, 2018). Available at: https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375 (last accessed November 19, 2019).
[7] Cal. Civ. Code § 1798.185(b)(2)(as amended by A.B. 1355).
[8] Rulemaking is governed by the California Administrative Procedure Act ("APA"), Government Code § 11340 *et seq*. Rulemaking must also comply with regulations adopted by the Office of Administrative Law ("OAL"), California Code of Regulations, Title 1, §§ 1-120.
[9] *See* Section II, *infra*, for a further discussion of the manner in which the AGO conflicts with and/or enlarges the requirements of the CPPA in the Modified Proposed Regulations.
[10] *See* Section II, *infra*, for arguments that new requirements exceed the AGO's authority.
[11] Cal. Gov. Code § 11349(a).
[12] Cal. Gov. Code § 11340 *et seq*. California Code of Regulations, Title 1, §§ 1-120. Cal. Gov. Code § 11342.2 states, "Whenever by the express or implied terms of any statute a state agency has authority to

comments remain in the Modified Proposed Regulations and are noted below in Section II. Specific Provisions, including obligations to accept notice of a consumer request to opt-out of sale via device or browser settings; to monitor not just "designated methods" for consumers to make requests, but all potential methods; to track and report publicly on metrics related to consumer requests; to calculate value of consumer data and disclose that in connection with financial incentives; and more.

IA Recommendation: The AGO should substantially revise the Modified Proposed Regulations to bring them more clearly within the authority of the rulemaking powers granted by the CCPA, to ensure consistency with the clear terms of the CCPA, and to abide by the APA and its regulations. This should include another notice and comment period due to the substantial changes to the Modified Proposed Regulations,[13] a new ISOR that appropriately considers reasonable alternatives,[14] and a new SRIA based on accurate understandings of the business impact of the regulations where they deviate from the requirements of the CCPA.[15]

3. The Modified Proposed Regulations place unnecessary burdens on consumers and businesses.

The Modified Proposed Regulations impose new requirements, beyond those required by the CCPA, which will impose unnecessary burdens on consumers and businesses. These unnecessary burdens undermine the statutory intent of the CCPA, by making it more difficult for consumers to understand and exercise rights over their data created by CCPA. The unnecessary burdens to business introduce new requirements without justification, require duplicative processes, enlarge obligations contained in the CCPA, make it more difficult for businesses to comply with the requirements of the CCPA, and expand the costs of compliance far beyond what was contemplated in the SRIA prepared in connection with this rulemaking process.

---

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."

[13] Cal. Gov. Code § 11346.8(c)(restricting the ability of an agency to adopt regulations with "nonsubstantial changes" from those noticed to the public. Title 1, Section 40 of the California Code of Regulations defines "nonsubstantial changes" to mean those that "clarify without materially altering the requirements, rights, responsibilities, conditions, or prescriptions contained in the original text." 1 C.C.R. § 40).

[14] Cal. Gov. Code § 11346.2(b)(4).

[15] Cal. Gov. Code §§ 11346.3 & 11346.36 set forth the requirements for the financial analysis for a Proposed Regulation. Due to the substantial deviations from CCPA and the baseline regulatory measures that purported to form the basis of the SRIA that was conducted, a new SRIA should be prepared that satisfies the requirement that "[t]he baseline for the regulatory analysis shall be the most cost-effective set of regulatory measures that are equally effective in achieving the purpose of the regulation in a manner that ensures full compliance with the authorizing statute or other law being implemented or made specific by the Proposed Regulation." Cal. Gov. Code § 11346.3(e).

IA Recommendation: The AGO should substantially revise the requirements of the Modified Proposed Regulations to remove unnecessary burdens on business and to ensure that consumers benefit from.

Section II. Specific Provisions of Modified Proposed Regulations

§ 999.301 Definitions

- **(a) "Affirmative Authorization"** requires that consumers undergo a two-step process to indicate and then confirm their request to opt-in to sale. This two-step process introduces unnecessary friction to consumers, as well as potential risks. For example, a consumer may believe that after completing step one of the process that they have successfully performed the task and leave the process. This will result in the consumer's intent going unfulfilled without their knowledge, and create a potential limbo state for the business which may be unsure how to treat a consumer who has initiated but not completed a process. It is important that consumers understand the significance of the action they intend to undertake, which is why CCPA requires clear consumer notices and the Modified Proposed Regulations define "affirmative authorization" as "an action that demonstrates the intentional decision by the consumer." This performance-based standard is preferable to a strict technical mandate to use two-steps. A business should not be able to rely on satisfying a technical requirement to have two steps, rather than satisfying an obligation to design a process that is clear to consumers and ensures they are intentionally exercising their rights to opt-in to the sale of their personal data. In addition, more "clicks" can be obstacles to the exercise of consumer rights and has the potential to numb consumers to the processes required to accomplish tasks associated with exercising their privacy rights.[16] To avoid these results, the Modified Proposed Regulations should establish a definition of "affirmative authorization" that is not dependent on a two-step process and then use the definition where appropriate to describe the process for a consumer to exercise the right to opt-in to sale, rather than prescribing a specific two-step process in each regulatory provision addressing methods for opting in to the sale of personal information. W226-1

  IA Recommendation: Revise the definition of "affirmative authorization" to read, "means an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. ~~opt-in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a child under 13, it means that the parent or guardian has provided consent to the sale of the child's personal information in accordance with the methods set forth in Section 999.330. For~~

[16] *See, e.g.*, Schaub, A Design Space for Effective Privacy Notices (discussing risks of notice fatigue and habituitzation in response to consumer notices and choices and alternatives for increasing consumer engagement in making choices).

~~consumers 13 years and older, it is demonstrated through two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.~~"

W226-1 (cont.)

- **(h) "Household"** as defined in the Modified Proposed Regulations, in combination with Section 999.318, is improved but still does not resolve concerns about risks to the physical safety of consumers that may result from allowing individual members of a household to obtain data that pertains to the entire household, as is discussed in detail, *infra,* in connection with Section 999.318.

W226-2

- **(l) "Price or service difference"** please see discussion of this definition and IA's recommendation for Section 999.337.

W226-3

999.305 Notice at collection

- **The Modified Proposed Regulations expand the purpose of the Notice of Collection and require that it be linked to on any webpage where personal information is collected, thus requiring multiple privacy notices to be linked to from a single page.** *See* 999.305(a)(3)(a). It is unclear how having a "Notice at Collection" link and a "Privacy Policy" link on each page where personal information is collected benefits consumers, since the information in the Notice at Collection is included within the privacy policy.

W226-4

- **The Modified Proposed Regulations create a just-in-time disclosure requirement that does not match the concern raised.** Modified Proposed Regulation Section 999.305(a)(4) would require a business that is collecting one piece of personal information that the consumer does not reasonably expect to provide a disclosure providing a summary of every category that is collected. This notice would not be parallel with the unexpected collection and would undermine the Modified Regulations directive for businesses to take reasonable steps to provide meaningful notice to consumers.

W226-5

- **The Modified Proposed Regulations contradict and enlarge CCPA provisions regarding new purposes for processing personal information.** Modified Proposed Regulation Section 999.305(a)(5) maintains the new requirement introduced via the Proposed Regulations for a business to obtain "explicit consent" from a consumer before processing personal information for a new purpose beyond those disclosed in prior consumer notices. This provision has been updated to modify new purposes with the term "materially," this language still contradicts the clear language of CCPA which requires notice to consumers of new purposes for processing personal information in Section 1798.100(b). Notably, the CCPA does not contain any consent requirements related to collection or processing of personal information, absent the singular example where the legal guardian of a minor or a minor under 16 must "opt-in" to the sale of personal information related to the child, as provided in Section 1798.120(c).

W226-6

The sole justification cited for the new explicit consent requirement stated,

> *The purpose of these subdivisions is to implement Civil Code Section 1798.100, subdivision (b). The subdivisions make clear that a business cannot change their practices after giving the notice at collection because the consumer could have reasonably relied on the information provided in the notice at collection when interacting with the business.*[17]

This explanation fails to explain why the AGO applied different treatment to changes in the categories of information collected and changes for purposes of collection in the Proposed Regulations when CCPA sets the same requirement for both changes - new notice to the consumer. The Proposed Regulations require a new notice for the collection of additional categories of information, but require explicit consent for any new purposes of processing.[18] The AGO has not provided an explanation of why explicit consent for new purposes of processing is required, when notice without explicit consent is sufficient for the original purposes of processing under the CCPA. Regardless of the objective, the AGO has not established that this significant new burden on business is justified, or even authorized.

W226-6 (cont.)

IA Recommendation: IA recommends that subdivision 999.205(a)(4) be revised to require businesses to take steps to provide a meaningful understanding of the processing activity that triggered the requirement to provide just-in-time notice.

W226-5 (cont.)

Further, IA recommends that the second sentence of 999.305(a)(5) be revised to, "If the business seeks to use a consumer's previously collected personal information for a purpose materially different than what was previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use ~~and obtain explicit consent from the consumer to use it for this new purpose~~."

W226-6 (cont.)

999.306 Notice of Right to Opt-Out

- **Subdivision (f) introduces the new "Opt-out Button" which has the potential to cause consumer confusion.** The button looks like a toggle that consumers are likely familiar with using to set their preferences in online services or mobile applications. However, the button's only functionality is as a link to a page where the consumer may learn how to exercise their right to opt-out. Consumers familiar with this symbol could be confused into thinking that clicking on the button (which looks like a toggle but which is not a toggle) has some effect. In addition, due to the size requirements for the button and the requirement to have the button accompanied by text, the use of image is likely to take up considerable space on a webpage or mobile screen. Thus, it is unlikely that use of the button will become widespread in electronic applications.

W226-7

[17] ISOR, p. 8.
[18] *Id.*

Outside of the context of online or app-based services, the toggle button icon makes even less sense as a means to quickly communicate to consumers that they have the ability to opt-out.

IA Recommendation: Continue work to refine the "button" or "logo" to ensure that consumers are able to recognize the purpose of that it symbolizes, are not confused as to its function, and will be able to understand its meaning in all contexts in which it may appear.

W226-7 (cont.)

999.307 Notice of Financial Incentive

- **Subdivision (b)(5) creates a new obligation, not present in CCPA, to provide consumers with a specific monetary value of their data despite a lack of consensus on reliable methodology for determining such value and dubious value to consumers in using such unreliable figures as a basis for making privacy choices.** See, *infra*, IA's comments on the requirement to provide an estimate of the value of a consumer's data (§ 999.336) and how that value is calculated (§ 999.337).

W226-3 (cont.)

999.308(c)(1)(C) Privacy Policy

- **Subdivision (c)(1)(C))(5) Privacy Policy Disclosures.** The Modified Proposed Regulations would require a business to describe the process it will use to verify the consumer request in its privacy policy disclosure. The processes and information required to verify a consumer's request may need to be changed or upgraded quickly to address emerging security concerns but privacy policies cannot be changed or upgraded as fast.

  IA Recommendation: Allow businesses to disclose a link to the company's current process for verifying requests in its privacy policy instead of describing the entire process.

W226-8

999.312 Methods for submitting requests to know and delete

- **Section 999.312 diverges from CCPA's clear requirements regarding designated methods for submitting consumer requests.** The Modified Proposed Regulations deviate from CCPA by disregarding the entire concept of "designated methods" for exercising consumer rights. Subdivision (e) requires that a business respond to all requests, *regardless of how they are submitted*, by either treating the requests as properly submitted or sending specific directions to the consumer to correct any deficiencies or follow the specified process.[19] This requirement undermines the purposes of designating methods for submitting requests and potentially expands the requirements for how a business responds to consumer requests to an untold number of potential avenues of contact. For exclusively online businesses, it is also unclear how

W226-9

[19] *See also*, ISOR, p. 16.

this provision interacts with subdivision (a) which states that such a business, if it has a direct relationship with the consumer, "shall only be required to provide an email address for submitting requests to know." Given that subdivision (a) was added to implement A.B. 1564, there is clear legislative intent to allow a single online submission mechanism for online companies. It would be inappropriate for this Section to deviate from the clear language of the CCPA, as amended in 2019.

If a business must respond to a consumer request submitted through an improper channel that will require a business to ensure that all potential avenues of contacting a business or any of its employees, representatives, contractors, service providers, etc. are monitored, all personnel are trained to recognize and determine the appropriate course of action, and are able to ensure that such response happens quickly enough to meet with 10 day deadline for confirmation of a consumer request. The language of subdivision (e) contains no limitation on the potential avenues for contact, stating "[i]f a consumer submits a request in a manner that is not one of the designated methods of submission," the business must respond. While this opens a whole range of potential options for directly contacting the business — such as letters directed to the CEO or General Counsel; emails to random employees in roles unrelated to privacy compliance or user requests; calls to hotlines maintained for conducting employment verification, press inquiries, law enforcement emergencies, or investor relations; requests directed to agents for service of process; walk-in requests to business offices — it also raises the prospect of potentially more indirect submissions of consumer requests, including direct contact to individual employees of a business via social media or email, requests directed to outside vendors such as law firms, or even publicly posting a request directed to a business via an "at mention" on social media. Monitoring this array of channels would be incredibly burdensome for business and would be prone to systematic failures. A request directed to a single employee could sit for months without reply if the employee is on parental leave or has left the company. By contrast, a designated method for submitting a request will have a plan in place to ensure it is appropriately staffed regardless of comings and goings of individual employees.

W226-9 (cont.)

When this potentially endless array of channels of communication are combined with the training mandate in the Modified Proposed Regulations, the burden becomes even more untenable. The training for personnel who are tasked with responding to consumer requests under CCPA is a reasonable requirement directly provided for in CCPA. However, if every employee of a business is converted into someone who requires training because a consumer request could be directed to them, and they must be able to recognize the nature of the request, know where to direct it or how to respond, and the appropriate timeframe for such response, it potentially amounts to every employee having to be trained on CCPA regardless of the nature of their job role or the likelihood that they will encounter a notice in the scope of their employment.

The AGO has not met its obligations to explain why this necessary, why it is consistent with CCPA's clear language regarding "designated methods," how it furthers the purposes of the CCPA in a material way, whether the burden associated has been considered and is reasonable, or even whether there are any reasonable alternatives to achieve the goal of making sure that a business does not refuse consumer requests because they are deficient based on a technicality. If this is in fact the true purpose of this Section, subdivision (e) is broader than necessary to the extent it imposes requirements on how businesses respond to requests submitted outside of designated methods.

W226-9 (cont.)

IA Recommendation: Revise Section 999. 312 by striking subdivision (e) in its entirety.

999.313 Requests to Know and Delete

- **Subdivision (a) of this Section creates new obligations and burdens on business by requiring that a business respond to a consumer request to confirm receipt and provide information on how business will respond**. While in the context of electronically submitted consumer requests, an auto-response can potentially satisfy this new requirement that is dependent on the consumer request being submitted via the "designated method" which the business has configured to send the appropriate auto-response. This is another reason why Section 999.312(e) should be struck, as is discussed above. If this requirement remains in the final regulations, businesses will face significant risks of violating the law because of a failure to provide an auto-response on channels that are not intended for processing consumer requests. Alternatively, a business would be forced to address this risk by sending a response to all inquiries of any kind a response that complies with subdivision (a). This could be very confusing to business partners, customers, job candidates, press, and other entities that may communicate with a business about issues completely unrelated to CCPA. For channels of communication that are not electronic, the 10 day response time may also be challenging.

  W226-10

  CCPA provides 45 days for a business to respond to consumer requests in Section 1798.130. In 2019, the California Legislature passed A.B. 1355 which amended this provision of the CCPA. While other changes were made to multiple provisions which include the 45 day initial response period language, the Legislature left the response deadline unchanged. In the absence of a statutory requirement for the 10 day deadline, the regulations should only add a new requirement if it is "necessary to further the purposes" of the CCPA.[20] At this point, it is unclear what benefit this requirement offers since the confirmation will only provide consumers with information that is not specific to their situation and is available in the notices and privacy policy (or as IA recommends, other privacy-related help content) mandated by the CCPA.

[20] Cal. Civ. Code § 1798.185(b)(2)(as amended by A.B. 1355).

IA Recommendation: IA reiterates its recommendation that subdivision (e) of Section 999.312 be struck in its entirety for the additional reasons discussed in reference to Section 999.313. In addition, IA recommends that subdivision (a) of Section 999.313 be struck in its entirety.

W226-10 (cont.)

- **Subdivision (c) is unnecessarily burdensome and duplicative, without adding additional value and transparency for consumers.** As discussed previously, the Modified Proposed Regulations' attempt to rearrange the CCPA's disclosures results in redundant notices, cumbersome privacy policies, and responses to consumer requests that are likely to overwhelm consumers with information that is readily available via privacy policies and notices, potentially obscuring the personal information that is of most value in response to an access request. This subdivision requires businesses to respond to a consumer access request not only with specific pieces of personal information but also with a second set of responses—namely, customized metadata regarding the information collected for each customer, categorized in a complicated manner outlined by the statute. These hyper detailed, specific disclosures duplicate information available via a request to know for specific pieces of information and more general information available in the privacy policy. For example, detailing for each category of personal information each business purpose for which that category of information was disclosed or each category of third party to whom it was sold, but on a customized basis for that specific consumer does not add any information which is not otherwise available via specific pieces of data or from the general information in the privacy policy. This subdivision has no equivalent in any privacy regime, is hugely burdensome, has no corresponding consumer benefit, and is completely unnecessary when a consumer is accessing the actual information.

  W226-11

  IA Recommendations: Revise subdivision (c) as follows:
  - (c)(2) "For requests that seek the disclosure of categories of personal 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 may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. <u>If the consumer also requested specific pieces of information and the business discloses specific pieces of information, the business is not required to respond to the request for categories of personal information.</u> 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.
  - (c)(9) "In responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response to the consumer ~~as required~~

W226-12

~~by the CCPA. It shall not refer the consumer to the businesses' general practices outlined in its privacy policy~~ unless its response would be the same for ~~all~~ most consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories." W226-12 (cont.)

- (c)(10) Strike the subdivision as it requires disclosures of categories, including categories of sources, categories of parties to whom the business has disclosed information to by broken out by category of information collected when the consumer is receiving the actual information. W226-13
- (c)(11) Clarify that a business has "provide[d] consumers a meaningful understanding of the categories listed" if it has used the language specifically enumerated in the CCPA or the regulations. W226-14

- **Subdivision (c)(1) creates risks of inappropriate disclosure of information about a consumer in response to an unverified consumer request.** The Modified Proposed Regulations treat verification of a consumer request as though it is appropriate to view identity verification across a spectrum of likelihood that the person making the request is the consumer, rather than as being a minimum requirement that must be satisfied. In doing so, the AGO appears to be more concerned about the potential harm to consumers that would result from not being able to access personal information, delete information, or opt-out than the harm that may result from bad actors inappropriately exercising a consumer right specifically to engage in illegal or malicious action. IA member companies believe that the regulations should focus more clearly on the risks from bad actors. If a business is not responding appropriately to consumer requests, the CCPA provides a remedy in the form of Attorney General enforcement. But for a consumer whose personal information is inappropriately obtained, account contents deleted, or accumulated benefits of a financial incentive program stolen, there is unlikely to be an adequate remedy. W226-15

  The AGO and the California Legislature know all too well how determined criminals will target consumers and their personal information. California was a leader in passing the first data breach notification requirement in the U.S. to specifically address the harms to consumers from their personal information ending up in the wrong hands. For this reason, IA believes that the Modified Proposed Regulations should not require that a consumer request that is rejected for failing verification be converted into a request to exercise a different CCPA consumer right.

  This analysis of subdivision (c)(1) is further complicated by the way the CCPA and the regulations approach categories of personal information. General disclosures of categories of personal information, such as those mandated in notices of collection or a privacy policy, pose no specific challenges since the disclosures are not consumer specific and apply broadly. However, subdivision (c)(1) contemplates disclosure of categories of personal information specific to a particular consumer in cases where

there is not appropriate verification to disclose "specific pieces" of personal information. It is unclear what types of information would go beyond generally applicable disclosures of categories of personal information without themselves raising the same issues as personal information. For example, if a request was made for personal information from a company that offers security devices and security monitoring services and the request was rejected for failure to meet the verification requirements, it would not be appropriate for the business to disclose any information, even "categories," to the individual who was unable to verify their identity. Even categories could reveal information that should remain private. For example, the business could disclose that personal information was collected for categories related to security devices, but not categories related to the monitoring service revealing that the account holder does not subscribe to this service. This information could result in a consumer being placed at risk of being targeted for a break-in.

In addition, if the business determines that categories of personal information are the same as those generally available in its privacy policy, the business is not required to send a detailed response to the consumer.

W226-15 (cont.)

Importantly, creating obligations in response to *unverified* requests is contrary to, and inconsistent with, the statute. The CCPA contemplates that unverified requests should be *discarded* precisely because they are unverified: "A business is not obligated to provide information to the consumer pursuant to Sections ... 1798.105 ... if the business cannot verify ... that the consumer making the request is the consumer about whom the business has collected information ..." Practically, the very reason a business should discard an unverified request is to protect the consumer—the business is unable to verify the individual's identity and therefore should not act on requests related to that consumer's personal information. And the statute creates a specific mechanism for opting-out of the sale of information. Collapsing verification and opt-out procedures is contrary to the statute and creates vectors for abuse.

IA Recommendation: Strike language in subdivision (c)(1) mandating that a request that fails verification be considered for disclosure of categories of personal information, as follows, "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).~~

The deletion of the language of the Proposed Regulations related to security in Subdivision (c)(3) causes concerns about requests to know that adversely impact the rights of other consumers and the security of businesses. Subdivision (c)(3) stated, "[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." This language served as an important protection for businesses that have legitimate concerns that responding to a request to know from a consumer, for example a consumer that defrauded other consumers, could create security risks for other users, individuals, or the business. This provision was clearly in line with CCPA's directive that access requests shall not "adversely affect the rights and freedoms of other consumers."[21] This limitation on the obligations under the CCPA should be reflected in this subdivision of the Modified Proposed Regulations and the original language of the Proposed Regulations retained. W226-16

Subdivision (c)(3) creates privacy and security concerns, is overly restrictive, and creates undue burdens for business. The right to know requires a business to disclose to the consumer personal information the business has "collected about that consumer." The statute requires the AGO to promulgate regulations for access requests that "tak[e] into account," inter alia, "security concerns, and the burden on the business." § 1798.185(a)(7). Subdivision (c)(3) properly recognizes that not all personal information a business has about a consumer need be made available. We agree with AGO that access cannot be absolute, for example, it should not apply when a business does not maintain the personal information in a searchable or reasonably accessible format, or when the business maintains the personal information solely for legal or compliance purposes. We appreciate and agree with the recognition that an absolute access requirement is not desirable or consistent with privacy best practices. The proposed provision, however, is too restrictive, does not recognize other important limitations to access, does not sufficiently limit the scope of the right to know to information the business has "collected," and does not recognize security concerns or undue burdens. As currently drafted, subdivision (c)(3) contemplates a four-part test for which, in practice, no information will meet all four prongs—particularly given the requirement that the information be maintained "solely for legal or compliance purposes." For example, information could be held by a business purely for legal compliance purposes, such as pursuant to a preservation request from law enforcement in anticipation of obtaining a court order, but if it is maintained in a "reasonably accessible format" in order to be disclosed to law enforcement once served with an order, this information would be subject to the access request even if it is only stored in a manner accessible to personnel who review and respond to law W226-17

[21] Cal. Civ. Code § 1798.145(j).

enforcement requests. Functionally, the four part test is too rigid to limit the scope of access requests.

The statute and draft regulations currently lack sufficient clarity regarding how far the access right extends, and as a result, businesses do not have clear guidance as to whether they must build new systems to reach anything that may technically be responsive. A clear regulation is necessary to draw outer lines around the information a business must make available. Many businesses possess data that may technically fall within the CCPA's broad definition of "personal information," but that is not used in the ordinary course of business, such as log data, that is not readily accessible, or has not been "collected." This is particularly true with data that the business has derived rather than collected or which may not be readily accessible. Requiring a business to identify, compile, and then make accessible such information has the adverse effects of forcing a business to face undue burdens in an effort to create new or more robust consumer profiles. This creates privacy and security concerns for consumers by associating more data with them than otherwise would be, as businesses will be required to build systems with more detailed consumer profiles and then send those profiles outside of the business. W226-17 (cont.)

A regulation drawing clearer lines regarding the scope of the right to know will have pro-privacy and pro-security ramifications and will save businesses from having to face significant burdens and legal uncertainty. IA's following recommendation draws a clearer line while properly taking into account the statutory limitation that the business must have "collected" the personal information, and the statutory requirements the regulations consider burden and security.

IA Recommendation: IA recommends retaining and amending this to reference security risks to personal information of other consumers as well, by revising the subdivision to read, "substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's or another consumer's account with the business, or the security of the business's systems or networks, or consumers." W226-16 (cont.)

Specifically, IA recommends that subdivision (c)(3) be amended to the following:

> 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, networks, or consumers. In responding to a request to know, a business is not required to provide personal information that meets any of the following conditions, provided the business describes to the consumer the categories of records that may contain personal information that it did not provide it because it meets one of the conditions stated below: W226-17 (cont.)

a. The business does not maintain the personal information in a searchable or reasonably accessible format;
b. The business maintains the personal information solely for legal or compliance purposes;
c. The business does not sell the personal information and does not use it for any commercial purpose.
d. The business does not associate the personal information with a consumer in the ordinary course of business; or
e. The personal information was not collected from the consumer or a third party, but was instead derived internally by the business

W226-17 (cont.)

- **Subdivision (c)(7) should be clarified to specify that a business may use a password protected account to respond to consumer requests submitted via an authorized agent.** This is necessary to ensure that online accounts, particularly those for whom verified personal information such as name, address, phone numbers, and other identifying information are not needed can be used to ensure that the party who will obtain the information has been properly authenticated using the account security controls that govern the log-in process for the password protected account.

  IA Recommendation: Revise subdivision (c)(7) as follows: If a business maintains a password-protected account with the consumer, it may comply with a request to know, submitted by a consumer or an authorized agent, by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 4.

W226-18

- **Subdivision (d)(1) adds new requirement that should be removed.** This subdivision would require that for any consumer making a deletion request, if a business cannot verify the consumer's identity, the business must "ask the consumer if they would like to opt-out of the sale of their personal information and shall include either the contents of, or al link to, the notice of right opt-opt out in accordance with section 999.206." This conflates the consumer expectations between opt-out requests and requests to delete. Further, it would have businesses combine two different request flows.

  IA Recommendation: Remove the requirement of an opt-opt prompt for consumers who cannot be verified during a deletion request. Alternatively, allow businesses to link to the privacy policy disclosure so consumer's who cannot be identified in a deletion request can find information on how to exercise all of their privacy rights.

W226-19

999.315 Requests to Opt-Out

- **Subdivision (a) requires that a business provide two or more designated methods for a consumer to opt-out from sale, one of which must be an interactive webform, adding an additional requirement to the CCPA.** CCPA Sections 1798.120, 1798.130, and 1798.135 only contemplate one method for opt-out from sale which is specified in Section 1798.135(a)(1).[22] While allowing more flexibility to businesses to adopt additional methods to offer to consumers to exercise their rights may be appropriate in terms of furthering the purposes of the title, a mandate to adopt multiple methods or to use any specific method other than the statutorily-mandated link exceeds the AGO's rulemaking authority. W226-20

  IA Recommendation: The Proposed Regulation should be revised to make the designation of any additional methods, beyond the link required in Section 1798.135(a)(1), discretionary, as follows: "A business shall provide ~~two or more designated methods for submitting requests to opt-out,including~~, 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. A business may, at its discretion, designate additional methods by which it will accept consumer requests to opt-out of sale of personal information."

- **There are technical and legal issues with the requirement in subdivision (d) that businesses that collect personal information from consumers online must treat consumer-enabled privacy controls as a valid request to opt-out under 1798.120.**
  - This method was not contemplated in the CCPA, as is discussed above in regard to subdivision (a). This requirement does not comply with the CA APA and regulations as it is: 1) in conflict and inconsistent with the statute, 2) not necessary; 3) beyond the authority of the AGO's rulemaking mandate; 4) it has not been adequately justified in the ISOR; 5) the financial impact was not adequately considered in the SRIA; and 6) reasonable alternatives were not adequately considered. W226-21
  - The language regarding the opt-out logo or button indicates an intent for that option to be used "by all businesses to promote consumer awareness of the opportunity to opt-out…" 1798.185(a)(4)(C). The Modified Proposed Regulations require "an interactive webform accessible via a clear and W226-22

[22] IA notes that the proposed ballot initiative by Alastair Mactaggart, as submitted to the AGO by letter dated October 9, 2019, (as amended November 13, 2019) would add language to CCPA 2018 to incorporate the concept of "opt-out preference signals" as an alternative mechanism to the single method of a "clear and conspicuous link" required by the CCPA as currently enacted. *See* Section 13, amending Cal. Civ. Code § 1798.135, of the text of the ballot initiative attached to the November letter (version three). Presumably, this indicates that Mr. Mactaggart agrees that CCPA 2018 does not include this option.

conspicuous link titled "Do Not Sell My Personal Information," or "Do Not Sell My Info," on the business's website or mobile application." W226-22 (cont.)

- If the business must provide two or more designated methods and one must be the webform/button/link, the business should be able to choose the other option to designate. As is discussed in IA's comments on Section 999.312 of the Modified Proposed Regulations regarding designated methods to submit access and deletion requests, this provision essentially eliminates any business choice and control over how to take-in consumer requests and to ensure adequate resources, technology, and training for handling consumer requests via the designated channels. Given the serious nature of the legal obligations which are triggered by a consumer request to opt-out, businesses need to have clarity around the potential avenues by which such requests will be submitted so that they may ensure the appropriate measures are in place for compliance. Creating uncertainty about which channels could be used for making such requests sets businesses up for failure. W226-20 (cont.)
- The Modified Regulations continue to conflate the CCPA's "Do Not Sell" requirements with tangentially related Do Not Track settings. While some businesses already offer account controls which may allow opt-out from sale to occur in a manner that is secure and will allow the consumer and the business to have a shared understanding of the nature and scope of the consumer's choice, there are significant issues of how a browser-plug in or another type of browser signal should be applied (for devices, browsers, consumers), how such a signal would interact with other rules (e.g., CCPA's waiting period to request opt-in), and would impact other users of shared devices or shared "unique identifiers" such as IP addresses. A consumer may think that use of a browser-based signal has an impact beyond what is technologically feasible, since it will be specific to that browser on that specific device and cannot be applied across all of the consumer's browsers and devices without specific action from the consumer. If a consumer wants to accomplish an "account-wide" opt-out, it will need to do so through direct communication with an online business in a manner that is specifically connected to the consumer's account. In addition, some browser or device based controls may deprive consumers of notice regarding the potential ramifications of their choice to opt-out, the availability of a financial incentive, or an alternative option that W226-21 (cont.)

would allow the consumer a more nuanced choice than "all or nothing."[23] This makes it harder, not easier, for consumers.

- The proposed regulation is therefore contrary to and inconsistent with the statutory text and purpose, and creates significant uncertainty and vagueness for both consumers and businesses regarding the opt-out right. They also exceed the delegation of authority to the AGO, as the statute instructs the AGO to :facilitate" opt-out requests and to promote "the development and use of a recognizable and uniform opt-out logo" -not to create *new ways* in which to characterize a consumer's behavior as an opt-out request.

IA Recommendation: This requirement should be made discretionary for online businesses that can implement it in a manner with adequate controls to determine the intent of the consumer to opt-out from sale and the scope of how such opt-out should be applied. This may be accomplished by revising subdivision (c) as follows, "If a business collects personal information from consumers online, the business **may** ~~shall~~ treat user-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism, ~~that communicate or signal the consumer's choice to opt-out of the sale of their personal information~~ as a valid request submitted pursuant to Civil Code Section 1798.120 **if the controls allow the consumer to clearly indicate an intent to opt-out of sale, in whole or in part, for an online account maintained with the business** ~~for that browser or device, or, if known, for the consumer~~."

W226-21 (cont.)

- **Subdivision (h) creates security risks for consumers and businesses by requiring a business to disclose in response to a suspected fraudulent consumer request the reason why it is believed to be fraudulent.** Subdivision (h) provides that a request to opt-out does not need to be verifiable, but a business can decline to comply if they have a "good faith, reasonable, and documented belief" that the request is fraudulent. Businesses must provide notice to consumers and explain why the business believes it is fraudulent. Such disclosures may harm business efforts to protect against fraud and undermine consumer protections for security and privacy. By explaining to a potential bad actor why the business has determined they are a bad actor, the business is essentially providing criminals with blueprints as to how to get around their fraud detection systems and protocols.

W226-23

[23] Version 3 of the 2020 ballot initiative to amend CCPA 2018 also acknowledges the need for rules regarding uses of opt-out signals in Section 13, by proposing an amendment to Cal. Civ. Code § 1798.135 to add as new (b)(1) a provision that allows use of opt-out preference signals that comply with technical specifications set forth in regulations to be promulgated under the statute. If the final regulations for CCPA 2018 will include a requirement to recognize an "opt-out preference signal" as currently contemplated in the Modified Proposed Regulations, then such a rulemaking in line with the proposed rulemaking mandate in Version 3 of the 2020 ballot initiative, described with specificity in the proposed new Cal. Civ. Code § 1798.185(20), should be added.

999.316 Requests to opt-in to sale after opting-out

- Please see IA comments, *supra*, regarding Section 999.301(a), the definition of "affirmative authorization" regarding the risks for requiring consumers to go through a two-step process. For the reasons explained with regard to the definition of affirmative authorization, subdivision (a) of this Section should be revised to eliminate mention of the two-step process and should be substituted with the term "affirmative authorization."

  IA Recommendation: Revise subdivision (a) to read, "Requests to opt-in to the sale of personal information shall require affirmative authorization ~~use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in~~."

W226-1 (cont.)

999.317 Training and record-keeping

- **The training requirement in subdivision (a) is vague and overly burdensome and offers no additional protections for consumers.** The CCPA already includes reasonable training requirements for staff dedicated to handling consumer requests under the statute.[24] Subdivision (a) expands this requirement to a mandate that individuals responsible for handling consumer inquiries "shall be informed of all the requirements in the CCPA and these regulations" rather than only the relevant Sections of CCPA. CCPA is a complex and difficult to understand statute that encompasses not only consumer rights but also enforcement, rulemaking authority, and security breach remedies. To require staff dedicated to handling consumer requests to be trained on *all* of CCPA, rather than the provisions which relate to consumer requests and consumer rights expands the CCPA's training mandate in a way that is unhelpful and may lead to more confusion and less effective training. The ISOR suggests that the training mandate was expanded because of gaps in CCPA's text. If there are specifically relevant Sections of CCPA to which the training requirement should apply because they are related to the exercise of consumer rights, then it would have been preferable for the AGO to expand the requirement to those Sections rather than the entirety of the statute and the regulations.

  IA Recommendation: Strike the entirety of subdivision (a).

W226-24

- **The recordkeeping requirement in subdivision (g) is vague, imposes an unjustified burden on business without promoting transparency to consumers or accountability, and exceeds the AGO's rulemaking authority.**

[24] *See, e.g.*, Cal. Civ. Code § 1798.135(a)(3) which provides, "Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 and this Section and how to direct consumer to exercise their rights under those Sections."

- The provisions of subdivision (g) are vague. First, the definition of "commercial purposes" in the CCPA is extremely broad.[25] This term is seldom used in the CCPA or in the Modified Proposed Regulations and it is unclear as to whether or not "business purposes" are encompassed or excluded from the scope. In addition, it is not clear what types of activities constitute "receipt" for commercial purposes. This is particularly troubling given the Modified Proposed Regulations' approach to "designated methods" for submitting requests and the inclusion of browser signals and other automated controls as "requests" to opt-out. W226-25
- Alternatives to the recordkeeping and publication requirements in the Modified Proposed Regulations were not adequately considered. The ISOR is not clear as to what types of alternatives to detailed metrics on consumer requests were considered to achieve the goals of transparency and accountability. It appears that the only alternatives considered were not having any requirements for reporting metrics or applying the metric reporting to all businesses. While California law does not require the AGO to invent alternatives where none exist, alternatives do exist in leading privacy regimes around the globe including the GDPR. For example, the AGO could have considered an in-take mechanism for consumer complaints regarding responses to consumer requests, periodic audits of businesses, or require businesses to maintain internal documentation of compliance with CCPA's requirements that would be available for review as a part of an enforcement investigation. W226-26
- Given the lack of understanding of the nature of the burden on businesses subject to the recordkeeping requirements and the potential that the aims could be achieved through less burdensome alternatives, the subdivision should be struck from the Modified Proposed Regulations.
- While the problems with the mismatch between the burdens of the provision and the benefits form an adequate basis for the subdivision to be deleted from the Modified Proposed Regulations as inconsistent with the APA, it is also worth noting that CCPA does not mandate this record-keeping requirement, nor any regulations in this area. Thus, this subdivision would only be appropriate if it was determined to be "necessary" to further the purposes of CCPA. The AGO has failed to meet this threshold. W226-27
- Given that the basis for such a recordkeeping obligation would be the rulemaking authority in Cal. Civ. Code Section 1798.185(b), the AGO is not subject to a requirement to publish the regulations by July 1, 2020 and also has significant discretion to allow a period of time for businesses that would have to comply with this new obligation to build the necessary systems and come into compliance. If the AGO keeps this proposed requirement, it should allow covered businesses one year to come into compliance after the final CCPA

[25] Cal. Civ. Code § 1798.140(f).

regulations take effect and after a business becomes subject to the requirement. W226-27 (cont.)

IA Recommendation: Subdivision (g) be struck in its entirety. W226-26 (cont.)

999.318 Access/Deletion for households

- **This section does not adequately address safety concerns raised with the "household" provision as it relates to access/deletion requests for several reasons:**
  - It assumes that an abusive member of a household will not coerce other members of the household to provide consent in order for the abuser to maintain control over his/her victims activities.
  - It fails to establish any timeframe for the concept of household or clarify what rights a consumer may have regarding personal information collected while they were a member of household once they leave the household.
  - This section of the Modified Proposed Regulations should be revised to tie "household" to a shared account, such as an account that specifically allows sub-accounts for spouses or children and for which all parties to the account will have notice of the potential that other household members participating in the account may be able to access information related to the use of the account.
  - This section should also be struck unless a mechanism can be developed to ensure that members of a household cannot be coerced or intimidated into providing consent for an access or deletion request.

W226-28

IA Recommendation: The AGO should strike this section in its entirety from the Modified Proposed Regulations and further contemplate the guidance in A.B. 1355 to address the safety concerns posed by "households" in the context of access and deletion requests. Such regulations can be issued separately from the regulations required to be issued by July 1, 2020, and processing of requests related to households postponed until such time as these critical issues of physical safety can be addressed.

999.324 Verification for password-protected accounts

- **Subdivision (a) should make clear that a business may require that a consumer request submitted through an authorized agent be authenticated through a password-protected account** as discussed in IA's comments to Section 999.313(c)(7), *supra*. In addition to IA's prior recommendation to revise Section 999.313, IA also recommends that subdivision (a) of Section 999.324 is revised to make this explicit.

IA Recommendation: Revise subdivision (a) to read, "If a business maintains a password-protected account with the consumer, the business may require the consumer to verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in Section 999.323. A business may require the consumer to verify

W226-29

the consumer's identity and the consumer's permission to act on the request of an authorization agent through the business's existing authentication practices for the account. The business shall also require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data."

999.326 Authorized agent

- **The interaction of the verification and authorized agent provisions do not provide needed clarity regarding proper verification and authentication of agents.** The verification provisions of the Modified Proposed Regulations do not adequately explain the proper interaction of a business' discretion in authentication with the requirement that authorized agents be allowed to make requests on behalf of consumers. In addition, it is not clear how business can be expected to reasonably authenticate agents. Because of these difficulties, as IA proposed in relation to Section 999.313(d)(7) and Section 999.324, businesses should be able to rely on their authority to require consumers to use existing accounts to make requests, to also require agents must make the requests through those same accounts as a way of demonstrating the agent's authority. The verification sections of these regulations should also provide greater specificity as to how authentication of authorized agents should progress including providing more substantial guidance on the minimum evidence required and a safe harbor for businesses.

W226-29 (cont.)

W226-30

- **Regulations are not clear regarding the use of an authorized agent to exercise the various consumer rights created by CCPA.** The CCPA only specifically includes the ability to authorize another person to exercise the right to opt-out of sale.[26] As has been previously discussed in the connection with use of an authorized agent, the difficulty of authenticating the agent's identity and authorization from the consumer create significant risks for consumers and will burden businesses who will work diligently to avoid acting on fraudulent requests. Consistent with CCPA, the Modified Proposed Regulations should restrict use of authorized agents to the exercise of the right to opt-out sale.

W226-31

999.330 Minors under 13 years of age

- **The Modified Proposed Regulations should be clear that a consent methodology that satisfies COPPA necessarily satisfies the "affirmative authorization" requirement of the CCPA.** Under COPPA's preemption standard, it is clear that the Attorney General may not impose additional or otherwise inconsistent consent requirements beyond those imposed by COPPA.[27] Under COPPA and the COPPA Rule, new approved methods for parental consent may become available in the future and

W226-32

[26] Cal. Civ. Code § 1798.135(c).

[27] *See* 15 U.S.C. § 6502(d) ("No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section.")

such methods should be available to be used by the clear terms of the CCPA regulations.

- **Subdivision (a)(1) requires "affirmative authorization" of the sale of personal information that is in "addition to any verifiable parental consent" required by COPPA creating a duplicative requirement for businesses that are covered by COPPA.** This provision could be drafted more narrowly to fit the need explained in the ISOR. The ISOR explains that "[t]his is necessary because the CCPA's prohibition on the sale of children's personal information covers information regardless of whether collected online, offline, or from a third party."[28] IA has no objection to entities that are not subject to COPPA being required to follow CCPA requirements. However, for a business that is subject to COPPA and has a federally-complaint process to obtain consent from parents or guardians of minors, there is no justification for requiring a completely separate and secondary consent flow. This is particularly true given that the Modified Proposed Regulations accept the adequacy of the existing COPPA parental consent mechanisms, by adopting them for the CCPA parental opt-in to sale. A more narrow provision requiring a COPPA-compliant parental consent process that also addresses opt-in to sale under the CCPA *or* a CCPA-compliant parental opt-in to sale process adequately addresses the critical interest in child safety and privacy, as well as parental interests in being empowered to make safety and privacy decisions on behalf of their young children. IA also believes that the imposition of additional requirements on "operators" regulated by COPPA is inconsistent with the preemption clause in COPPA.[29] W226-32 (cont.)

  IA Recommendation: Revise subdivision (a)(1) to read, "A business that has actual knowledge that it sells the personal information of a child~~ren~~ under the age of 13 shall utilize ~~establish, document, and comply with~~ a reasonable method, in light of available technology, for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. Verifiable parental consent that complies with the Children's Online Privacy Protection Act and regulations thereunder shall satisfy this obligation. ~~This affirmative authorization is in addition to any verifiable parental consent required under the Children's Online Privacy Protection Act...~~"

999.336 Discriminatory practices

- Please also see IA comments and recommendations related to financial incentives in regards to Modified Proposed Regulations Section 999.307, *supra*. W226-3 (cont.)
- **Subdivision (a) ties CCPA's non-discrimination provisions to the exercise of consumer rights created by regulations which exceeds the AGO's rulemaking authority.** The CCPA is clear that non-discrimination obligations only apply to the rights W226-33

[28] ISOR, p. 34.
[29] 15 U.S.C. § 6502(d).

"created by this title."[30] Where the California Legislature wanted to incorporate future provisions created by AGO rulemaking in CCPA, it did so with specific language.[31] Thus, consistent with rules of statutory construction, an intent to include new rights created by regulation cannot be read into Section 1798.125 of CCPA. This also exceeds the rulemaking mandate in Section 1798.185(a)(6) which charges the AGO with "establishing rules and guidelines regarding financial incentive offerings." Thus, this subdivision should be revised to be consistent with CCPA.

W226-33 (cont.)

IA Recommendation: Revise subdivision (a) as to read, "[a] financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code Section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA ~~or these regulations~~."

999.337 Calculating value of consumer data

- **There is no basis for a requirement to calculate and disclose the value of consumer data in CCPA.** In fact, the California Legislature had at least one bill introduced in the 2019 which would have amended CCPA to require exactly this. A.B. 950 proposed to require businesses to disclose the monetary value of consumer data, but that bill did not pass. If CCPA included this requirement, such a bill would not have been necessary. In addition, unlike other bills that would have amended CCPA which were considered and ultimately passed in the same legislative session, A.B. 950 was not acted on by legislators. Where the Legislature chooses not to enact a proposal, the AGO should not legislate such proposal through the rulemaking process.

W226-34

- **This new obligation is not necessary, is burdensome, and is of questionable value.** The SRIA notes a significant lack of agreement on how to value data and on whether it can be done accurately. This lack of agreement is reflected in this Section of the Modified Proposed Regulations in that it allows a number of different methodologies for calculating the value of data. The lack of an agreed method of calculation means that the approaches taken and the resulting values will differ significantly which will limit the utility to consumers.

  The perceived value of data is subjective, in flux and depends on context. Because data lacks clear, objective value, academics have come up with wildly different estimates for the value of certain services to people, and experts are likely to come up with differing values for other services as well. More generally, the idea of valuing personal information and it being disclosed in a general fashion will bear no relation to the actual value of the data. The actual value of personal data will be highly variable, based not just on the specific business but also larger market considerations. For example, the

W226-3 (cont.)

[30] *See* Cal. Civ. Code § 1798.125(a)(1).
[31] *See, e.g.*, Cal. Civ. Code § 1798.140(i)("and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185").

value of data to a business is variable, particularly as the amount of data grows.[32] Depending on other variables in a given business arrangement, the value of the personal information could also vary widely.

Concerning free, ads-based services, personalized services, people don't give up or exchange data for their experience; instead the experience is made possible by data. This is an important distinction. Data is what enables ads-based services to provide the core of the service itself, which is personalized content. The reason certain businesses can offer their services for free is not that they are being compensated with people's data. It's that they make money by selling ads: these businesses sell advertisers the opportunity to present their messages to people. And advertisers pay the businesses based on objective metrics such as the number of people who see their ads or the number of people who click on their ads.

W226-3 (cont.)

Given the significant questions about how to generate a value for data and well-founded skepticism on whether any disclosed value for data will accurately inform consumers of information related to the transaction they are considering, there is not an adequate benefit to consumers to justify the corresponding burden to business. Needless to say, undertaking an entirely new process to generate a value of data for publication to consumers will require businesses to engage in work that is not required by the CCPA, will require substantial investigation to determine the most workable methodology among those approved in the Proposed Regulation, and new legal risks for potentially publishing a figure that is challenged.

The AGO should strike this provision and allow the plain language of the CCPA to guide business and regulatory enforcement efforts on whether financial incentive programs have an appropriate correlation of value to the consumer and value to the business.

IA Recommendation: Strike Section 999.337 in its entirety.

[32] https://www.nber.org/papers/w24334.pdf

From: Scott Jordan
To: Privacy Regulations
Subject: Written comments regarding revised proposed CCPA regulations
Date: Tuesday, February 25, 2020 4:15:48 PM
Attachments: Jordan CCPA regulations comments2.pdf

Attached please written comments regarding the revised proposed CCPA regulations (Sections 999.300 through 999.341 of Title II, Division 1, Chapter 20 of the CCR).

-Scott Jordan

Scott Jordan
3214 Bren Hall, Department of Computer Science, University of California, Irvine, CA 92697-3435
[redacted], http://www.ics.uci.edu/~sjordan

BEFORE THE
CALIFORNIA ATTORNEY GENERAL

In the Matter of
Sections §§ 999.300 through 999.341
of Title 11, Division 1, Chapter 20,
of the California Code of Regulations (CCR)
concerning the California Consumer Privacy Act (CCPA)

COMMENTS OF SCOTT JORDAN

Scott Jordan
Department of Computer Science
University of California, Irvine
Irvine, CA 92697-3435
[redacted]

February 25, 2020

About the Author: Scott Jordan is a Professor of Computer Science at the University of California, Irvine. Scott received the Ph.D. degree in Electrical Engineering & Computer Science from the University of California, Berkeley. In 2006, he served as an IEEE Congressional Fellow, working in the United States Senate on communications policy issues. During 2014-2016, Scott served as the Chief Technologist at the Federal Communications Commission, advising on technological issues across the Commission. In writing these reply comments, Professor Jordan represents no one but himself, and is not speaking on behalf of his employer or any other party.

Table of Contents

1. Disclosure of purposes for collecting a category of personal information (§999.305 Notice at Collection of Personal Information, §999.308 Privacy Policy, and §999.313 Responding to Requests to Know)

In the Initial Proposed Regulations §999.305(b), the information that a business shall include in its notice at collection included: (i) "[a] list of the categories of personal information about consumers to be collected" and (ii) "[f]or each category of personal information, the business or commercial purpose(s) for which it will be used."[1] However, in the Revised Proposed Regulations §999.305(b), "[f]or each category of personal information" was deleted.

In addition, in the Initial Proposed Regulations §999.308(b)(1)(d), the information that a business must include in its privacy policy regarding a consumer's right to know personal information collected similarly included: (i) "the categories of consumers' personal information the business has collected" and (ii) "[f]or each category of personal information collected, … the business or commercial purpose(s) for which the information was collected".[2] However, in the Revised Proposed Regulations §999.308(c)(1)(d), "[f]or each category of personal information collected, … the business or commercial purpose(s) for which the information was collected" was deleted.

W227-1
W227-2
W227-3

In addition, in the Initial Proposed Regulations §999.313(c)(10), the information that a business shall provide to a consumer in a response to a verified request to know the categories of personal information collected similarly included "for each identified category of personal information it has collected about the consumer" "[t]he business or commercial purpose for which it collected the personal information"[3] However, in the Revised Proposed Regulations §999.313(c)(10), "for each identified category of personal information it has collected about the consumer" was deleted.

These deletions remove the ability of a consumer to know why a business wants to collect a category of her personal information. For example, under the Revised Proposed Regulations, a business may now only disclose the following:

> Collection: The personal information that we collect includes: (a) your address and (b) the IP addresses of the websites you visit.
>
> Purposes: We use some of the personal information we collect to route your Internet traffic to the intended destination. We use some of the personal information we collect for advertising.

[1] *Initial Proposed Regulations*, § 999.305(b).
[2] *Initial Proposed Regulations*, § 999.308(b)(1)(d).
[3] *Initial Proposed Regulations*, § 999.313(c)(10).

Under such a disclosure, a consumer will be left in the dark about whether the business uses the IP addresses of the websites that she visited for advertising (i.e., behavioral advertising) or whether the business uses her address for advertising (i.e., location-based advertising). These two possibilities have very different consequences, and consumers have the right to know which is occurring.

The comments in the record that objected to the requirements in the Initial Proposed Regulations for a business to disclose the purposes for collecting a category of personal information presented three objections, each of which is fallacious.

First, some commenters asserted that this disclosure requirement goes beyond the specific categories of information that CCPA requires. This is wrong. This requirement is consistent with Section 1798.100(b). They facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130(a)(5)(B), and therefore fall within CCPA's delegation of authority to the Attorney General.[4] In particular, the requirement to disclose the business or commercial purposes(s) *for each category of personal information* furthers the purpose of "inform[ing] consumers at or before the time of collection of a consumer's personal information"[5], furthers "[t]he right of Californians to know what personal information is being collected about them"[6], and provides Californians with the information that empowers their "right … to say no to the sale of personal information"[7]. Only by knowing the purpose for each category of personal information may consumers meaningfully exercise their right to say no to the sale of personal information.

W227-1 (cont.) W227-2 (cont.) W227-3 (cont.)

Second, some commenters asserted that this disclosure requirement is an undue burden since it would require a business to update its notice at collection and its privacy policy whenever it changes the purposes for which it collects personal information. However, CCPA explicitly dictates that a "business shall not … use personal information collected for additional purposes without providing the consumer with notice".[8] The intent is clear. When a business starts using a category of personal information for a new purpose, the business should inform consumers of this new use of their personal information, so that a consumer may take an appropriate action if desired.

Third, some commenters asserted that this disclosure requirement would make privacy policies too complicated. This is also fallacious. Over 15 years of research has demonstrated multiple effective techniques that can be used to add useful and potentially actionable detail to privacy policies while simultaneously improving readability. Indeed, many businesses already use layered privacy policies, where the top layer is a simple disclosure and the next layer contains additional disclosures of interest to some consumers. For example, Google's privacy policy[9] includes links to certain parts of the top-level disclosure, and when a user clicks on the link it opens a side panel with additional detail. As another example, AT&T's privacy policy[10] includes in each section "LEARN MORE", and when a user clicks on the phrase it expands the section to disclose additional detail. If a business is concerned that disclosing the purposes for each category of information it collects is too complicated for the average consumer, it may simply disclose the purposes *for all collected personal information* in the top layer of its privacy policy and then disclose the purposes *for each category of information* it collects in the next layer of its privacy policy. Surely, such a layered approach would add useful and potentially actionable detail while not reducing the readability of

[4] *CCPA*, Section 1798.185(a)(7).
[5] *Initial Proposed Regulations*, § 999.305(a)(1).
[6] AB 375, Section 2(i)(1).
[7] AB 375, Section 2(i)(3).
[8] *CCPA*, Section 1798.100(b).
[9] Google Privacy Policy, available at https://policies.google.com/privacy?hl=en-US.
[10] AT&T Privacy Policy, available at https://about.att.com/csr/home/privacy/full_privacy_policy.html.

privacy policies. Alternatively, a business may simply place the additional detail at the end of the privacy policy.

It is a reasonable question for the Attorney General's office to ask where in the regulations the requirement to disclose the purpose for collecting each category of personal information should be placed, i.e. in §999.305, §999.308, and/or §999.313. CCPA requires disclosure of purposes for which the categories of personal information shall be used in both the notice at collection[11] and the right to know[12].

In particular, the primary reason for the existence of a notice at collection is to answer the question "Why do you want to collect this category of my personal information?". The regulations should, at a minimum, restore in the notice at collection the requirement to disclose the purpose for collecting each category of personal information.

W227-1 (cont.) W227-2 (cont.) W227-3 (cont.)

2. DISCLOSURE OF PURPOSES FOR SELLING OR DISCLOSING A CATEGORY OF PERSONAL INFORMATION (§999.308 PRIVACY POLICY, AND §999.313 RESPONDING TO REQUESTS TO KNOW)

In the Initial Proposed Regulations §999.313(c)(10), the information that a business shall provide to a consumer in a response to a verified request to know the categories of personal information disclosed or sold included "for each identified category of personal information it has collected about the consumer" "[t]he business or commercial purpose for which it sold or disclosed the category of personal information".[13] However, in the Revised Proposed Regulations §999.313(c)(10), "for each identified category of personal information it has collected about the consumer" was deleted, and "[t]he business or commercial purpose for which it sold or disclosed the category of personal information" was replaced by "[t]he business or commercial purpose for which it … sold the personal information".

W227-4 W227-5

These revisions remove the ability of a consumer to know why a business wants to sell or disclose a category of her personal information. For example, under the Revised Proposed Regulations, a business may now only disclose the following:

> Sharing: The personal information that we share includes: (a) your address and (b) your browsing history.
>
> Purposes: We share some of the personal information we collect for advertising. We share some of the personal information we collect to improve insurance rate-setting.

Under such a disclosure, a consumer will be left in the dark about whether the business shares her browsing history for advertising (i.e., behavioral advertising) or for insurance rate-setting (e.g., risk estimation). These two possibilities have very different consequences, and consumers have the right to know which is occurring.

The comments in the record that objected to the requirements in the Initial Proposed Regulations for a business to disclose the purposes for selling or disclosing a category of personal information presented two objections, both of which are fallacious.

First, some commenters asserted that this disclosure requirement is beyond the ability of most businesses to determine, because businesses do not track this information individually for every consumer. However, this disclosure requires no such thing. It merely requires that a business disclose the purpose for which it

[11] *CCPA*, Section 100(b).
[12] *CCPA*, Sections 110(a)(3), 110(c)(3).
[13] *Initial Proposed Regulations*, § 999.313(c)(10).

sells or discloses each category of personal information. It does not require that a business disclose a different purpose for each consumer. Surely a business knows why it discloses or sells each category of personal information.

Second, some commenters asserted that this disclosure requirement would make privacy policies too complicated. This is also fallacious, for the same reasons given above in section 1 of these comments.

W227-4 (cont.)

The regulations should restore in §999.313(c)(10) the requirement to disclose the purpose for selling or disclosing each category of personal information.

W227-5 (cont.)

In addition, the regulations should place a similar requirement in §999.308(c)(1)(e) to disclose the purpose for selling or disclosing each category of personal information. This proposed requirement is consistent with Sections 1798.110(a), 1798.110(c), and 1798.115(a). It facilitates a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130(a)(5)(B), and therefore falls within CCPA's delegation of authority to the Attorney General.[14] It furthers the purpose of "provid[ing] the consumer with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information"[15], furthers "[t]he right of Californians to know whether their personal information is sold or disclosed and to whom"[16], and provides Californians with the information that empowers their "right … to say no to the sale of personal information"[17]. Only by knowing the purpose for which personal information is shared for each category of personal information may consumers meaningfully exercise their right to say no to the sale of personal information.

3. DISCLOSURE OF CATEGORIES OF SOURCES FROM WHICH A CATEGORY OF PERSONAL INFORMATION WAS COLLECTED (§999.308 PRIVACY POLICY, AND §999.313 RESPONDING TO REQUESTS TO KNOW)

In the Initial Proposed Regulations §999.308(b)(1)(d), the information that a business must include in its privacy policy regarding a consumer's right to know personal information collected included: (i) "the categories of consumers' personal information the business has collected" and (ii) "[f]or each category of personal information collected, … the categories of sources from which that information was collected".[18] However, in the Revised Proposed Regulations §999.308(c)(1)(d), "[f]or each category of personal information collected, … the categories of sources from which that information was collected" was deleted.

W227-6
W227-7

In addition, in the Initial Proposed Regulations §999.313(c)(10), the information that a business shall provide to a consumer in a response to a verified request to know the categories of personal information collected similarly included "for each identified category of personal information it has collected about the consumer" "[t]he categories of sources from which the personal information was collected"[19] However, in the Revised Proposed Regulations §999.313(c)(10), "for each identified category of personal information it has collected about the consumer" was deleted.

---

[14] *CCPA*, Section 1798.185(a)(7).
[15] *Initial Proposed Regulations*, § 999.308(a)(1).
[16] AB 375, Section 2(i)(1).
[17] AB 375, Section 2(i)(3).
[18] *Initial Proposed Regulations*, § 999.308(b)(1)(d).
[19] *Initial Proposed Regulations*, § 999.313(c)(10).

These deletions remove the ability of a consumer to know the category of source from which a business obtained a category of her personal information. For example, under the Revised Proposed Regulations, a business may now only disclose the following:

> Collection: The personal information that we collect includes: (a) your address and (b) your browsing history.
>
> Sources: We obtain some of the personal information that we collect directly from you and we obtain some of the personal information that we collect from Internet Service Providers.

Under such a disclosure, a consumer will be left in the dark about whether the business is obtaining information about her browsing history from her Internet Service Provider. Such information is critical to a consumer's decisions about the use of her personal information.

The comments in the record that objected to the requirements in the Initial Proposed Regulations for a business to disclose the categories of sources from which a category of personal information was collected presented two objections, each of which is fallacious.

First, some commenters asserted that this disclosure requirement goes beyond the specific categories of information that CCPA requires. This is wrong. These requirements are consistent with Sections 1798.100(a), 1798.110(a), 1798.110(c), 1798.115(a), and 1798.115(c). They facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130(a)(5)(B), and therefore fall within CCPA's delegation of authority to the Attorney General.[20] In particular, the requirement to disclose the categories of sources *for each category of personal information collected* furthers the purpose of "provid[ing] the consumer with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information"[21], furthers "[t]he right of Californians to know what personal information is being collected about them"[22], furthers "[t]he right of Californians to know whether their personal information is sold or disclosed and to whom"[23], and provides Californians with the information that empowers their "right … to say no to the sale of personal information"[24]. Only by knowing the categories of sources for each category of personal information may consumers meaningfully exercise their right to say no to the sale of personal information.

W227-6 (cont.)
W227-7 (cont.)

Second, some commenters asserted that this disclosure requirement would make privacy policies too complicated. This is also fallacious, for the same reasons given above in section 1 of these comments.

It is a reasonable question for the Attorney General's office to ask where in the regulations the requirement to disclose the categories of sources from which a category of personal information was collected should be placed, i.e. in §999.308 and/or §999.313. CCPA requires disclosure of categories of sources in the right to know[25]. **The regulations should, at a minimum, restore in §999.313 the requirement to disclose the categories of sources from which each category of personal information is collected.**

---

[20] *CCPA*, Section 1798.185(a)(7).
[21] *Initial Proposed Regulations*, § 999.308(a)(1).
[22] AB 375, Section 2(i)(1).
[23] AB 375, Section 2(i)(1).
[24] AB 375, Section 2(i)(3).
[25] *CCPA*, Sections 110(a)(2), 110(c)(2).

From: Kevin Gould
To: Privacy Regulations
Subject: California Consumer Privacy Act of 2018 -- Revised Rulemaking Comment Letter
Date: Tuesday, February 25, 2020 4:11:14 PM
Attachments: image003.png
California Consumer Privacy Act of 2018 Revised Rulemaking Comment Letter.pdf

---

Thank you for the opportunity to provide written comments on the revised rulemaking pertaining to the California Consumer Privacy Act of 2018. Please find attached a comment letter prepared by the American Bankers Association, the California Bankers Association, the California Mortgage Bankers Association, and the Mortgage Bankers Association. Please let us know if you have any questions. Thank you.

Kevin Gould
SVP, Director of Government Relations
California Bankers Association
1303 J Street, Suite 600 | Sacramento, CA 95814
T: [redacted]
F: (916) 438-4310
Connect: Website | Twitter | LinkedIn

February 25, 2020

Ms. Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

RE: California Consumer Privacy Act of 2018 – Revised Rulemaking Comment Letter

Dear Ms. Kim:

The American Bankers Association (ABA), the California Bankers Association (CBA), the California Mortgage Bankers Association (California MBA), and the Mortgage Bankers Association (MBA) appreciate the opportunity to submit written comments in response to the revised rulemaking undertaken by the California Department of Justice pertaining to the California Consumer Privacy Act of 2018 (CCPA). We appreciate revisions that have been made to the initial draft regulations released on October 11, 2019, that are responsive to the comments we submitted in our December 6, 2019, letter.

ABA 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.

CBA is a division of the Western Bankers Association, one of the largest banking trade associations and regional educational organizations in the United States. CBA advocates on legislative, regulatory and legal matters on behalf of banks doing business in the state of California.

California MBA is a California corporation operating as a non-profit association that serves members of the real estate finance industry doing business in California. California MBA's membership consists of approximately three hundred companies representing a full spectrum of residential and commercial lenders, servicers, brokers, and a broad range of industry service providers.

The Mortgage Bankers Association is the national association representing the real estate finance industry, an industry that employs more than 280,000 people in virtually every community in the country. Headquartered in Washington, DC, the association works to ensure the continued strength of the nation's residential and commercial real estate markets; to expand homeownership; and to extend access to affordable housing to all Americans. MBA promotes fair and ethical lending practices and fosters professional excellence among real estate finance employees through a wide range of educational programs and a variety of publications. Its membership of over 2,200 companies includes all elements of real estate finance: mortgage companies, mortgage brokers, commercial banks, thrifts, REITs, Wall Street conduits, life insurance companies, and others in the mortgage lending field.

As your office prepares to issue final regulations in accordance with the CCPA, we respectfully urge that you consider the following requests to clarify aspects of the proposed regulations and the CCPA. While our letter makes several specific observations regarding the revised regulations, as a general matter, we urge that final regulations avoid inconsistencies with the CCPA, such as the provision in Section 999.315, requiring companies to provide a method of consumer opt-out that does not exist within the current law, and, moreover, that businesses not be required to provide notifications that may confuse consumers and obfuscate relevant information.

The requests outlined below should not be considered an effort to undermine the CCPA but are rather intended to assist in clarifying aspects of the law to better facilitate compliance by financial institutions.

ARTICLE 2: NOTICES TO CONSUMERS. (SECTIONS 999.305-999.308).

- **Notice at Collection of Personal Information. (Section 999.305).**

Revised regulations in Section 999.305(a)(4) require that when a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, the business must provide the consumer a just-in-time notice summarizing the categories of personal information being collected and a link to the full notice at collection. We request this provision be removed or that the regulations clarify when the collection is for purposes a consumer would not reasonably expect. W228-1

Pursuant to Civil Code Section 1798.100(b) of the CCPA, a business must inform consumers, at or before the time of information collection, as to the categories of personal information that will be collected and the purposes for which that information will be used. Should this change—i.e. the business wishes to collect a different category of personal information or use information collected for a different purpose—the business must provide consumers with an updated notification that reflects the change before information collection. As currently proposed, Section 999.305(a)(5) of the draft regulations require much more than the updated notification required by statute. Specifically, under Section 999.305(a)(5), a business that seeks to use W228-2

previously collected personal information for a purpose materially different from the purpose previously disclosed must first obtain the consumer's explicit consent for the new purpose.

Accordingly, we believe that this provision impermissibly amends the statute in place of implementing the intent of the Legislature. Moreover, this requirement creates a conflict between the statute and the regulations. A financial institution that provides notice consistent with the requirements of the law may nonetheless be charged with violating the statute because the regulations provide that a "violation of these regulations shall constitute a violation of the CCPA and be subject to the remedies provided for therein." Given that this concept of obtaining explicit consent for the use of a consumer's personal information for a new purpose goes beyond the text of the CCPA, we request that it be removed. W228-2 (cont.)

In addition, the revised regulations have further confused the notice at collection requirements. Section 999.305(a)(3) has been revised to require that the notice be made "readily available" and it is unclear what the new language means. The proposed regulation does not specify that the notice must always be given in the same location and manner that the information is being collected, but the "illustrative examples" suggest that this may be the case, which is extremely difficult, if not impossible, to comply with. W228-3

- **Privacy Policy. (Section 999.308).**

Revised regulations in Section 999.308(c)(1)(e)(2) require a business to match each category of personal information collected with the categories of third parties to whom information was disclosed or sold. This requirement is excessive and does not meaningfully aid transparency.

Civil Code Section 1798.115 treats information that the business collected and sold differently from personal information the business simply collected or personal information the business collected and disclosed for a business purpose. Under the CCPA, cross-referencing is only required for personal information that is collected and sold.

Specifically, as it relates to personal information that is sold, Civil Code Section 1798.115(a)(2) states specifically, that the business must disclose "the categories of third parties to whom the personal information was sold, by category or categories of personal information for each category of third parties to whom the personal information was sold." This different treatment is a logical consequence of the fact that the statute gives consumers the right to opt-out of sale. A consumer exercising that right has an interest in knowing which information is sold to which third party. The same cannot be said for a business's information collecting or sharing activities given that a consumer's right to opt-out does not extend to these activities. Applying the same level of granularity to information that is collected and shared needlessly complicates the disclosure. This is likely to cloud the facts that are most relevant to the consumer, such as, the categories of third parties to whom the personal information is sold. W228-4

ARTICLE 3: BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS. (SECTIONS 999.312-999.318).

- **Responding to Requests to Know and Requests to Delete. (Sections 999.313).**

Section 999.313(c)(3), as proposed in October 2019, provided that a business shall not provide a consumer with specific pieces of information if the disclosure created "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." The revised regulations have deleted this requirement. We request that the deleted language be reinserted.

W228-5

Without the ability to withhold specific pieces of particularly sensitive information, like usernames and out-of-wallet information, sending responses, for example, in plain text via postal mail as the CCPA allows consumers to request, puts customers and their financial records at risk if a hacker or other bad actor makes the request fraudulently or intercepts the response. Credential stuffing and identity theft is already a security problem, and businesses need the ability to withhold actual data where necessary to protect consumers from fraud.

In the place of the requirement to withhold information that could present a security risk, the revised regulations propose a new exception to the requirement to fulfill consumer requests. While this new exception in Section 999.313(c)(3) is helpful, we are uncertain whether a business will ever be able to satisfy all the conditions in (a)-(d), particularly the requirement in Section 999.313(c)(3)(c) that the business does not use personal information for any commercial purpose. In addition, Section 999.313(c)(3)(b), does not permit a business to retain personal information for internal record-keeping purposes, analytics or quality assurance. We request additional clarity as to these new provisions.

W228-6

W228-7

Further, in retaining section 999.313(c)(3) and subsections (a)-(d), we request clarity on how the provision would apply. As written, the revised provision would excuse a business from requiring it to provide or delete information if the information is not, "in a searchable or reasonably accessible format." We appreciate that the Attorney General recognizes that we cannot provide or delete the information if a business cannot search for it. It further provides, however, in the conjunctive, that all conditions must be met, meaning the business maintains the information only for legal or compliance reasons, does not sell or use it for commercial purposes, and describes for consumers the categories of records that were not searched. What is not clear is, if the information is not searchable, how the other conditions will apply. Perhaps applying this in the disjunctive "or" would resolve this ambiguity, or otherwise further explanation of how this would apply is needed.

W228-8

Revised regulations proposed in Section 999.313(d)(6) pertain to cases where a business denies a consumer's request to delete personal information. New language added to Section 999.313(d)(6)(a) is confusing and onerous. Proposed language requires that a business inform the consumer that it will not comply with the consumer's request to delete and that the business

W228-9

must describe the basis for the denial, including when the business has applied an exception to the CCPA or where there is a conflict with federal or state law.

This new language in Section 999.313(d)(6)(a) conflates two concepts: (1) the application of the statutory exceptions and (2) the actual denial of a request to delete, for instance because a request cannot be verified. If a business deletes information that does not fall into one or more exceptions, but keeps information it is permitted to retain under the CCPA, it has complied with the request. Similarly, if a business after a review of searchable databases, determines that it does not hold personal information of the consumer in such databases, the business has not denied the request. In these situations, a business should not be subject to new and onerous response requirements. W228-9 (cont.)

Section 999.313(d)(6)(c), applicable to a denial of a request to delete, provides that the business is not permitted to use the consumer's personal information for any other purpose than provided for by that exception. This restriction improperly prevents a business from using the consumer's personal information for other lawful purposes including fighting fraud or even completing a consumer's transaction if that reason was not included in the denial letter. Accordingly, we request that these provisions be removed from the regulation. W228-10

- **Service Providers. (Section 999.314).**

The revised rule now provides at section 999.314(c)(3) that a service provider may retain, use, or disclose personal information obtained in the course of providing services for "internal use by the service provider to build or improve the quality of its services, *provided that the use does not include building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source.*" (emphasis added). This may be inconsistent with CCPA section 1798.140(v) (definition of "service provider") whereby a service provider is permitted to use the personal information to fulfill the terms of the contract, and where a contract may allow or require a service provider to use the information to clean or augment the data acquired from another source. We ask that the language in this subsection allow for a service provider to use the information in accordance with its contract. W228-11

- **Requests to Opt-Out. (Section 999.315).**

Section 999.315(f) requires that a business must act on a consumer's request to opt-out of the sale of their personal information in no more than 15 business days. This period of time is significantly less than the time period provided to a business responding to a request to know or delete (45 days). Where a consumer makes an opt-out request, particularly a consumer who has authorized another person to opt-out of sale on their behalf, this proposed 15 business day deadline fails to provide sufficient time to confirm that the individual making the request has the proper authorization. We request that this provision be removed or extended to 45 days. W228-12

Section 999.315(f) also requires a business that sells a consumer's personal information to notify those third parties to whom it has sold the personal information that the consumer has exercised their right to opt-out and instruct them not to sell that consumer's information. This requirement is inconsistent with the corresponding provisions in CCPA, wherein a business is only required to cease selling the information it has collected from the consumer. Under the CCPA, the business in not required to take the additional, burdensome step of contacting third parties and instructing them to cease selling the consumer's personal information. Since this provision in the regulation is inconsistent with the corresponding provision in CCPA and given that consumers are adequately protected by existing law, we request that this section be removed from the proposed regulations. W228-13

The proposed regulations have introduced a method for consumers to opt-out that is not included in the CCPA. The concept of "user-enabled global privacy controls" in Section 999.315(g) is entirely new. In this regard, the regulations recognize the use of "user-enabled privacy global controls, such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information…" This new requirement is inconsistent with the CCPA.

Existing law includes robust provisions establishing how a business must communicate a consumer's right to opt-out and provides acceptable methods to evidence the consumer's intent to opt-out. It is unclear why these carefully considered provisions should be augmented by adding new, largely unproven opt-out channels without first assessing their effectiveness and consumer value. In addition, businesses may not be able to comply with this new requirement without the technological capability to track or respond to such browser plugins or similar mechanisms. W228-14

Since this provision in the regulation is inconsistent with the corresponding provision in CCPA and given that consumers are adequately protected by existing law, we request that this provision be removed from the regulations. In the alternative, we request that the effective date of this provision be delayed, thereby allowing businesses the opportunity to investigate and test the effectiveness of user-enabled controls, and should it be necessary an opportunity to make adjustments to ensure they are positioned to comply with the provision.

- **Training: Record-Keeping. (Section 999.317).**

Revised regulations pertaining to record-keeping proposed in Section 999.317(e) include an express prohibition on sharing information maintained for record-keeping purposes with any third party. This new requirement directly conflicts with a central goal of the regulations, which is to permit record sharing with regulators. Particularly for highly regulated financial institutions, a prohibition on sharing records with third parties, such as state and federal regulators, agencies, and other parties who request them via lawful process is untenable. We request this new provision be removed. W228-15

Section 999.317(g) of the proposed regulations expand record-keeping obligations for businesses that buy, receive, sell or share the personal information of ten million or more consumers. For companies that meet this threshold, the regulation requires publishing consumer request metrics in the business's privacy policy or website. This mandate is not derived from the CCPA and does not benefit consumers. Nor do the regulations provide any guidance relating to the calculation of the ten million consumers. We urge that this provision be removed from the regulations or alternatively that the requirement to publish these metrics be replaced with a requirement that they be provided to your office upon request. W228-16

- **Requests to Access or Delete Household Information. (Section 999.318).**

Revised regulations in Section 999.318 reflect improvements for requests to know or delete personal information for "households." We continue to have significant concern with these requirements. Operationally, it will be impossible to ascertain who occupies a residence on a given date, how to identify an intent to submit a joint request and whether anyone age 13 or younger is a household member.

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. W228-17

For these reasons, we urge the deletion of "household" from the definition of "personal information." We believe the unauthorized disclosure or deletion of personal information by one household member is an unintended consequence of the CCPA. If the final rule does not delete "household" from the definition of personal information or otherwise exempt businesses from disclosing personal information or deleting personal information 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 personal information.

ARTICLE 4: VERIFICATION OF REQUESTS. (SECTIONS 999.323-999.326).

- **Provide additional clarity around what is necessary, and what will be deemed in compliance, when authenticating a verifiable consumer request and include a safe harbor. (Sections 999.323-999.325).**

As part of routine transactions with consumers, financial institutions collect personal information in order to facilitate customer requests. Furnishing personal information to consumers purporting to exercise their rights under the CCPA, in response to a verifiable consumer request, may result in unintended risk and harm to the consumer, including misuse of personal information to perpetrate fraud and identity theft. W228-18

A business receiving a consumer's request will need sufficient data to verify the consumers identity as a safeguard to ensure the information provided in return is associated with the requesting individual. Regulations established by the Attorney General should provide flexibility for a business to decline a consumer's request where the data presented by the consumer is insufficient to authenticate a request. Further, in circumstances where limited information is provided by the consumer, a business endeavoring to authenticate a request should have flexibility, but not be required, to furnish non-sensitive personal information (excluding personal information that if disclosed would otherwise result in a data breach) to the consumer as a means to satisfy its compliance and to protect the consumer against fraud and identity theft. W228-18 (cont.)

We believe that a safe-harbor from liability should be granted to businesses that satisfy the criteria adopted pursuant to the promulgated regulations, or situations where the evidence shows the business was justified to use the degree of due diligence it did in verifying the identity of the requestor. Financial institutions generally have been quite capable in identifying false requests for information. Limiting the tools institutions can use to protect consumers' personal information from false requestors will not promote consumer protection.

Further, the new requirement added in Section 999.323(d) that businesses not charge consumers for proper identity verification is overbroad and needs refinement. Paired with the example highlighted in the revised regulations, this new language effectively discourages the use of notaries, which is a commonly accepted legal method for authenticating the identity of an individual. The Uniform Statutory Form Power of Attorney (California Probate Code Section 4401) even references the attachment of a required notary certification. W228-19

When read in tandem with Section 999.326(b), which explicitly references the Probate Code's requirements as a means for businesses to streamline the verification of authorized agents, the new text in Section 999.323(b) creates an unnecessary barrier to consumer choice and a direct conflict with Section 999.323(e)'s requirement that businesses "implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information."

Businesses required to ensure the security of the personal information they are tasked with disclosing or deleting should not be penalized for employing a separately required method for authenticating legal affidavits signed by consumers. We recommend that the regulations make clear that use of a notary to verify the identity of the consumer does not trigger a monetary penalty to businesses looking to secure personal information when a consumer chooses to exercise his or her rights under the CCPA.

Section 999.325(b)-(c) appears to identify two potential distinct tiers of authentication for requests for rights to know, depending on whether the request is for categories or specific pieces of personal information. This two-tiered approach imposes additional burdensome implementation requirements beyond the statute. We request that this two-tiered system be optional or removed from the regulations. W228-20

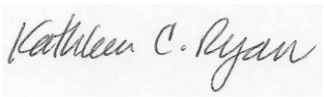
Section 999.326(a) outlines procedures for verifying a request sent by an authorized agent. The revised proposal states that the business may require the consumer to provide "written and signed" permission to the agent. The regulations should clarify what is meant by "written and signed." Additional clarity is need regarding verification. Specifically, the proposal states that a business may also require the consumer to verify their own identity directly with the business. If the business requires the consumer to verify their own identity, the regulations should clarify that the 45-day period to respond to the request does not begin until the business makes contact with the consumer (and not from the date the request is received from the authorized agent). W228-21 W228-22

CONCLUSION

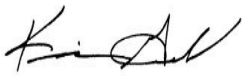
We appreciate the opportunity to comment on the proposed revisions to the draft regulations released in October 2019. With this comment letter endeavoring to focus on the revised provisions to the draft regulations, we respectfully wish to redraw your attention and underscore comments we included in our letter dated December 6, 2019. In addition to the comments provided herein, we urge that the final regulations: provide sample notification forms; clarify that the 12-month lookback period in Civil Code Section 1798.130 applies from January 1, 2020; exempt from the Act trade secrets and intellectual property, including data that, if disclosed, would impede the prevention and detection of fraud or the authentication of an individual; and, grant an 18-month implementation period for the final regulations. W228-23

Thank you again for the opportunity to comment. We welcome any questions you may have regarding our letter.

Sincerely,



Kathleen C. Ryan
Vice President and Senior Counsel
American Bankers Association



Kevin Gould
SVP/Director of Government Relations
California Bankers Association

Susan Milazzo
Chief Executive Officer
California Mortgage Bankers Association

Pete Mills
Senior Vice President, Residential Policy & Member Engagement
Mortgage Bankers Association

From: Alex Propes
To: Privacy Regulations
Subject: Interactive Advertising Bureau Comments on Proposed Modified CCPA Regulations
Date: Tuesday, February 25, 2020 4:06:31 PM
Attachments: IAB Comments on Proposed Modified CCPA Regulations.pdf

---

Please find attached written comments by the Interactive Advertising Bureau in response to the proposed modified CCPA regulations. We appreciate this opportunity to submit these comments. If you have questions, please contact me.

Kind regards,

Alex Propes
Vice President, Public Policy & International
Interactive Advertising Bureau
Office: [redacted]
Mobile: [redacted]

February 25, 2020

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

Submitted via privacyregulations@doj.ca.gov

RE: California Consumer Privacy Act Proposed Modified Regulations

The Interactive Advertising Bureau ("IAB") provides these comments on the proposed modified regulations issued by the California Attorney General ("AG") on February 10, 2020 to implement the California Consumer Privacy Act ("CCPA").

Founded in 1996 and headquartered in New York City, the IAB (www.iab.com) represents over 650 leading media and technology companies that are responsible for selling, delivering, and optimizing digital advertising or marketing campaigns. Together, our members account for 86 percent of online advertising in the United States. In California, we contribute $168 billion to the state gross domestic product and support over 478,000 full-time jobs in the state.[1] Working with our member companies, the IAB develops technical standards and best practices and fields critical research on interactive advertising, while also educating brands, agencies, and the wider business community on the importance of digital marketing. The organization is committed to professional development and elevating the knowledge, skills, expertise, and diversity of the workforce across the industry. Through the work of our public policy office, the IAB advocates for our members and promotes the value of the interactive advertising industry to policymakers and legislators across the country.

IAB broadly supports the CCPA's purpose and intent to enhance consumer privacy by providing transparency and choice about the use of personal information. And we appreciate the AG's consideration of our comments to the AG from December 6, 2019. However, certain provisions of the modified rules continue to stray from or contradict the text of the CCPA itself. Other provisions, as drafted, may ultimately reduce consumer choice and undermine privacy, rather than advancing it. IAB urges the AG to consider consumers' support for the ad-driven Internet model and asks the AG to update the modified rules so they empower consumers by giving them increased choices and control over online data. IAB provides the following comments below, addressing specific provisions of the modified rules that should be updated or clarified to further consumer choice and privacy and enable compliance with the law.

I. Update the Guidance Regarding the Definition of "Personal Information" to Encourage Privacy by Design

[1] John Deighton, *The Economic Value of the Advertising-Supported Internet Ecosystem* (2017), available at https://www.iab.com/insights/economic-value-advertising-supported-internet-ecosystem/.

The modified regulations state as an example that "if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be "personal information."[2] Businesses that maintain pseudonymous information such as an IP address are often structured to separate that non-identified information from a consumer's identity. Furthermore, businesses often apply security measures, such as encryption, and administrative controls, such as contractual requirements, to further protect the consumer. The modified regulations do not clarify what would constitute the ability to "reasonably link" information with a particular consumer or household. They consequently emphasize an indeterminate and ambiguous standard in the definition of personal information without providing any clarity as to what it means. We encourage the AG to recognize privacy by design measures taken by businesses to separate identifiable data from non-identifiable data and clarify the draft rules by modifying section 999.302 as follows: W229-1

> *Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "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." For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be "personal information."*

II. Clarify that Notice Obligations for Data Brokers Apply to Explicit Notice

The modified regulations state that "a business that does not collect information directly from consumers [that] is registered with the Attorney General as a data broker pursuant to Civil Code section 1798.99.80, et seq…. does not need to provide a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out."[3]

However, the regulations do not specifically indicate whether or not this section also applies to the explicit notice requirements for onward sales of personal information about a consumer by a third party that appear in the text of the CCPA. The CCPA itself states that a third party may not "sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provide an opportunity to exercise the right to opt-out pursuant to Section 1798.120."[4] We ask the AG to clarify that a business has met its "explicit notice" and opt-out opportunity requirements under 1798.115(d) if it is registered as a data broker and includes in its registration submission a link to its online privacy policy with instructions on how a consumer can submit a request to opt-out. This clarification would help bring the CCPA's express provisions regarding explicit notice in line with the modified proposed rules' terms, thereby enhancing clarity and consistency within the CCPA's regulatory framework. W229-2

[2] Cal. Code Regs. tit. 11, § 999.302(a) (proposed Feb. 10, 2020).
[3] *Id*. at § 999.305(d).
[4] Cal. Civ. Code § 1798.115(d).

III. Ensure Requirements for an Opt-Out Button Align with CCPA Requirements

The CCPA requires businesses to "[p]rovide a clear and conspicuous link on the business's internet homepage, titled 'Do Not Sell My Personal Information,' to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information."[5] The modified regulations state that "[w]hen the opt-out button is used, it shall appear to the left of the 'Do Not Sell My Personal Information' or 'Do Not Sell My Info' link as demonstrated below, and shall be approximately the same size as other buttons on the business's webpage."[6] This provision of the draft regulations is ambiguous and fails to capture the nuances of providing consumer choice across diverse contexts and applications. It refers to "the opt-out button" generally, and therefore it is unclear whether the regulation is specifying that businesses must place the button *next to* the "Do Not Sell My Personal Information" link on their webpage, or whether the regulation is only requiring a toggle button, and unclearly describing where the toggle button is required to be placed. It is also unclear whether the toggle button or the opt out link itself must "link to a webpage or online location containing the information specified in section 999.306(c)." W229-3

In order for this instruction from the AG to be consistent with the requirements of the CCPA, the AG should clearly state that when used, a toggle button is required to be placed next to the words "Do Not Sell My Personal Information" or "Do Not Sell My Info" on an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information." The regulations need to make clear that a toggle button is not required to be placed on a business's homepage next to the "Do Not Sell My Personal Information" link or in the business's privacy policy.

IV. Remove the Requirement to Provide an Estimate of the Value of Consumer Data and the Method of Calculating the Value of Consumer Data in a Notice of Financial Incentive

If a business offers a financial incentive or a price or service difference to a consumer in exchange for the retention or sale of personal information, the proposed regulations require the business to provide a notice to the consumer that includes: (1) 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 (2) a description of the method the business used to calculate the value of the consumer's data.[7] IAB respectfully asks the AG to remove the requirement to provide an estimate of the value of the consumer's data and the method of calculating such value, as these obligations are not contemplated by the CCPA itself, would be difficult if not impossible for a business to provide, and could potentially reveal confidential or proprietary information about the business's internal practices and economic assessments. W229-4

First and foremost, the requirement to provide an estimate of the value of the consumer's data and the method of calculating such data exceeds CCPA's statutory obligations. These provisions of the proposed regulations represent brand new business obligations that were not

[5] *Id*. at § 1798.135(a)(1).
[6] Cal. Code Regs. tit. 11, § 999.306(f)(2) (proposed Feb. 10, 2020).
[7] *Id*. at § 999.307(b)(5).

included in the text of the CCPA itself. Businesses have spent over a year preparing for the CCPA's effective date of January 1, 2020. Adding substantial and disruptive new requirements to the CCPA, such as these requirements related to financial incentives, mere months before the law will go into effect causes significant compliance complications and challenges for businesses of all sizes.

Second, it may be impossible for businesses to comply with the requirement to provide an estimate of the value of the consumer's data, because data lacks clear, objective value. Academics have come up with wildly different estimates for the value of data-enabled services,[8] and experts are likely to come up with differing values for these services in the future as well. The reason certain businesses can offer their services free of charge is because they derive revenue from selling advertisements. Businesses sell advertisers the opportunity to present their messages to users, and advertisers pay businesses based on objective metrics such as the number of people who see their ads or the number of people who click on their ads. As a result, any revenue linked to a particular advertising campaign is determined when the campaign is completed. The final figures, however, have little relation to any single consumer's data, and thus providing an estimation of the value of such data would be inaccurate and misleading to consumers.

W229-4 (cont.)

Finally, the requirement to provide an estimate of the value of the consumer's data and the method for computing such value could expose confidential, proprietary business information or put a business's competitive position at risk.[9] The method by which a business values personal information associated with a consumer may constitute proprietary information about the business's commercial practices. Forcing businesses to reveal such confidential, secret information could harm businesses' ability to compete in the marketplace, as competitors and customers would become aware of the value a business has assigned to the data it maintains. Obligating businesses by law to reveal this information could harm the economy and healthy business competition by forcing companies to reveal confidential information.

For the foregoing reasons, IAB asks the AG to remove the proposed regulations' requirement that a business must, in a notice of financial incentive, provide an estimate of the value of the consumer's data and the method by which it calculated such value. This directive constitutes a requirement that goes far beyond the requirements of the CCPA itself.

V. Ensure Requirements for Requests to Know and Delete Align with the CCPA's Text, Consider Real-World Implications, and Empower Consumer Choice

Certain provisions in the proposed regulations set forth rules about consumer requests to know and requests to delete that do not align with the CCPA, and other portions of the proposed

[8] Asha Saxena, *What is Data Value and should it be Viewed as a Corporate Asset?* (2019), located at *https://www dataversity net/what-is-data-value-and-should-it-be-viewed-as-a-corporate-asset*

[9] IAB also respectfully disagrees with the AG's assessment that providing consumers with these calculations will provide meaningful information about the costs and benefits of the financial incentive to the consumer specifically. *See* Office of the California Attorney General, *Initial Statement of Reasons for Proposed Adoption of California Consumer Privacy Act Regulations* at 12 (Oct. 2019) (hereinafter, "ISOR"), located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccps-isor-appendices.pdf. The calculations described in the proposed regulations reflect the value proposition to the business, not to the consumer, as expressly indicated in Section 999.301(w).

regulations fail to consider significant real-world outcomes associated with their requirements. Finally, some of the provisions thwart consumers' ability to make choices and require businesses to take action on personal information in ways that may not be approved by the consumer. IAB requests that the AG update the proposed rules, as further described below, to conform them with the CCPA's text, better align them with practical realities, and empower consumers to make meaningful choices that businesses must respect.

a. Expressly acknowledge that a business may withhold specific pieces of personal information if divulging such information could lead to unreasonable security risks

The modified regulations remove language that states "[a] business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks."[10] The modified regulations replace this language with language relating to when a business is not required to search for personal information when responding to requests to know.

W229-5

In many instances, businesses may not be able to verify consumers to a degree of certainty necessary to disclose specific pieces of personal information. For example, a business may maintain data that would not, on its own, be associated with a named actual consumer. For example, a company may associate a random ID number with other non-identifying information about a consumer for internal use only. Because this information may not be tied to actual consumer names or identifying information, businesses holding such information may not be able to verify a consumer's request for specific pieces of personal information to a "reasonably high degree of certainty," as the consumer may not be able to provide "pieces of personal information" the business would need to verify the consumer's request.[11] However, in the absence of clear guidance, as provided in the previous draft regulation, that a business shall not provide consumers with specific pieces of information, a business may feel compelled to divulge the information it maintains due to a legal requirement. This result could put the consumer, the consumer's information, and/or the business at unreasonable risk, such as unauthorized access. Such a requirement would be contrary to the intent of CCPA and less privacy protective for consumers. IAB requests that the AG reinsert the provision that was deleted from section 999.313(c)(3) that enables a business to decline to provide specific pieces of information to a consumer if doing so would create a substantial, articulable, and unreasonable risk to the security of that personal information.

b. Provide needed improvements on the scope of the right to know considering the burden on businesses.

The modified regulations include new limitations on when a business is required to search for personal information in response to a request to know.[12] However, these limitations are too narrow to effectively protect consumers from the risks associated with identifying,

W229-6

[10] Cal. Code Regs. tit. 11, § 999.313(c)(3) (proposed Feb. 10, 2020).
[11] Cal. Code Regs. tit. 11, § 999.325(c) (proposed Feb. 10, 2020).
[12] Cal. Code Regs. tit. 11, § 999.313(c)(3) (proposed Feb. 10, 2020).

compiling, and making available upon request detailed information. Furthermore, the modified regulations create significant costs for businesses.

Under the proposed regulations, a business would not be required to search for personal information that the business (1) does not maintain in a searchable or reasonably accessible format; (2) maintains solely for legal or compliance purposes; and (3) does not sell and does not use for any commercial purpose. In most instances, it is unlikely that personal information would meet these requirements. As a result, the proposed regulations provide for few practical limitations on access requests, and businesses could be required to associate information with an identifiable consumer than they would otherwise keep separate and secure. IAB suggests the AG revise the regulations to permit businesses not to provide personal information that meets any, rather than all, of the conditions in section 999.302(c)(3). In addition, IAB suggests an new limitation in section 999.302(c)(3) for personal information the business does not associate with an identifiable consumer in the ordinary course of business.

W229-6 (cont.)

VI. The AG Should Modify Service Provider Requirements to Provide Greater Certainty and Align with Business Realities

The modified regulations exclude "cleaning or augmenting data acquired from another source" as a permissible internal use by a service provider.[13] The regulations do not define these new terms. To avoid unnecessary confusion, better align the text of the regulations with the legislative intent of the CCPA, and preserve service provider uses that have clear consumer privacy benefits, IAB asks that the AG remove "cleaning or augmenting data acquired from another source" from the modified regulations.

W229-7

The ability of service providers to conduct ordinary business activities, such as updating data with a service provider's data, provides a variety of benefits to consumers. For example, cleaning or augmenting data could include activities that allow service providers to correct personal information and better ensure that it is accurate, which enhances consumer privacy. Without this ability, for example, service providers would not be able to accurately update consumers' postal addresses when they relocate. This could result in consumers receiving mail and other information, such as offers and notices, that are not relevant to or intended for them. Consequently, restricting service providers' ability to clean data could result in consumers receiving more information than they presently do. Service providers' ability to internally clean and augment personal information to improve services makes the overall market more efficient and provides a benefit to both consumers and businesses alike. Accordingly, this valuable and privacy enhancing activity should not be limited or restricted.

VII. The AG Should Remove the Obligation for Businesses to Comply with User-Enabled Privacy Controls, Such as Browser Settings

W229-8

The proposed regulations state that "[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 request submitted… for that

[13] *Id*. at § 999.314(c)(3).

browser or device, or, if known, for the consumer."[14] This proposed regulation exceeds the CCPA's scope, imposing new substantive requirements on businesses that the legislature has previously considered and elected to not include.[15] We request that the AG remove this requirement, or alternatively, where a business offers a "Do Not Sell My Info" link as a means to opt out from sale, the business should not be required to treat the proposed user-enabled privacy controls as a verifiable opt-out request. Such an approach would be consistent with the approach taken by the legislature when it amended the California Online Privacy Protection Act.

Mandating that businesses treat browser-based signals as valid consumer opt-out requests removes the option for consumers to make their own choices regarding the selling of personal information directly with relevant businesses. Given the CCPA's broad definition of sale, which may cover a range of activities that the ordinary consumer would not regard as a "sale" of personal information, it is further questionable whether a global device setting accurately reflects this intent on the part of consumers. Such settings mean that consumers would be limited from allowing some businesses to sell data while prohibiting others from engaging in these uses. This result would remove meaningful consumer choice from the marketplace and reduce the options available to consumers to set personalized preferences for the use and transfer of data.

W229-8 (cont.)

In addition, requiring businesses to honor user-enabled privacy controls could enable intermediaries to tamper with or block the individualized choices that consumers communicate directly to businesses. For example, intermediaries can interfere with businesses that use plugins, cookies, JavaScript, and other technologies to catalog and act on consumer preferences. Intermediaries such as browsers stand between consumers and businesses in the Internet ecosystem and provide no way for individual businesses to verify whether an expressed privacy control signal is truly a consumer-set preference. These parties are able to manipulate signals and alter settings in ways that may not reflect actual consumer preferences and could potentially stand in the way of a consumer's actual choice being expressed or communicated to a business. As such, concentrating power in the hands of these intermediaries could hinder consumers' from seeing their actual choices expressed in the marketplace, which could have a negative revenue impact on the publishers and services consumers rely on and trust.

The AG takes the position that in the absence of mandatory support for privacy controls, "businesses are likely to reject or ignore consumer tools."[16] While it is true that adoption of certain existing privacy controls has varied across publishers and platforms (*i.e.*, adoption of the Do-Not-Track standard), IAB urges the AG to recognize that the CCPA is without precedent and represents a fundamental shift in California privacy law. IAB expects to see market forces continue to drive strong demand for compliance solutions that can facilitate both consumer choice and business compliance. Throughout the online ecosystem, IAB also expects to see consumers take advantage of multiple compliance solutions, informed by privacy notices directing consumers on how to communicate their privacy choices. Mandating that businesses respect ill-defined global opt-out technologies could impede the development of various helpful tools and solutions for consumers to use to exercise choice in the marketplace, increasing the

[14] *Id*. at § 999.315(d).
[15] *See* AB 370 (Cal. 2013); AB 25 (Cal. 2019); AB 874 (Cal. 2019); AB 1146 (Cal. 2019); AB 1355 (Cal. 2019); AB 1564 (Cal. 2019).
[16] *See* ISOR at 24.

likelihood of disharmonized and conflicting signals. This could create confusion and uncertainty for consumers and businesses alike.

For these reasons, and in light of significant issues around reliability and authenticity of browser-based signals as well as difficulties with clearly communicating which consumers are California residents, it would be premature to regulate in this area or mandate that every business comply with each and every type of user-enabled signal developed to facilitate CCPA compliance. We therefore respectfully ask the AG to remove the requirement to treat user-enabled privacy controls as valid requests to opt out of personal information sale and update the draft rules so that businesses may respect such user-enabled controls *or* offer consumers with another workable method to opt out of personal information sale, such as a "Do Not Sell My Personal Information" button.

W229-8 (cont.)

VIII. Provide Additional Flexibility for the Two-Step Requirement for Opting In to the Sale of Personal Information

Per the proposed rules, if a consumer wishes to opt in to the sale of personal information after previously opting out of such sale, the consumer must undertake a two-step process to confirm their choice to opt in.[17] "Requests to opt-in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in."[18] This two-step requirement creates unnecessary friction in the user experience and makes it more difficult for businesses to take action to effectuate a consumer's valid choice to opt in to personal information sale. Businesses should be able to accept a consumer's single communication of a desire to opt in to personal information sale as a legitimate consumer preference and should be able to act on that validly communicated consumer choice. IAB therefore requests that the AG reconsider this requirement to empower businesses to act on consumers' expressed choices to opt in to personal information sale after previously opting out.

W229-9

IX. Clarify that Businesses Need Not Keep Records About Opt Out Requests Served on Other Businesses

The proposed regulations require all businesses to "maintain records of consumer requests made pursuant to the CCPA and how the business responded to said requests for at least 24 months."[19] This requirement creates compliance challenges for businesses when it comes to retaining records about consumer opt-out requests depending on the actual entity that is effectuating the opt out. For example, in many situations in the online Internet ecosystem, first-party publisher businesses may not have any control over or the ability to know how a third-party business responds to a consumer's opt-out choice. IAB therefore asks the AG to clarify that businesses only must keep records about the opt out requests they receive directly from consumers and the actions the business itself took to respond to those requests. Businesses should not be required to maintain information about other businesses' responses to consumer opt out requests.

W229-10

[17] Cal. Code Regs. tit. 11, § 999.316(a) (proposed Feb. 10, 2020).
[18] *Id.*
[19] *Id.* at § 999.317(b).

X. Affirm that Businesses Are Not Required to Identify Pseudonymized Information Stored in a Manner that is Non-Identifiable and Not Associated with an Actual Person

The proposed regulations state that "[w]henever feasible," a business must "match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service" in order to verify a consumer request.[20] This requirement threatens to destroy the longstanding privacy-protective business practice of keeping pseudonymized and non-identified personal information separate from personal information that could identify a consumer. In addition, this requirement may contravene a provision in the proposed regulations stating that "[i]f 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," a concept that is also mirrored in the CCPA itself.[21] IAB therefore asks the AG to clarify that businesses are not required to identify pseudonymized information stored in a manner that is non-identifiable and not associated with a named actual person in order to effectuate CCPA requests. W229-11

Businesses that maintain non-identified data such as cookie or device IDs are usually structured to separate that non-identified information from a consumer's identity. This practice is privacy-protective for consumers, because it maintains a level of anonymity for the consumer within the business's database. Without an update to the proposed rules, businesses may feel compelled to collect information from consumers so that they can associate or combine non-identifiable personal information with identifiable personal information to meet the CCPA's verification requirements. IAB therefore respectfully asks the AG to clarify the proposed rules such that businesses do not need to identify non-identified information with a named actual person in order to facilitate CCPA requests. This clarification would benefit consumers by keeping non-identified data separate from other personal information that directly links it to an identified consumer.

* * *

We appreciate the opportunity to submit these comments, and we look forward to working with the AG on developing final regulations to interpret the CCPA. If you have questions, please contact me at [redacted].

Respectfully submitted,

Alex Propes
Vice President, Public Policy & International
Interactive Advertising Bureau

[20] *Id*. at § 999.323(b)(1).
[21] Cal. Civ. Code § 1798.145(k); Cal. Code Regs. tit. 11, § 999.323(f) (proposed Feb. 10, 2020).

From:	Peter Leroe-Muñoz
To:	Privacy Regulations
Subject:	Written Comments on Proposed CCPA Regulations, modified on February 10, 2020| Silicon Valley Leadership Group
Date:	Tuesday, February 25, 2020 4:02:22 PM
Attachments:	Attorney General CCPA Regulations 2.0 - Public Comment - FINAL.pdf

Please find attached written comments from the SV Leadership Group regarding the Attorney General's proposed regulations for the CCPA, modified on February 10, 2020.

We look forward to working with the Attorney General to clarify the CCPA and ensure that its operation and enforcement protects consumers and enables economic growth.

Best,
Peter

Peter Leroe-Muñoz
General Counsel & Vice President, Tech & Innovation
Silicon Valley Leadership Group
[redacted]

SILICON VALLEY LEADERSHIP GROUP

2001 Gateway Place, Suite 101E
San Jose, California 95110
(408)501-7864 svlg.org

CARL GUARDINO
President & CEO

February 19, 2019

Honorable Xavier Becerra
California Attorney General

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

RE: California Consumer Privacy Act – Proposed Regulations of

Honorable Xavier Becerra:

I am writing on behalf of the Silicon Valley Leadership Group to provide feedback on the second draft of the California Consumer Privacy Act (CCPA) Implementation Regulations that were released on February 7, 2020.

The Leadership Group was founded in 1978 by David Packard of Hewlett-Packard and represents more than 350 of Silicon Valley's most respected employers. Leadership Group member companies collectively provide nearly one of every three private sector jobs in Silicon Valley and we have a long history of supporting policies that promote innovation, stronger economic growth and improved transportation in California.

Our feedback for additional improvements to the proposed regulations is provided in the attached Appendix A.

We are eager to work with your office to help clarify portions of the CCPA, bring greater certainty to consumers and business about their respective rights and responsibilities, and establish a framework that promotes both privacy and economic growth.

Sincerely,

Peter Leroe-Muñoz
General Counsel and VP of Tech & Innovation Policy
Silicon Valley Leadership Group

SILICON VALLEY LEADERSHIP GROUP

APPENDIX A

Public Comment on California Consumer Privacy Act Proposed Regulations

§ 999.305(a)(5) Notice at Collection of Personal Information
Where a business has proactively and directly notified consumers that the business intends to use personal information in a new way, explicit consumer consent should not be required for such use. W230-1

§ 999.305, § 999.306, § 999.307, § 999.308 Notices and Privacy Policy
Web content accessibility requirements are sufficiently important that they deserve their own legislation or regulation, and should not be drafted onto unrelated regulations. W230-2

§ 999.306 Notice of Right to Opt-Out of Sale of Personal Information
A business should be exempt from providing a notice of a right to opt-out when the business publishes a change in its Privacy Policy for a determined period of time to give consumers the right to opt-out. W230-3

§ 999.307(b) Notice of Financial Incentive
This section should eliminate language referencing any estimated value of a consumer's data, as well as any description of the methodology for calculating such value. Determining the value of any particular consumer's personal information is highly-specific and time-intensive. Moreover, any estimation would require significant speculation at the time of collection, rendering the calculation unreliable. W230-4

§ 999.312(e) Methods for Submitting Requests to Know and Requests to Delete
If a consumer submits a request in a non-conforming method or manner, businesses should not attempt to treat the request as if it were properly submitted, nor should they be required to remedy any such request. W230-5

§ 999.313(b) Responding to Requests to Know and Requests to Delete
The proposed requirement that businesses are required to respond to a request within 45 days of receipt should be amended to "respond within 45 days of when the request was verified." This allows businesses to properly verify requests, which may take an extended period of time through no fault of the businesses. W230-6

§ 999.317 Training; Record-Keeping
The requirement of maintaining records of consumer requests for a minimum of 24 months is overly lengthy. W230-7

§ 999.323(f) General Rules Regarding Verification
Businesses should be able to use their industry's standard authentication methodology to verify information submitted in consumer requests. This methodology may be promulgated by industry associations, research institutions, or common business practice. W230-8

§ 999.337 Calculating the Value of Consumer Data

Determining the value of any particular consumer's personal information is highly-specific and time-intensive. Moreover, any estimation would require significant speculation at the time of collection, rendering the calculation unreliable. This element should be removed from consideration.

W230-4 (cont.)

From: Tavana, Ayla
To: Privacy Regulations
Cc: Forsheit, Tanya
Subject: 2020.02.25 NMA California AG Regs Comments
Date: Tuesday, February 25, 2020 4:00:06 PM
Attachments: NMA California AG Comments Final-c.pdf

Hello,

On behalf of Tanya Forsheit, Frankfurt Kurnit Klein & Selz, attached please find Comments on the Modified CCPA Regulations submitted by the News Media Alliance.

Thank you,
Ayla

Ayla Tavana | Office Coordinator
Frankfurt Kurnit Klein & Selz PC
2029 Century Park East Suite 1060N | Los Angeles, CA 90067
t: [redacted] | f: (347) 438-2149 | [redacted]

February 25, 2020

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

Dear Attorney General Becerra,

The News Media Alliance (the "Alliance") commends the Office of the Attorney General for its thoughtful modifications to the proposed California Consumer Privacy Act of 2018 ("CCPA") regulations (the "Regulations") issued on February 7 and 10, 2020 (the "Modified Regulations"). It submits these new comments on the Modified Regulations in the interest of further strengthening the Regulations to foster consumer protection and business compliance.

The Alliance represents over 2,000 media outlets and works every day to protect the interests of the free press and the more than 120 million adults that read a daily or Sunday print paper. Alliance members hold our nation's leaders accountable by providing cost-efficient, independent news sources for all consumers. Consumers put their trust in our members every time they read an article or access other content via a member publication. This trust is important to our members and motivates our efforts to advocate for a well-designed privacy law.

I. The Regulations Should Provide Further Guidance on Requirements and Methods for Honoring "Global Privacy Controls"

A. The Regulations Should Define and Provide Examples of "Global Privacy Controls"

The Modified Regulations were revised to now provide as follows:

> If a business collects personal information from consumers online, the business shall treat user-enabled ***global*** privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.[1]

W231-1

[1] 11 CCR §999.315(d) (*emphasis added*).

The Alliance respectfully requests that the Attorney General define and include examples of "global privacy controls" for purposes of this provision. For example, if the Attorney General intends that existing "Do Not Track" signals, which differ by browser type, must be honored as an opt-out of sale, the Regulations should so state and should (a) explain the relationship between "Do Not Track" signals and the "Do Not Sell My Personal Information" link required under the CCPA; and (b) provide guidance on specific technological steps publishers and other websites must take for each browser type in order to treat such signals as an opt-out of sale in a manner that the Attorney General would deem compliant.

W231-1 (cont.)

B. The Regulations Should Require Browser Developers to Update and Standardize Their Technology to Support Automated Treatment of Browser-Based Privacy Controls (Including But Not Limited to "Do Not Track" Signals) as an Opt Out of Sale.

The Modified Regulations have been revised to require as follows:

> Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to the [sic] opt-out of the sale of personal information. The privacy control shall require that the consumer affirmatively select their choice to opt-out and shall not be designed with any pre-selected settings.[2]

W231-2

The burden of meeting such new requirements should fall on the organizations that control the development of global privacy control technology, specifically browser developers. Alliance member are concerned that browser developers will utilize their control of such technology to either hinder or render impossible compliance by other organizations in the digital ecosystem, including news publishers.

For example, Google recently announced that it will phase out third party cookies from the Google Chrome browser over the next two years. It remains unclear how this change will impact other organizations that are required to treat as-of-yet-undefined "global privacy controls" to be developed by Google in this new ecosystem as a "do not sell" opt out. If Google phases out cookies, Google should be required to institute a new mechanism for users to easily signal their desire to opt-out of sale in an affirmative way that can be honored by publishers and other websites in an automated fashion.

In light of the foregoing, the Alliance respectfully requests that the Attorney General place the burden on browser developers to update their technology in a way that facilitates automated compliance by publishers and other websites with "global privacy settings," existing and later-developed. To the extent browser developers fail to standardize and update such technology, publishers and other websites that rely on such browsers should be deemed immune from liability based on a presumption that they are unable honor "global privacy controls" as an opt out of sale.

C. In the Event of a Conflict, A Consumer's Publisher- or Website-Specific Privacy Settings Should Prevail Over "Global Privacy Controls"

W231-3

The Modified Regulations were revised to provide as follows:

[2] 11 CCR §999.315(d)(1).

> If a global privacy control conflicts with a consumer's existing business-specific privacy setting or their participation in a business's financial incentive program, the business shall respect the global privacy control but may notify the consumer of the conflict and give the consumer the choice to confirm the business-specific privacy setting or participation in the financial incentive program.[3]

This new construct fails to honor consumer preferences for how they interact with particular businesses with whom they have first party relationships and places an undue burden on those consumers to change their business-specific privacy settings prior to and after each and every visit. In addition to this burden, prioritizing "global privacy settings" will necessarily interfere with a consumer's prior choices taken with respect to specific publishers and websites via the "Do Not Sell" links already required and placed by many publishers and websites on their pages effective January 1, 2020. Allowing global privacy controls to prevail will necessarily require every business to revisit its prior compliance steps in ways that confuse and hurt consumers. W231-3 (cont.)

The simple solution is to put the consumer's choices based on their direct relationship with specific publishers and websites first. In other words, the Regulations should flip the order of precedence and require that, in the event a consumer's existing business-specific privacy settings conflicts with a "global privacy setting," the business-specific privacy settings shall prevail and govern.

II. The Regulations Should Explicitly Provide That the 45-Day Response Time for Requests to Know and to Delete Starts to Run at the Time of Verification is Complete.

The Regulations provide:

> Businesses shall respond to requests to know and requests to delete within 45 calendar days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request.[4]

W231-4

The specific requirements governing how a business must verify requests to know and requests to delete mandate that a business invest time and resources to treat each request on a case-by-case basis. Alliance members would like the flexibility to utilize more than 45 days, if needed, to confirm the requestor's identity and honor a lawful request. Thus, the Alliance respectfully requests that the Attorney General modify the Regulations to specify that the 45-day window shall not begin until the request is verified.

III. The Attorney General Should Provide Guidance on the Purpose of the Required Metrics Reporting

The Attorney General has proposed explicit metrics reporting requirements for businesses "that alone or in combination, annually buy[], receive[], for business's commercial purposes, sell[], or share[] for commercial purposes, the personal information of 10,000,000 or more consumers."[5] W231-5

In compiling and reporting these metrics, it would be extremely helpful to businesses to understand the broader goals of such a disclosure in the privacy policy. For example, Alliance members are concerned

[3] 11 CCR §999.315(d)(2).

[4] 11 CCR §999.313(b).

[5] 11 CCR §999.317(g).

that the Modified Regulations' allowance for a business to provide a *mean* number rather than a *median* number of days taken to respond to requests will confuse consumers as to a business' record of compliance. The Alliance therefore respectfully requests that the Attorney General provide guidance on the purpose, goals, and potential use by the Attorney General of the metrics reporting requirements.

W231-5 (cont.)

IV. The Regulations Should Reinstate a Business's Right to Deny Requests for Specific Pieces of Personal Information in Order to Mitigate Security Risks

In the Modified Regulations, the Attorney General struck the right of businesses to "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."[6]

W231-6

Alliance members want to honor the privacy *and* security interests of their readers. The removal from the Regulations of a business' explicit right to deny a request for specific personal information if the disclosure creates a security risk exponentially increases the risks to security of consumer personal information without enhancing consumer privacy rights. As such, the Alliance strongly encourages the Attorney General to reinstate the removed language before issuing the finalized Regulations.

V. The Regulations Should Clarify the Placement Requirements for the Notice at Collection in Mobile Applications and Eliminate or Narrow the New Just-in-Time Notice Provision

The Modified Regulations include new language, as follows:

> When a business collects personal information through a mobile application, it may provide a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu.[7]
> …
>
> When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection. For example, if the business offers a flashlight application and the application collects geolocation information, the business shall provide a just-in-time notice, such as through a pop-up window when the consumer opens the application, which contains the information required by this subsection.[8]

It is unclear from the language in the first paragraph quoted above whether a business must provide the Notice at Collection in *both* locations - on the download page and within the application (e.g., settings menu).

W231-7

[6] 11 CCR §999.313(c)(3).

[7] 11 CCR §999.305(a)(3)(b).

[8] 11 CCR §999.305(a)(4).

An obligation to provide the Notice at Collection at both locations can be problematic to implement, especially on the download page, because businesses do not control the layout of download pages found in the app platforms (e.g., Apple's App Store and Google Play). Currently, these platforms provide app owners with limited space for privacy notices and multiple links. As such, the Alliance recommends the Attorney General clarify that the Notice at Collection can be provided in both or either locations, provided that the business makes the Notice at Collection "readily available where consumers will encounter it at or before the point of collection of any personal information."[9]

W231-7 (cont.)

The language in the second paragraph quoted above is extremely ambiguous in that it is impossible for a business to know what purposes any given consumer would "reasonably expect." The example provided makes sense and is consistent with the Federal Trade Commission's ("FTC") consent order in *In the Matter of GOLDENSHORES TECHNOLOGIES, LLC*, FILE NO. 132 3087. If this new language in the Modified Regulations is intended to address the collection of precise geolocation information in situations where the consumer would not expect such sensitive information to be collected – such as for purposes of a flashlight app – such a requirement is consistent with existing practices post-*Goldenshores.* However, the language set forth above is much more broad and appears to cover any information, not just precise geolocation or other sensitive information. The Alliance therefore respectfully requests that this language be removed or narrowed to be consistent with the FTC's prior actions and related guidance.

W231-8

VI. The Regulations Should Further Clarify the Verification Process for Authorized Agents

The Modified Regulations have been revised to provide as follows:

> When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require that the consumer do the following: (1) Provide the authorized agent written and signed permission to do so. (2) Verify their own identity directly with the business. (3) Directly confirm with the business that they provided the authorized agent permission to submit the request.[10]

W231-9

The Alliance asks the Attorney General to clarify if a business is required to ask consumers to follow all three of the verification methods described above or if it sufficient for a business to require the consumer to use any one of the methods set forth to verify authorization of an agent-made request.

VII. The Regulations Should Clarify That the CCPA's Application is Limited to Living Consumers

The CCPA defines a consumer as "a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier."[11] The definition of "resident" in Section 17014 of Title 18 of the California Code of Regulations does not specify if the resident must be living.

W231-10

[9] 11 CCR §999.305(a)(3).

[10] 11 CCR §999.326(a)(1)-(3).

[11] CIV. CODE §1798.140(g)

Alliance members anticipate that household and/or family members, or estates, will attempt to use the consumer rights afforded in the CCPA to make requests on behalf of a decedent. The European Union's General Data Protection Regulation explicitly confirms that data subject rights do not apply to the personal data of deceased persons.[12] For the sake of clarity, the Alliance recommends the Attorney General make explicit that the CCPA applies only to living natural persons.

W231-10 (cont.)

Sincerely,

David Chavern
President & CEO
News Media Alliance

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (Recital 27) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

From: Ron Ceguera
To: Privacy Regulations
Subject: CCPA Regulations Comment Letter
Date: Tuesday, February 25, 2020 4:00:01 PM
Attachments: CCPA Regs Comment Letter_02.25.20.pdf

Dear Ms. Kim,

Please see attached.

Ramon (Ron) Ceguera
Legal Assistant, Office of the General Counsel
[redacted]

BAY AREA METRO | BayAreaMetro.gov
Association of Bay Area Governments
Metropolitan Transportation Commission

Bay Area Metro Center | 375 Beale Street | Suite 800
San Francisco, CA 94105
O: [redacted] | **F:** (415) 536-9801
Main phone number: 415-778-6700

(Note: Visitors must check in with the receptionist on the 7th floor)

METROPOLITAN
TRANSPORTATION
COMMISSION

Bay Area Metro Center
375 Beale Street, Suite 800
San Francisco, CA 94105
415.778.6700
www.mtc.ca.gov

February 25, 2020

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

Re: California Consumer Privacy Act Regulations

Dear Ms. Kim,

The Metropolitan Transportation Commission (MTC) is the regional transportation planning agency for the nine-county San Francisco Bay Area and was established in state law by Government Code Section 66500, *et seq*. MTC is responsible for a number of customer-facing transportation payment programs, including Clipper® — an electronic transit fare collection system — and FasTrak® — the Bay Area's electronic toll collection system. To assist us with the administration of these programs, MTC contracts with private vendors. State law, in particular, Streets and Highways Code (SHC) Section 31490 places restrictions on the disclosure and retention of personally identifiable information (PII) obtained from customers subscribing to Clipper or FasTrak or who use toll bridges that employ electronic toll collection. SHC Section 31490 also requires establishment of privacy policies with specific disclosures to customers and prohibits transportation agencies and their contractors from selling PII.

The California Consumer Privacy Act (CCPA) does not appear to apply to government agencies because government agencies are not businesses pursuant to Civil Code Section 1798.140(c). We are concerned, however, with draft regulation Section 999.314 entitled "Service Providers."

Section 1798.140(v) of the CCPA limits "service providers" to entities that process information on behalf of *businesses*. The draft regulations, however, expand the definition of service provider. More specifically, under draft regulation Section 999.314(a), businesses that provide services to "a person or organization that is not a business . . . shall be deemed a service provider for purposes of the CCPA and these regulations." This raises the question of whether a government agency is considered "a person or organization" such that personal information a business may be holding or processing on behalf of a government agency would come within the CCPA and the regulations. Further, there is no definition for "organization" under the CCPA, although Section 1798.140(n) of the Civil Code defines a person as follows: "'Person' means an individual, proprietorship, firm, partnership, joint venture, syndicate, business, trust company corporation, limited liability company, association, committee and any other organization or group of persons acting in concert." This definition does not encompass government agencies. We are therefore requesting clarification about whether a government agency is "a person or organization" for purposes of draft regulation Section 999.314. W232-1

In addition, the requirements applicable to the "person or organization" vis a vis "services providers" is difficult to understand. For example, Section 999.314(e) states: "If a service provider receives a request to know or a request to delete from a consumer, the service provider shall either act on behalf of the business in responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider." As noted previously, a government agency is not a business. Nonetheless, in such a scenario, if the service provider chooses to inform the consumer that the request cannot be acted upon, would there be any obligation on the non-business "person or organization" to comply with the consumer's request?

W232-1
(cont.)

We appreciate the opportunity to submit comments on this regulation and respectfully request that the final regulations remove any ambiguity in this matter that could result in confusion to consumers and potential litigation at the expense of the taxpayer.

Sincerely,

Cynthia Segal
Deputy General Counsel and Privacy Officer

From: Elizabeth Bojorquez
To: Privacy Regulations
Cc: Jacqueline Kinney
Subject: CCTA Comments on CCPA Modified Regs
Date: Tuesday, February 25, 2020 3:59:32 PM
Attachments: CCTA Comments to AG on CCPA 2-25-20.pdf

Good Afternoon,

The California Cable and Telecommunications Association submits the attached comments regarding the modified regulations for the California Consumer Privacy Act.

Thank you,

Elizabeth Bojorquez
California Cable & Telecommunications Association
1001 K Street, 2nd Floor
Sacramento CA 95814
(916) 446-7732 (office)
[redacted] (direct)

Carolyn McIntyre
President

1001 K STREET, 2ND FLOOR
SACRAMENTO, CA 95814

916/446-7732
FAX 916/446-1605

February 25, 2020

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

Submitted via electronic mail to privacyregulations@doj.ca.gov

RE: California Consumer Privacy Act Proposed Regulations – Modified Text

The California Cable and Telecommunications Association ("CCTA") submits these comments pursuant to the "Updated Notice of Modifications to Text of Proposed Regulations and Addition of Documents and Information to Rulemaking File" ("Revised Regulations") issued February 10, 2020, by the Attorney General ("AG") as part of its rulemaking to implement the California Consumer Privacy Act ("CCPA").[1]

CCTA submitted comments on December 6, 2019, on the AG's originally proposed CCPA regulations and appreciates that the AG's Revised Regulations include changes to address some of the issues raised in those comments. Below are CCTA's recommendations for a few narrow and targeted additional revisions to the Revised Regulations. These modest recommendations are aimed at ensuring consistency with the CCPA, furthering the legislative purpose, and achieving greater clarity that will enhance compliance with the CCPA and meet requirements of the Administrative Procedure Act ("APA").

Each of CCTA's recommended revisions are described below with corresponding numbers and text changes designated in yellow highlight on the attached redline of the Revised Regulations.

[1] The AG's Revised Regulations and all related CCPA rulemaking information is at https://oag.ca.gov/privacy/ccpa.

1. Categories of Third Parties – Section 999.301(e)

Proposed regulation 999.301(e), which defines "categories of third parties," has been revised to be more consistent with the CCPA definition of a "third party" in Civil Code Section 1798.140(w).[2] The original proposed regulation designated specific types of entities as "categories of third parties" that do not collect personal information directly from consumers, including "internet service providers" ("ISPs"). CCTA's December comments pointed out that this created a factual inaccuracy regarding ISPs. The Revised Regulations largely address this concern by stating that categories of third parties "may include" ISPs. W233-1

CCTA recommends one additional modest tweak to Section 999.301(e) of the Revised Regulations – addition of "among others" prior to the list. This will more clearly state that the list of third parties set out in the definition is simply *illustrative* and not *exhaustive*, thereby furthering "clarity" required by the APA.

2. Notice of Right to Opt-Out of Sale – Section 999.306(b)(1)

Proposed regulation 999.306(b)(1) requires a business to post the notice of the right to opt-out on the Internet web page the consumer is directed to after clicking on the "Do Not Sell My Personal Information" or "Do Not Sell" link on the website homepage or the download or landing page of a mobile application ("app"). The Revised Regulations add language to specify the option of providing this link within a mobile app for a business that collects personal information through a mobile app. CCTA is aware that businesses are reporting having challenges with app stores in getting "Do Not Sell" links posted on the download or landing page of mobile apps and have therefore instead put this link in the app settings menu. CCTA recommends an additional minor revision to Section 999.306(b)(1) of the Revised Regulations to address this practical problem by allowing a business to locate the link at a place that is within its control and still helpful to consumers. W233-2

3. Request to Know -- Section 999.313(c)(4)

Proposed regulation Section 999.313(c)(4), which governs how a business is required to respond to consumer requests for specific pieces of personal information, identifies certain information that should never be disclosed because of its highly sensitive nature, such as a Social Security numbers and bank account numbers. The Revised Regulations add to this list "unique biometric data generated from measurements or technical analysis of human characteristics." W233-3

CCTA recognizes that this list could become easily outdated and underinclusive by not including other types of personal information that, if disclosed, would be equally problematic and create similar security risks. Even with the addition of biometric data, the list is likely to be outdated even before the AG finalizes these CCPA regulations.

[2] All further section references are to the Civil Code.

Thus, CCTA recommends adding a phrase that is a catch-all of other personal information, but with clear parameters so as to not be too broad. To be covered by the prohibition against disclosure under CCTA's recommended language, it must create a "substantial, articulable, and unreasonable risk to security of that personal information, the consumer's account with the business, or the security of the business's systems or networks." This language is based on the provision that was in the original version of the regulations in Section 313(c)(3) but that was deleted in the Revised Regulations. CCTA believes that restoring this language at the end Section 313(c)(4) is both logical and helpful to address the above concerns. W233-3 (cont.)

CCTA respectfully requests that the AG accept these recommendations for additional minor changes to the Revised Regulations in order to comply with clear direction in the APA and CCPA to adopt reasonable regulations that advance consumer privacy while minimizing implementation obstacles and burdens on business.

4. <u>Service Providers – Section 999.314(c)(3) and (d)</u>

<u>4-A</u> -- Proposed regulation 999.314(c)(3), which specifies limitations on responsibilities and functionalities that may be undertaken and performed by service providers, has been revised to be more consistent with CCPA definitions of "service provider," "sale," and "business purpose." The Revised Regulations more closely align with the CCPA plain language and intent in preserving the ability of a business to use service providers to improve their products and services for the benefit of consumers.

CCTA recommends one revision to the new language that prohibits an internal use by a service provider of personal information for "cleaning or augmenting data acquired from another source." It is unclear what this phrase means, and, especially given this ambiguity, it appears the phrase would overly restrict service providers' internal uses of data beyond what the CCPA authorizes. In this regard, the CCPA Section 1798.140(v) defines "service providers" to allow them to do the following: "retaining, using, or disclosing the personal information for … the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title." W233-4

The CCPA's definition of "sale" also is on point. Specifically, the CCPA Section 1798.140(t)(2)(C) expressly states that it is *not* a sale triggering the law's opt-out requirement if:

> "(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:
>
> (i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.
>
> (ii) ***<u>The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose</u>***." (emphasis added)

The emphasized language makes clear that a service provider *can use* internally or *even sell* a consumer's personal information that it receives from a business so long as it is "necessary to perform the business purpose" for which the business hired the service provider.

W233-4 (cont.)

Thus, to achieve clarity and consistency with the CCPA, CCTA recommends striking the phrase "or cleaning or augmenting data acquired from another source" from Section 999.314(c) of the Revised Regulations.

4-B – The Revised Regulations include a new provision in Section 999.314(d) that states as follows: "A service provider shall not sell data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business." This language conflicts with the CCPA, making the regulation inconsistent with the statute. Specifically, the CCPA Section 1798.140(t)(2)(C) expressly states that it is *not* a sale triggering the law's opt-out requirement if:

> "(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:
>
> (i) The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.
>
> (ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

W233-5

CCTA recommends some clarifying language to Section 999.314(d) of the Revised Regulations to make it consistent with the CCPA and its legislative purpose of authorizing businesses to continue use of service providers.

5. Request to Opt-In After Opting Out – Section 999.316

5-A -- Proposed regulation 999.316(a) requires that requests to opt-in to the sale of personal information shall use a two-step opt-in process. The Revised Regulations retain this mandate even though the CCPA does not require this double opt-in. In fact, the CCPA Section 1798.120(d) provides that, even where a consumer previously opted out, a business may sell the consumer's personal information as long as the consumer "subsequently provides express authorization for the sale of the consumer's personal information." Thus, only a ***single*** opt-in is required by the plain language of the CCPA, making the Revised Regulations inconsistent with the statute. Moreover, this proposed double opt-in requirement would impose unnecessary burdens on businesses and create additional, annoying speed-bumps for consumers. Accordingly, CCTA recommends changing a single word in Section 999.316(a) of the Revised Regulations to make this double-check an optional step that businesses may take.

W233-6

5-B – The Revised Regulations change Section 999.316(b) in a manner that creates inconsistency with the CCPA. Specifically, the revised provision would require a business to obtain opt-in consent from a consumer who previously opted out before selling the consumer's personal information in order to complete a transaction that the consumer initiated. However, that requirement is squarely inconsistent with the CCPA, which makes clear that neither opt-out nor opt-in consent is required for the sale of personal information in connection with a transaction requested or initiated by the consumer. This includes where "[t]he business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose," as provided in the CCPA Section 1798.140(t)(2)(C). The CCPA clearly defines "business purpose" to include "[p]erforming services on behalf of the business or service provider, including … processing or fulfilling orders and transactions, verifying customer information … or providing similar services on behalf of the business or service provider." W233-7

To prevent this inconsistency with the plain language of the CCPA, CCTA recommends restoring Section 999.316(b) of the Revised Regulations to its original text, which simply stated that the business "may" provide additional information to the consumer and explain to them how to opt-in after having previously opted out.

Respectfully submitted,

/s/Jacqueline R. Kinney

Jacqueline R. Kinney
CCTA Senior Vice President and General Counsel

CCTA RECOMMENDATIONS
FEBRUARY 25, 2020
TEXT OF MODIFIED REGULATIONS

The original proposed language is in single underline. Changes are illustrated in red by double underline for proposed additions and by ~~strikeout~~ for proposed deletions.

TITLE 11. LAW

DIVISION 1. ATTORNEY GENERAL

CHAPTER 20. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

PROPOSED TEXT OF REGULATIONS

Article 1. General Provisions

§ 999.300. Title and Scope

(a) This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as "these regulations." These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have.

(b) A violation of these regulations shall constitute a violation of the CCPA~~,~~ and be subject to the remedies provided for therein.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100-1798.199, Civil Code.

§ 999.301. Definitions

In addition to the definitions set forth in Civil Code section 1798.140, for purposes of these regulations:

(a) "Affirmative authorization" means an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a child under 13 years of age, it means that the parent or guardian has provided consent to the sale of the child's personal information in accordance with the methods set forth in section 999.330. For consumers 13 years and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

(b) "Attorney General" means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General.

(c) "Authorized agent" means a natural person or a business entity registered with the Secretary of State to conduct business in California that a consumer has authorized to act on their behalf subject to the requirements set forth in section 999.326.

(d) "Categories of sources" means types or groupings of persons or ~~of~~ entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They may include, ~~including but not limited to~~ the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers ~~from which public records are obtained, and consumer data resellers~~.

(e) "Categories of third parties" means types or groupings of third parties with whom the business shares ~~of entities that do not collect~~ personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include, among others, ~~directly from consumers, including but not limited to~~ advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and ~~consumer~~ data brokers ~~resellers~~.

W233-1 (cont.)

CCTA Recommendation #1

(f) "CCPA" means the California Consumer Privacy Act of 2018, Civil Code sections 1798.100 *et seq*.

(g) "COPPA" means the Children's Online Privacy Protection Act, 15 U.S.C. sections 6501 to 6508 and 16 Code of Federal Regulations part 312.5.

(h) "Employment benefits" means retirement, health, and other benefit programs, services, or products to which consumers or their beneficiaries receive access through the consumer's employer.

(i) "Employment-related information" means personal information that is collected by the business about a natural person for the reasons identified in Civil Code section 1798.145, subdivision (h)(1). The collection of employment-related information, including for the purpose of administering employment benefits, shall be considered a business purpose.

(j) ~~(g)~~ "Financial incentive" means a program, benefit, or other offering, including payments to consumers as compensation, for the disclosure, deletion, or sale of personal information.

(k) ~~(h)~~ "Household" means a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier ~~occupying a single dwelling~~.

(l) ~~(i)~~ "Notice at collection" means the notice given by a business to a consumer at or before the ~~time~~ point at which a business collects personal information from the consumer as required by Civil Code section 1798.100, subdivision (b), and specified in these regulations.

(m) ~~(j)~~ "Notice of right to opt-out" means the notice given by a business informing consumers of their right to opt-out of the sale of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations.

(n) ~~(k)~~ "Notice of financial incentive" means the notice given by a business explaining each financial incentive or price or service difference ~~subject to~~ as required by Civil Code section 1798.125, subdivision (b), as required by that section and specified in these regulations.

(o) ~~(l)~~ "Price or service difference" means (1) any difference in the price or rate charged for any goods or services to any consumer related to the disclosure, deletion, or sale of personal information, including through the use of discounts, financial payments, or other benefits or penalties; or (2) any difference in the level or quality of any goods or services offered to any consumer related to the disclosure, deletion, or sale of personal information, including the denial of goods or services to the consumer.

(p) ~~(m)~~ "Privacy policy" means the policy referred to in Civil Code section 1798.130, subdivision (a)(5), and means the statement that a business shall make available to consumers describing the business's practices, both online and offline, regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their own personal information.

(q) ~~(n)~~ "Request to know" means a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections 1798.100, 1798.110, or 1798.115. It includes a request for any or all of the following:

(1) Specific pieces of personal information that a business has collected about the consumer;

(2) Categories of personal information it has collected about the consumer;

(3) Categories of sources from which the personal information is collected;

(4) Categories of personal information that the business sold or disclosed for a business purpose about the consumer;

(5) Categories of third parties to whom the personal information was sold or disclosed for a business purpose; and

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

(r) ~~(o)~~ "Request to delete" means a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105.

(s) ~~(p)~~ "Request to opt-out" means a consumer request that a business not sell the consumer's personal information to third parties, pursuant to Civil Code section 1798.120, subdivision (a).

(t) ~~(q)~~ "Request to opt-in" means the affirmative authorization that the business may sell personal information about the consumer required by Civil Code section 1798.120 subdivision (c), by a parent or guardian of a consumer less than 13 years of age, by a minor at least 13 and less than 16 years of age, or by a consumer who had previously opted out of the sale of their personal information.

(u) "Signed" means that the written attestation, declaration, or permission has either been physically signed or provided electronically per the Uniform Electronic Transactions Act, Civil Code section 1633.7 *et seq*.

(v) ~~(r)~~ "Third-party identity verification service" means a security process offered by an independent third party ~~who~~ that verifies the identity of the consumer making a request to the business. Third-party verification services are subject to the requirements set forth in Article 4 regarding requests to know and requests to delete.

~~(s) "Typical consumer" means a natural person residing in the United States.~~

~~(t) "URL" stands for Uniform Resource Locator and refers to the web address of a specific website.~~

(w) "Value of the consumer's data" means the value provided to the business by the consumer's data as calculated under section 999.337.

(x) ~~(u)~~ "Verify" means to determine that the consumer making a request to know or request to delete is the consumer about whom the business has collected information, or is the parent or legal guardian of that consumer who is less than 13 years of age.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100-1798.199, Civil Code.

§ 999.302. Guidance Regarding the Interpretation of CCPA Definitions.

(a) Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "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." For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be "personal information."

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.140, Civil Code.

Article 2. Notices to Consumers

§ 999.304. Overview of Required Notices.

(a) Every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and these regulations, including section 999.308.

(b) A business that collects personal information from a consumer shall provide a notice at collection in accordance with the CCPA and these regulations, including section 999.305.

(c) A business that sells personal information shall provide a notice of right to opt-out in accordance with the CCPA and these regulations, including section 999.306.

(d) A business that offers a financial incentive or price or service difference shall provide a notice of financial incentive in accordance with the CCPA and these regulations, including section 999.307.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.115, 1798.120, 1798.125, 1798.130, and 1798.135, Civil Code.

§ 999.305. Notice at Collection of Personal Information

(a) Purpose and General Principles

(1) The purpose of the notice at collection is to ~~inform~~ provide consumers with timely notice, at or before the ~~time~~ point of collection ~~of a consumer's personal information of~~, about the categories of personal information to be collected from them and the purposes for which the ~~categories of~~ personal information will be used.

(2) 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~~ consumers. 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 in California.

~~d.~~ Be reasonably accessible to consumers with disabilities. ~~At a minimum,~~ For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

(3) ~~e. Be visible or accessible~~ The notice at collection shall be made readily available where consumers will ~~see~~ encounter it at or before the point of collection of any personal information ~~is collected~~. Illustrative examples follow:

~~a. For example, when~~ When a business collects consumers' personal information online, it may ~~conspicuously~~ post a conspicuous link to the notice on the introductory page of the business's website ~~homepage or the mobile application's download page, or~~ and on all webpages where personal information is collected.

~~b.~~ When a business collects personal information through a mobile application, it may provide a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu.

~~c.~~ 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

W233-8
Typo

signage directing consumers to ~~the web address~~ where the notice can be found online.

~~d.~~ When a business collects personal information over the telephone or in person, it may provide the notice orally.

(4) When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection. For example, if the business offers a flashlight application and the application collects geolocation information, the business shall provide a just-in-time notice, such as through a pop-up window when the consumer opens the application, which contains the information required by this subsection.

(5) ~~(3)~~ A business shall not use a consumer's personal information for a~~n~~y purpose ~~other~~ materially different than those disclosed in the notice at collection. If the business ~~intends~~ seeks to use a consumer's previously collected personal information for a purpose ~~that~~ materially different than what 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.

(6) ~~(4)~~ A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection.

(7) ~~(5)~~ If a business does not give the notice at collection to the consumer at or before the point of collection of their personal information, the business shall not collect personal information from the consumer.

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

(1) A list of the categories of personal information about consumers to be collected. Each category of personal information shall be written in a manner that provides consumers a meaningful understanding of the information being collected.

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

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

(4) A link to the business's privacy policy, or in the case of offline notices, ~~the web address of the~~ where the business's privacy policy can be found online.

(c) If a business collects personal information from a consumer online, the notice at collection may be given to the consumer by providing a link to the section of the business's privacy policy that contains the information required in subsection (b).

(d) If a ~~A~~ business that does not collect information directly from consumers is registered with the Attorney General as a data broker pursuant to Civil Code section 1798.99.80, *et seq.* it does not need to provide a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out. ~~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. Confirm that the source provided a notice at collection to the consumer in accordance with subsections (a) and (b); and~~

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

(e) A business collecting employment-related information shall comply with the provisions of section 999.305 except with regard to the following:

(1) The notice at collection of employment-related information does not need to include the link or web address to the link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info".

(2) The notice at collection of employment-related information may include a link to, or paper copy of, a business's privacy policies for job applicants, employees, or contractors in lieu of a link or web address to the business's privacy policy for consumers.

(f) Subsection (e) shall become inoperative on January 1, 2021, unless the CCPA is amended otherwise.

Note: Authority: Section 1798.185, Civil Code. Reference: Sections 1798.99.82, 1798.100, 1798.115, and 1798.185, Civil Code.

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

(a) Purpose and General Principles

(1) The purpose of the notice of right to opt-out ~~of sale of personal information~~ is to inform consumers of their right to direct a business that sells ~~(or may in the future sell)~~ their personal information to stop selling their personal information~~, and to refrain from doing so in the future~~.

(2) The notice of right to opt-out shall be designed and presented ~~to the consumer~~ in a way that is easy to read and understandable to ~~an average~~ consumers. 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 in California.

d. Be reasonably accessible to consumers with disabilities. ~~At a minimum,~~ For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

(b) A business that sells the personal information of ~~a~~ consumers shall provide ~~a~~ the notice of right to opt-out to ~~the~~ consumers as follows:

(1) A business shall post the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link on the website homepage or the download or landing page of a mobile application. ~~In addition, a~~ A business that collects personal information through a mobile application may instead provide a link to the notice within the application, such as through the application's settings menu. The notice shall include the information specified in subsection (c) or link to the section of the business's privacy policy that contains the same information.

W233-2 (cont.)

CCTA Recommendation #2

(2) A business that substantially interacts with consumers offline shall also provide notice to the consumer by an offline method that facilitates consumer awareness of their right to opt-out. Such methods include, but are not limited to, printing the notice on paper forms that collect personal information, providing the consumer with a paper version of the notice, and posting signage directing consumers to ~~a website~~ where the notice can be found online.

(3) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to direct ~~a~~ the business that sells their personal information to stop selling their personal information. That method shall comply with the requirements set forth in subsection (a)(2).

(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~~ interactive form 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; and

(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.~~

(d) A business ~~is exempt from providing~~ does not need to provide 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.~~

(e) A business shall not sell the personal information it collected during the time the business did not have a notice of right to opt-out notice posted unless it obtains the affirmative authorization of the consumer.

(f) ~~(e)~~ Opt-Out Button ~~or Logo~~

(1) The following opt-out button ~~or logo~~ may be used in addition to posting the notice of right to opt-out, but not in lieu of any posting of the notice of right to opt-out.

(2) When the opt-out button is used, it shall appear to the left of the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link, as demonstrated below, and shall be approximately the same size as other buttons on the business's webpage. ~~[BUTTON OR LOGO TO BE ADDED IN A MODIFIED VERSION OF THE REGULATIONS AND MADE AVAILABLE FOR PUBLIC COMMENT.]~~

(3) This opt-out button ~~or logo~~ shall link to a webpage or online location containing the information specified in section 999.306(c), or to the section of the business's privacy policy that contains the same information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

§ 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~~ the material terms of a financial incentive or price or service difference the ~~a~~ business ~~may offer in exchange for the retention or sale of a consumer's personal information~~ is

offering so that the consumer may make an informed decision on whether to participate. A business that does not offer a financial incentive or price or service difference related to the disclosure, deletion, or sale of personal information is not required to provide a notice of financial incentive.

(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~~ consumers. 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 in California.

d. Be reasonably accessible to consumers with disabilities. ~~At a minimum,~~ For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

e. Be readily available ~~online or other physical location~~ where consumers will ~~see~~ encounter it before opting into the financial incentive or price or service difference.

(3) If the business offers the financial incentive or price ~~of~~ or 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 and the value of the consumer's data;

(3) How the consumer can opt-in to the financial incentive or price or service difference;

(4) ~~Notification~~ A statement 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~~ how the financial incentive or price or service difference is ~~permitted under the CCPA~~ reasonably related to the value of the consumer's data, 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.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.130, Civil Code.

§ 999.308. Privacy Policy

(a) Purpose and General Principles

(1) The purpose of the privacy policy is to provide ~~the~~ consumers with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information. ~~The privacy policy shall not contain specific pieces of personal information about individual consumers and need not be personalized for each consumer.~~

(2) The privacy policy shall be designed and presented in a way that is easy to read and understandable to ~~an average~~ consumers. The notice shall:

a. Use plain, straightforward language and avoid technical or legal jargon.

b. Use a format that makes the policy readable, including on smaller screens, if applicable.

c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.

d. Be reasonably accessible to consumers with disabilities. ~~At a minimum,~~ For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

e. Be available in ~~an additional~~ a format that allows a consumer to print it out as a ~~separate~~ document.

(3)

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

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

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

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

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

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

d. Identify ~~Collection of Personal Information 1. List~~ the categories of ~~consumers'~~ personal information the business has collected about consumers in the preceding 12 months. The ~~notice~~ categories shall be described ~~written~~ in a manner that provides consumers a meaningful understanding of the information being collected.

~~1. For each category of personal information collected, provide the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties with whom the business shares personal information. The notice shall be written in a manner that provides consumers a meaningful understanding of the categories listed.~~

e. Disclosure or Sale of Personal Information

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

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

2. For each category of personal information identified, provide the categories of third parties to whom the information was disclosed or sold.

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

(2) Right to Request Deletion of Personal Information

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

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

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

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

a. Explain that the consumer has a right to opt-out of the sale of their personal information by a business.

b. State whether or not the business sells personal information. If the business sells personal information, i~~I~~nclude either the contents of the notice of right to opt-out or a link to it in accordance with section 999.306.

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

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

(5) Authorized Agent

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

(6) Contact for More Information~~:~~

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

(7) Date the privacy policy was last updated.

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

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.115, 1798.120, 1798.125 and 1798.130, Civil Code.

Article 3. Business Practices for Handling Consumer Requests

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

(a) A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to know. All other businesses shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free

telephone number~~, and if the business operates a website, an interactive webform accessible through the business's website or mobile application~~. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.

(b) A business shall provide two or more designated methods for submitting requests to delete. Acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a link or form available online through a business's website, a designated email address, a form submitted in person, and a form submitted through the mail.

(c) A business shall consider the methods by which it primarily interacts with consumers when determining which methods to provide for submitting requests to know and requests to delete. If the business interacts with consumers in person, the business shall consider providing an in-person method such as a printed form the consumer can directly submit or send by mail, a tablet or computer portal that allows the consumer to complete and submit an online form, or a telephone by which the consumer can call the business's toll-free number. ~~At least one method offered shall reflect the manner in which the business primarily interacts with the consumer, even if it requires a business to offer three methods for submitting requests to know. Illustrative examples follow:~~

~~(1) *Example 1:* If the business is an online retailer, at least one method by which the consumer may submit requests should be through the business's retail website.~~

~~(2) *Example 2:* If the business operates a website but primarily interacts with customers in person at a retail location, the business shall offer three methods to submit requests to know—a toll-free telephone number, an interactive webform accessible through the business's website, and a form that can be submitted in person at the retail location.~~

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

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

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

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

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

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140, and 1798.185, Civil Code.

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

(a) Upon receiving a request to know or a request to delete, a business shall confirm receipt of the request within 10 business days and provide information about how the business will process the request. The information provided shall describe in general the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request. The confirmation may be given in the same manner in which the request was received. For example, if the request is made over the phone, the confirmation may be given on the phone during the phone call.

(b) Businesses shall respond to requests to know and requests to delete within 45 calendar days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request. If the business cannot verify the consumer within the 45-day time period, the business may deny the request. If necessary, businesses may take up to an additional 45 calendar days to respond to the consumer's request, for a maximum total of 90 calendar days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

(c) Responding to Requests to Know

(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~~ requestor 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).

(2) For requests that seek the disclosure of categories of personal 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 may deny the request to disclose the categories and other information requested and shall inform the requestor 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.

(3) ~~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.~~ In responding to a request to know, a business is not required to search for personal information if all the following conditions are met:

a. The business does not maintain the personal information in a searchable or reasonably accessible format;

b. The business maintains the personal information solely for legal or compliance purposes;

c. The business does not sell the personal information and does not use it for any commercial purpose; and

d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.

(4) A business shall not ~~at any time~~ disclose in response to a request to know 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, ~~or~~ unique biometric data generated from measurements or technical analysis of human characteristics, or any other information that creates a substantial, articulable, and unreasonable risk to security of that personal information, the consumer's account with the business, or the security of the business's systems or networks."

CCTA Recommendation #3

W233-3 (cont.)

(5) If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial, unless prohibited from ~~doing~~ doing so by law. If the request is denied only in part, the business shall disclose the other information sought by the consumer.

W233-9

Typo

(6) A business shall use reasonable security measures when transmitting personal information to the consumer.

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

(8) Unless otherwise specified, the 12-month period covered by a consumer's verifiable request to know referenced in Civil Code section 1798.130, subdivision (a)(2), shall run from the date the business receives the request, regardless of the time required to verify the request.

(9) In responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response to the consumer as required by the CCPA. It shall

not refer the consumer to the businesses' general practices outlined in its privacy policy unless its response would be the same for all consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories.

(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 personal information the business has collected about the consumer in the preceding 12 months;

b. ~~a.~~ The categories of sources from which the personal information was collected;

c. ~~b.~~ The business or commercial purpose for which it collected or sold the personal information;

d. ~~c.~~ The categories of third parties with which the business shares personal information; ~~to whom the business sold or disclosed the category of personal information for a business purpose; and~~

e. ~~d. The business or commercial purpose for which it sold or disclosed the category of personal information~~The categories of personal information that the business sold in the preceding 12 months, and for each category identified, the categories of third parties to which it sold that particular category of personal information;

f. The categories of personal information that the business disclosed for a business purpose in the preceding 12 months, and for each category identified, the categories of third parties to whom it disclosed that particular category of personal information.

(11) A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner that provides consumers a meaningful understanding of the categories listed.

(d) Responding to Requests to Delete

(1) For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified ~~and shall instead treat the request as a request to opt-out of sale~~. If the business sells personal information and the consumer has not already made a request to opt out, the business shall ask the consumer if they would like to opt out of the sale of their personal information and shall include either the contents of, or a link to, the notice of right to opt-out in accordance with section 999.306.

(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~~ Deidentifying the personal information; or

c. Aggregating the ~~personal~~ consumer information.

(3) If a business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or next accessed or used for a sale, disclosure, or commercial purpose.

(4) ~~In its response to a consumer's request to delete, the business shall specify the manner in which it has deleted the personal information.~~

(4) In responding to a request to delete, a business shall inform the consumer whether or not it has complied with the consumer's request.

(5) If the business complies with the consumer's request, the business shall inform the consumer ~~disclose~~ that it will maintain a record of the request ~~pursuant to~~ as allowed by Civil Code section 1798.105, subdivision (d). A business may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from the business's records.

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

a. Inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including any conflict with federal or state law, or exception to the CCPA, unless prohibited from doing so by law ~~statutory and regulatory exception therefor~~;

b. Delete the consumer's personal information that is not subject to the exception; and

c. Not use the consumer's personal information retained for any other purpose than provided for by that exception.

(7) In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information only if a global option to delete all personal information is also offered, and more prominently presented than

the other choices. ~~The business shall still use a two-step confirmation process where the consumer confirms their selection as required by section 999.312(d).~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

§ 999.314. Service Providers

(a) ~~To the extent that a person or entity~~ A business that provides services to a person or organization that is not a business, and that would otherwise meet the requirements and obligations of a "service provider" under ~~Civil Code section 1798.140(v)~~ the CCPA and these regulations, ~~that person or entity~~ shall be deemed a service provider for purposes of the CCPA and these regulations.

(b) To the extent that a business directs a ~~person or entity~~ second business to collect personal information directly from a consumer on the first business's behalf, and the second business would otherwise meet ~~all other~~ the requirements and obligations of a "service provider" under the CCPA and these regulations ~~Civil Code section 1798.140(v), that person or entity~~ the second business shall be deemed a service provider of the first business for purposes of the CCPA and these regulations.

(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.~~ A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except:

(1) To perform the services specified in the written contract with the business that provided the personal information;

(2) To retain and employ another service provider as a subcontractor, where the subcontractor meets the requirements for a service provider under the CCPA and these regulations;

(3) For internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles, ~~or cleaning or augmenting data acquired from another source~~;

(4) To detect data security incidents, or protect against fraudulent or illegal activity; or

(5) For the purposes enumerated in Civil Code section 1798.145, subsections (a)(1) through (a)(4).

(d) A service provider shall not sell ~~data~~ personal information of a consumer on behalf of a business when such ~~a~~ consumer has opted-out of the sale of their personal information with the business, except as necessary to perform the business purposes for which the business contracted with such service provider. ~~If a service provider receives a request to know or a~~

W234-4 (cont.) — **CCTA Recommendation #4-A**

W233-5 (cont.) — **CCTA Recommendation #4-B**

~~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.~~

~~(d)~~(e) If a service provider receives a request to know or a request to delete from a consumer, the service provider shall either act on behalf of the business in responding to the request or, inform the consumer that the request cannot be acted upon because the request has been sent to a service provider.

~~(e)~~(f) ~~(e)~~ 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.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140, and 1798.185, Civil Code.

§ 999.315. Requests to Opt-Out

(a) A business shall provide two or more designated methods for submitting requests to opt-out, including~~, at a minimum,~~ an interactive ~~web~~form 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 global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information.

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

(c) A business's methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out. A business shall not utilize a method that is designed with the purpose or substantial effect of subverting or impairing a consumer's decision to opt-out.

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

(1) Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to ~~the~~ opt-out of the sale of personal

W233-10

Typo

information. The privacy control shall require that the consumer affirmatively select their choice to opt-out and shall not be designed with any pre-selected settings.

(2) If a global privacy control conflicts with a consumer's existing business-specific privacy setting or their participation in a business's financial incentive program, the business shall respect the global privacy control but may notify the consumer of the conflict and give the consumer the choice to confirm the business-specific privacy setting or participation in the financial incentive program.

(e) ~~(d)~~ In responding to a request to opt-out, a business may present the consumer with the choice to opt-out of sale~~s of~~ for certain ~~categories~~ uses of personal information as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices.

(f) ~~Upon receiving~~ A business shall comply with a request to opt-out~~, a business shall act upon the request~~ as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. ~~(g) A~~ If a business ~~shall notify all third parties to whom it has sold the~~ sells a consumer's personal information ~~of~~ to any third parties after the consumer~~within 90 days prior to the business's receipt of the consumer's~~ submits their request but before the business complies with that request, it shall notify those third parties ~~request~~ that the consumer has exercised their right to opt-out and ~~instruct them~~ shall direct those third parties not to ~~further~~ sell ~~the~~ that consumer's information. ~~The business shall notify the consumer when this has been completed.~~

(g) A consumer may use an authorized agent to submit a request to opt-out on the consumer's behalf if the consumer provides the authorized agent written permission ~~to do so~~ signed by the consumer. A business may deny a request from an authorized agent that does not submit proof that they have been authorized by the consumer to act on the consumer's behalf. User-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.

(h) A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request. The business shall inform the requestor ~~requesting party~~ that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent.

Note: Authority cited: Sections 1798.135 and 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140, and 1798.185, Civil Code.

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

W233-6 (cont.)

CCTA Recommendation #5-A

(a) Requests to opt-in to the sale of personal information ~~shall~~ may use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

W233-7 (cont.)

~~A business may inform If a consumer who has opted-out when of the sale of their personal information initiates a transaction or attempts to use a product or service that~~

~~requires the sale of their personal information as a condition of completing, a business may inform the consumer that the transaction, along with product, or service requires the sale of their personal information and provide instructions on how the consumer can opt in opt in.~~

(b) A business may inform a consumer who has opted out when a transaction requires the sale of their personal information as a condition of completing the transaction, along with instructions on how the consumer can opt-in.

W233-7 (cont.)

CCTA Recommendation #5-B

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, and 1798.185, Civil Code.

§ 999.317. Training; Record-Keeping

(a) All individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA shall be informed of all the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.

(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. The business shall implement and maintain reasonable security procedures and practices in maintaining these records.

(c) The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.

(d) A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.

(e) Information maintained for record-keeping purposes shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and these regulations. Information maintained for record-keeping purposes shall not be shared with any third party.

(f) Other than as required by subsection (b) ~~Aside from this record-keeping purpose~~, a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.

(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 in a calendar year, 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 mean number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.

(2) Disclose, by July 1 of every calendar year, 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) In its disclosure pursuant to subsection (g)(1), a business may choose to identify the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.

(4) A business may choose to compile and disclose the information required by subsection (g)(1) for requests received from all individuals, rather than requests received from consumers. The business shall state whether it has done so in its disclosure and shall, upon request, compile and provide to the Attorney General the information required by subsection (g)(1) for requests received from consumers.

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

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.135, and 1798.185, Civil Code.

§ 999.318. Requests to Access or Delete Household Information

(a) Where a ~~consumer~~ household does not have a password-protected account with a business, a business ~~may respond to~~ shall not comply with a request to know ~~or request to delete as it pertains to household~~ specific pieces of personal information ~~by providing aggregate~~ about the household or a request to ~~deleted~~ delete household personal information~~, subject to verification requirements set forth in Article 4. (b) If~~ unless all of the following conditions are satisfied:

W233-11
Typo

(1) All consumers of the household jointly request access to specific pieces of information for the household or the deletion of household personal information~~, and the business~~

~~can individually verify all the members of the household subject to verification requirements set forth in Article 4, then the business shall comply with the request.;~~

(2) The business individually verifies all the members of the household subject to the verification requirements set forth in section 999.325; and

(3) The business verifies that each member making the request is currently a member of the household.

(b) Where a consumer has a password-protected account with a business that collects personal information about a household, the business may process requests to know and requests to delete relating to household information through the business's existing business practices and in compliance with these regulations.

(c) If a member of a household is a minor under the age of 13, a business must obtain verifiable parental consent before complying with a request to access specific pieces of information for the household or the deletion of household personal information pursuant to the parental consent provisions in section 999.330.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.140, and 1798.185, Civil Code.

Article 4. Verification of Requests

§ 999.323. General Rules Regarding Verification

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

(b) In determining the method by which the business will verify the consumer's identity, the business shall:

(1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section.

(2) Avoid collecting the types of personal information identified in Civil Code section 1798.81.5, subdivision (d), unless necessary for the purpose of verifying the consumer.

(3) Consider the following factors:

a. The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive or valuable personal information shall warrant a more stringent verification process. The types of personal information identified in Civil Code section 1798.81.5, subdivision (d) shall be considered presumptively sensitive;

b. The risk of harm to the consumer posed by any unauthorized access or deletion. A greater risk of harm to the consumer by unauthorized access or deletion shall warrant a more stringent verification process;

c. The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be;

d. 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;

e. The manner in which the business interacts with the consumer; and

f. Available technology for verification.

(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.

(d) A business shall not require the consumer to pay a fee for the verification of their request to know or request to delete. For example, a business may not require a consumer to provide a notarized affidavit to verify their identity unless the business compensates the consumer for the cost of notarization.

(e) ~~(d)~~ 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.

(f) ~~(e)~~ If a business maintains consumer information that is ~~de-identified~~ deidentified, 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.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140, and 1798.185, Civil Code.

§ 999.324 Verification for Password-Protected Accounts

(a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section

999.323. The business shall also require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data.

(b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to know or request to delete until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 999.325 to further verify the identity of the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

§ 999.325. Verification for Non-Accountholders

(a) If a consumer does not have or cannot access a password-protected account with ~~the~~ a business, the business shall comply with ~~subsections (b) through (g) of~~ this section, in addition to section 999.323.

(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~~ If a business uses this method for verification, the business shall maintain all signed declarations as part of ~~their~~ its record-keeping obligations.

(d) A business's compliance with a request to delete may require that the business verify the identity of the consumer to a reasonable degree or a reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion. For example, the deletion of family photographs and documents may require a reasonably high degree of certainty, while the deletion of browsing history may require only a reasonable degree of certainty. A business shall act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with these regulations ~~set forth in Article 4~~.

(e) Illustrative ~~scenarios~~ examples follow:

(1) *Example 1:* If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if ~~the business~~ a retailer maintains ~~the consumer's name and credit card number~~ a record of purchases made by a consumer, the business may require the consumer to ~~provide the credit card's security code and identifying a~~ identify items that they recently purchased from the store or the dollar amount of their most recent purchase ~~made with the credit card~~ to verify their identity to a reasonable degree of certainty.

(2) *Example 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. For example, a business may have a mobile application that collects personal information about the consumer but does not require an account. The business may determine whether, based on the facts and considering the factors set forth in section 999.323, subdivision (b)(3), it may reasonably verify a consumer by asking them to provide information that only the person who used the mobile application may know or by requiring the consumer to respond to a notification sent to their device. ~~This may require the business to conduct a fact-based verification process that considers the factors set forth in section 999.323(b)(3).~~

(f) A business shall deny a request to know specific pieces of personal information if it cannot verify the identity of the requestor pursuant to these regulations.

(g) ~~(f)~~ If there is no reasonable method by which a business can verify the identity of the consumer to the degree of certainty required by this section, the business shall state so in response to any request and~~, if this is the case for all consumers whose personal information the business holds, in the business's privacy policy. The business shall also~~ explain why it has no reasonable method by which it can verify the identity of the requestor. If the business has no reasonable method by which it can verify any consumer, the business shall explain why it has no reasonable verification method in its privacy policy. The business shall evaluate and document on a yearly basis whether ~~such~~ a reasonable method can be established ~~and shall document its evaluation.~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

§ 999.326. Authorized Agent

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

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

(2) Verify their own identity directly with the business.

(3) Directly confirm with the business that they provided the authorized agent permission to submit the request.

(b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4000 to 4465.

(c) A business may deny a request from an authorized agent that does not submit proof that they have been authorized by the consumer to act on their behalf.

(d) An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information.

(e) An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purpose other than to fulfill the consumer's requests, for verification, or for fraud prevention.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

Article 5. Special Rules Regarding Minors

§ 999 330 Minors Under 13 Years of Age

(a) Process for Opting-In to Sale of Personal Information

(1) A business that has actual knowledge that it ~~collects or maintains~~ sells the personal information of children under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. This affirmative authorization is in addition to any verifiable parental consent required under ~~the Children's Online Privacy Protection Act, 15 U.S.C. sections 6501, *et seq*~~ COPPA.

(2) Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to:

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

b. Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

c. Having a parent or guardian call a toll-free telephone number staffed by trained personnel;

d. Having a parent or guardian connect to trained personnel via video-conference;

e. Having a parent or guardian communicate in person with trained personnel; and

f. Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information, where the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.

(b) When a business receives an affirmative authorization pursuant to subsection (a) ~~of this section~~, the business shall inform the parent or guardian of the right to opt-out at a later date and of the process for doing so on behalf of their child pursuant to section 999.315, subdivision (a) through (f).

(c) A business shall establish, document, and comply with a reasonable method, in accordance with the methods set forth in subsection (a)(2), for determining whether a person submitting a request to know or a request to delete the personal information of a child under the age of 13 is the parent or guardian of that child.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, and 1798.185(a)(6), Civil Code.

§ 999.331. Minors 13 to 16 Years of Age

(a) A business that has actual knowledge that it ~~collects or maintains~~ sells the personal information of minors at least 13 and less than 16 years of age shall establish, document, and comply with a reasonable process for allowing such minors to opt-in to the sale of their personal information, pursuant to section 999.316.

(b) When a business receives a request to opt-in to the sale of personal information from a minor at least 13 and less than 16 years of age, the business shall inform the minor of the right to opt-out at a later date and of the process for doing so pursuant to section 999.315.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, and 1798.185, Civil Code.

§ 999.332. Notices to Minors Under 16 Years of Age

(a) A business subject to sections 999.330 and 999.331 shall include a description of the processes set forth in those sections in its privacy policy.

(b) A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell the personal information of such minors without their

affirmative authorization, or the affirmative authorization of their parent or guardian for minors under 13 years of age, is not required to provide the notice of right to opt-out.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, and 1798.185, Civil Code.

Article 6. Non-Discrimination

§ 999.336. Discriminatory Practices

(a) A financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations.

(b) ~~Notwithstanding subsection (a) of this section, a~~ A business may offer a financial incentive or price or service difference if it is reasonably related to the value of the consumer's data ~~as that term is defined in section 999.337~~. If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference.

(c) A business's denial of a consumer's request to know, request to delete, or request to opt-out for reasons permitted by the CCPA or these regulations shall not be considered discriminatory.

(d) ~~(c)~~ Illustrative examples follow:

(1) *Example 1*: A music streaming business offers a free service as well as ~~and~~ a premium service that costs $5-per-month. If only the consumers who pay for the music streaming service are allowed to ~~opt-out~~ opt out of the sale of their personal information, then the practice is discriminatory, unless the $5 per month payment is reasonably related to the value of the consumer's data to the business.

(2) *Example 2*: ~~A retail store offers discounted prices to consumers who sign up to be on their mailing list. If the consumer on the mailing list can continue to receive discounted prices even after they have made a request to know, request to delete, and/or request to opt-out, the differing price level is not discriminatory.~~ A clothing business offers a loyalty program whereby customers receive a $5-off coupon to their email address after spending $100 with the business. A consumer submits a request to delete all personal information the business has collected about them but also informs the business that they want to continue to participate in the loyalty program. The business may deny their request to delete as to their email address and the amount the consumer has spent with the business because that information is necessary for the business to provide the loyalty program requested by the consumer and is reasonably anticipated within the context of the business's ongoing relationship with them pursuant to Civil Code section 1798.105, subdivision (d)(1).

(3) *Example 3:* A grocery store offers a loyalty program whereby consumers receive coupons and special discounts when they provide their phone numbers. A consumer submits a request to opt-out of the sale of their personal information. The retailer complies with their request but no longer allows the consumer to participate in the loyalty program. This practice is discriminatory unless the grocery store can demonstrate that the value of the coupons and special discounts are reasonably related to the value of the consumer's data to the business.

(4) *Example 4:* An online bookseller collects information about consumers, including their email addresses. It offers discounts to consumers through browser pop-up windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information that the bookseller has collected about them, including their email address and their browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide coupons is discriminatory unless the value of the coupons are reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete as to the email address because the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

~~(d) A business's denial of a consumer's request to know, request to delete, or request to opt-out for reasons permitted by the CCPA or these regulations shall not be considered discriminatory.~~

~~(e)~~ A business shall notify consumers of any financial incentive or price or service difference subject to Civil Code section 1798.125 that it offers in accordance with section 999.307.

~~(f)~~ A business's charging of a reasonable fee pursuant to Civil Code section 1798.145, subdivision (~~g~~i)(3) shall not be considered a financial incentive subject to these regulations.

~~(g)~~ A price or service difference that is the direct result of compliance with federal law shall not be considered discriminatory.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130, and 1798.185, Civil Code.

§ 999.337. Calculating the Value of Consumer Data

~~(a) The value provided to the consumer by the consumer's data, as that term is used in Civil Code section 1798.125, is the value provided to the business by the consumer's data and shall be referred to as "the value of the consumer's data."~~

(a) ~~(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~~ consider 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;~~

(3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers;

(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 reasonably reliable method of calculation used in good-faith.

(b) For the purpose of calculating the value of consumer data, a business may consider the value of the data of all natural persons to the business and not just consumers.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130, and 1798.185, Civil Code.

Article 7. Severability

§ 999.341.

(a) If any article, section, subsection, sentence, clause or phrase of these regulations contained in this Chapter is for any reason held to be unconstitutional, contrary to statute, exceeding the authority of the Attorney General, or otherwise inoperative, such decision shall not affect the validity of the remaining portion of these regulations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.145, 1798.185, and 1798.196, Civil Code.

From:	Pierre Valade
To:	Privacy Regulations
Cc:	Zoe Vilain
Subject:	2121 Atelier Inc, Comment for General Attorney
Date:	Tuesday, February 25, 2020 3:58:19 PM
Attachments:	Jumbo Privacy comments - CCPA proposed regulation .eml

Greetings Deputy Attorney General Kim,

Please find the following attachment commenting on the modification of the California AG in regards to the CCPA.

Please feel free to reach out to me or Zoe Vilain, our Chief Privacy Officer if you have any question regarding this document.

Thank you

From:	Zoe Vilain
To:	Privacy Regulations
Cc:	Pierre Valade
Subject:	Jumbo Privacy comments - CCPA proposed regulation
Date:	Tuesday, February 25, 2020 3:58:43 PM
Attachments:	comment for ga.pdf

Greetings Deputy Attorney General Kim,

Please find the following attachment commenting on the modification of the California AG in regards to the CCPA.

Please feel free to reach out to me or Pierre Valade, our CEO if you have any question regarding this document.

Thank you,
Sincerely,
Zoe Vilain
—
Jumbo Privacy
Chief Privacy Advisor

Jumbo

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

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

February 25th, 2020

By email (privacyregulations@doj.ca.gov)

Subject: Written comments regarding the proposed CCPA regulations

Dear Deputy Attorney General Kim,

We revert to you concerning the proposed modifications to the rulemakings of the California Attorney General with regards to the California Consumer privacy Act ("CCPA") made on February 7th and 14th, 2020, to suggest some comments.

2121 Atelier Inc. dba Jumbo Privacy has been acting as registered authorized agent in California for California residents, thanks to the introduction of such role in the CCPA since Feb 1st, 2020. Jumbo Privacy notably represents California consumers to request opt-out of sale of their personal information from businesses falling under the scope of the CCPA, as selected by such consumers.

Requests sent by Jumbo Privacy all contain identification of the consumer and a signed mandate executed through and stored by a third-party certifier, authorizing Jumbo to act on behalf of the consumer.

As of date, 85% of refusal replies received by Jumbo Privacy from these businesses, are based on the argument that such businesses refuse to comply with third-party requests to opt-out of sale and require the consumer to take further action directly. Jumbo Privacy has therefore been pushing back against such refusals by quoting sections 1798-135. of the CCPA and § 999.315.e. of the California Attorney General text of Regulations and indicating that such refusals are a restriction of consumer's rights.

As mentioned in our first letter dated December 6th, 2019, we believe that privacy rights are fundamental rights, therefore that the exercise of such rights should be easy and accessible to all individuals in particular to consumers. We believe that mandating an authorized agent to exercise one's data privacy rights is the most efficient way to ensure this.

We are concerned that proposed modifications to the rulemakings of the California Attorney General with regards to the CCPA might highly restrict the efficiency and opportunity for consumers to mandate an Authorized Agent. Therefore, we are addressing our suggestions and comments to the proposed rulemakings of the California Attorney General notably regarding provisions related to such "authorized agent".

We would like to take advantage of this letter to inform you that as authorized agent, we believe that every business falling under the scope of the CCPA should implement a dedicated communication channel with Authorized Agents, preferably an email address for purpose of simplicity, to facilitate the management of requests made on behalf of consumers they represent. Indeed, if businesses force Authorized Agents to use web forms or postal mail, then Authorized Agents will not be able to manage privacy requests on behalf of their mandators efficiently. W234-1

We remain of course at your disposal for any query,

Sincerely,

Pierre Valade,
Jumbo Privacy
www.jumboprivacy.com

Appendix
Jumbo Privacy Proposed Amendments

1. § 999.326. Authorized Agent

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

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

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

(3) Directly confirm with the business that they provided the authorized agent permission to submit the request in case the authorized agent has not provided proof of the existence of the signed mandate.

(b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4000 to 4465.

W234-2

(c) A business may deny a request from an authorized agent that does not submit proof that they have been authorized by the consumer to act on their behalf.

(d) An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information.

(e) An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purpose other than to fulfill the consumer's requests, for verification, or for fraud prevention."

Jumbo Privacy Comment: Consumers that mandate Jumbo Privacy as authorized agent to submit requests to know, or to delete, are doing so, to avoid having to manage such requests themselves, notably to avoid receiving numerous emails from businesses to confirm the validity of their requests or their identity.

We believe that allowing a business to contact the consumer directly for additional identity verification after receipt of a request by mandate through an Authorized Agent, would lead to additional heavy processes and unnecessary delays to the processing of the original request.

Security of personal information and verification of identity are a priority for Jumbo Privacy when acting as authorized agent. We understand perfectly the importance of ensuring the validity of received requests to know or requests to delete. However, we would like to emphasize the fact that providing a general possibility for a business to proceed to a verification of identity or request made through an agent, might highly impair consumer rights by restraining the practicality to mandate an authorized agent.

Therefore, we would suggest these additions to ensure that businesses need to, or can, verify the consumer's identity only if the business can prove the Authorized Agent has not provided reasonable proof of such consumer's identity or the existence of a valid mandate. We believe from requests we have made so far on behalf of consumers, that businesses may be tempted to use such article to bypass an authorized agent's authority to act on behalf of said consumers. This addition would prevent any unnecessary verification by the business, and disproportionate verification measures, ensuring respect of the consumer's privacy rights.

W234-2 (cont.)

2. **§ 999.325. Verification for Non-Accountholders**

> *« Example 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. For example, a business may have a mobile application that collects personal information about the consumer but does not require an account. The business may determine whether, based on the facts and considering the factors set forth in section 999.323, subdivision (b)(3), it may reasonably verify a consumer by asking them to provide information that only the person who used the mobile application may know or by requiring the consumer to respond to a notification sent to their device. This may require the business to conduct a fact-based verification process that considers the factors set forth in section 999.323(b)(3). »*

W234-3

Jumbo Privacy Comment: In the event where such example addresses processing of personal information associated with an advertising identifier (such as an IDFA or GAAID), we would like to suggest that such example does not apply to requests made by Authorized Agents that directly collect and verify the consumer's advertising identifier through their mobile device.

Indeed, for opt-out requests made by consumers regarding mobile services only based on advertising identifiers, Jumbo Privacy has developed a tool that directly collects such advertising identifier in the consumer's mobile device making the opt-out of sale request. In such case, the consumer cannot temper with such advertising identifier. In order to protect the consumer's identity that was never known to the business to which the request is sent to in the first place, the opt-out of sale request only contains the advertising identifier of such consumer, at the exclusion of any other information.

Adding a layer of verification of information for opt-out of sale request by sending notifications to the consumer upon receipt of such opt-out of sale request would also highly restrict the benefits of mandating an Authorized Agent, where risks of security and error are practically null.

From: Tonsager, Lindsey
To: Privacy Regulations
Subject: CCPA Rulemaking - Written Comments of the Entertainment Software Association
Date: Tuesday, February 25, 2020 3:51:48 PM
Attachments: 2.25.2020 ESA CCPA Comments.pdf

Dear Privacy Regulations Coordinator:

Please find attached the comments of the Entertainment Software Association regarding the modifications to the proposed regulations implementing the California Consumer Privacy Act.
Respectfully submitted,
Lindsey Tonsager
Counsel for the Entertainment Software Association

Lindsey Tonsager

Covington & Burling LLP
Salesforce Tower, 415 Mission Street, Suite 5400
San Francisco, CA 94105-2533
T [redacted] | [redacted]
www.cov.com

COVINGTON

February 25, 2020

Via Email

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

RE: Written Comments on the Modified Draft CCPA Regulations

To Whom It May Concern:

The Entertainment Software Association ("ESA")[1] submits these comments in response to the Attorney General's Updated Notice of Modifications to Text of Proposed Regulations implementing the California Consumer Privacy Act ("CCPA").[2] These modifications take several important steps in the right direction to ensure the privacy and security of Californians' is protected, consistent with the statute. ESA and its members respectfully request that the Attorney General further clarify the four points described below to avoid confusion about how the Attorney General's office plans to interpret and enforce the statutory requirements.[3]

[1] ESA is the U.S. association for companies that publish computer and video games for video game consoles, handheld devices, personal computers, and the internet. There are over 900 video game companies in the State of California.

[2] California Department of Justice, Updated Notice of Modifications to Text of Proposed Regulations And Addition Of Documents And Information To Rulemaking File (Feb. 10, 2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-mod-020720.pdf?.

[3] In addition, ESA reiterates its request that the Attorney General strike the requirement in Section 999.317(g) to publish certain metrics regarding responses to consumer requests. While raising the threshold for this requirement from four to ten million consumers diminishes the impact of this provision, this revision does not address the underlying concerns raised by ESA and a number of other commenters, that (for example) compiling the required metrics may not be practically feasible and that publication could unintentionally mislead consumers about a company's compliance. *See, e.g.* Comments of ESA at 6-8; Comments of California Chamber of Commerce at 21; Comments of California Retailers' Association at 17; Comments of CCIA at 9-10; Comments of News Media Alliance at 8; Comments of American Bankers Association at 7; Comments of U.S. Chamber of Commerce at 7-8.

W235-1

1. Reaffirm that businesses may refuse consumer requests that create a risk to security or the integrity of a business's systems.

The modified draft regulations strike the language in Section 999.313(c)(3) explaining 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."

Clearly, the deletion of this language could not have intended to require a company to provide access to an individual reasonably believed to be unauthorized or a malicious actor trying to compromise the integrity or security of the business's systems or networks. Such an interpretation would not only undermine the purposes of the statute, but also would force businesses to act in a manner inconsistent with other legal obligations, such as California's requirement to "maintain reasonable security procedures and practices" to protect the security of personal information.[4] W235-2

Consequently, ESA and its members understand that this language was deleted because it is not necessary. For example, it would be redundant with the statute's requirement that consumer requests be "verifiable" and with existing exemptions permitting a business to deny a consumer request if it would impede a business's ability to comply with law, exercise or defend legal claims, or avoid adversely affecting the rights and freedoms of other consumers.[5] Clarifying this point in the Final Statement of Reasons, however, would avoid any doubt regarding the Attorney General Office's intentions in deleting the draft language.

2. Further clarify the CCPA's "sale" definition.

ESA appreciates the clarifications in the modified draft regulations that (1) the only user-enabled privacy controls covered under the statute are those that communicate or signal a consumer's choice to opt out of the ***sale*** of personal information and that (2) sale opt-outs must require the consumer to affirmatively select their choice.[6] This language not only reaffirms ESA's understanding that the Attorney General never intended to force businesses to honor do-not-track signals as opt-out-of-sale requests,[7] but also clarifies that businesses need not honor third-party settings that opt consumers out of data sales by default. By emphasizing that businesses must honor the consumer's expressed preference and because a consumer might make a different choice (or no choice at all) on other browsers or devices, this language also helps clarify that, to the extent controls for sales of personal information are specific to a particular browser or device, such controls should apply only to that particular browser or device. W235-3

[4] *See* Cal. Civ. Code § 1798.81.5(b).

[5] *See, e.g., id.* §§ 1798.110(b), 1798.115(b), 1798.145(a)(1), (4), 1798.145(l).

[6] Modified Proposed Text of Regulations, § 999.315(d)(1).

[7] *See* Comments of ESA at 11 n.32.

However, notwithstanding multiple requests from commenters for further guidance on the scope of the "sale" definition, the modified draft regulations do not explicitly address this issue.[8] As ESA explained in its prior comments, the statutory text and legislative history are clear that a disclosure is not a "sale" if the exchange of personal information is not "for monetary or other valuable consideration."[9] Consequently, disclosures of personal information to third parties who receive personal information in order to (for example) provide or facilitate video game services to players should be treated as a disclosure of personal information for a business purpose, and not a "sale" of such information. If the Attorney General does not address this issue in the final regulations, ESA requests that it be clarified in the Final Statement of Reasons. W235-4

In addition, the modified draft regulations make permissive the double opt-in for consumers to submit a deletion request, but retains a two-step process when a consumer opts in to data sales (either because the consumer reverses their decision to opt out or is at least 13 and less than 16 years of age).[10] ESA requests that the Attorney General harmonize these provisions so that a double opt-in, which is not contemplated anywhere in the statutory text, is permissive in all circumstances, and is not legally required. W235-5

3. Further conform the children's privacy language with the helpful COPPA clarifications included in the modified draft regulations.

Commenters overwhelmingly supported bringing the initial draft regulations into alignment with the Children's Online Privacy Protection Act ("COPPA"), and ESA appreciates the revisions in the modified draft regulations come closer to this goal.[11] However, some legacy language remains in the regulations that inadvertently could be interpreted to require multiple parental consents. Specifically, the modified draft regulations suggest that the affirmative authorization required under the CCPA is "in addition to" verifiable parental consent obtained under COPPA. As a result, there could be some confusion over whether two methods of parental consent are required—one for CCPA and a second one for COPPA. Such a result clearly would be duplicative and unduly burdensome for parents. Consequently, ESA respectfully requests that the Attorney General make one additional conforming edit to Section 999.330(a)(1): W235-6

> A business that has actual knowledge that it sells the personal information of children under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. This affirmative authorization ~~**is in addition to**~~ *may include* any verifiable parental consent required under COPPA.

[8] *See, e.g.*, Comments of Computer and Communications Industry Association (CCIA) at 2; Comments of ESA at 10-11; Comments of IG US Holdings, Inc. at 6-7; Comments of the Association of Test Publishers at 7; Comments of Consumer Bankers Association at 4-5; Comments of SchoolsFirst Federal Credit Union at 1.

[9] Comments of ESA at 10-11.

[10] *Compare* Modified Proposed Text of Regulations, § 999.312(d), *with id.* §§ 999.316(a) and 999.301(a).

[11] *See, e.g.* Comments of CCIA at 10; Comments of Consumer Technology Association at 13; Comments of CTIA at 22-24.

4. Further clarify that the service provider provision is consistent with the statutory text.

Multiple commenters, including ESA, noted that the initial draft regulations governing service providers were inconsistent with the statutory text and needed to be revised to permit the processing of personal information for the service provider's "business purposes," as that term is defined under the statute.[12]

The modified draft regulations expand the circumstances in which a service provider may process personal information.[13] And a reasonable interpretation of the modified draft regulations is that processing of the personal information as permitted in the written contract is a "notified purpose" permitted under the statute's "business purpose" definition.[14] For example, if the services specified in the written contract with the business include allowing the service provider to segment households or consumers into audiences for advertising or marketing, then this would be permissible under Section 999.314(c)(1) of the modified draft regulations. W235-7

This interpretation is consistent with the statute's "business purpose" definition, which explicitly authorizes "the use of personal information for . . . 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" and includes "providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider."[15] ESA encourages the Attorney General to explicitly adopt this interpretation in the Final Statement of Reasons.

* * *

ESA appreciates the significant efforts of the Attorney General's Office in this rulemaking and welcomes the opportunity to continue working with the Attorney General and his staff on these important issues.

[12] *See, e.g.*, Comments of California Cable and Telecommunications Association at 8-11; Comments of California Chamber of Commerce at 11-12; Comments of CCIA at 7; Comments of Consumer Data Industry Association at 13; Comments of Consumer Technology Association at 9-11; Comments of CTIA at 14-16; Comments of Engine Advocacy at 5-6; Comments of NAI at 24-25.

[13] Modified Proposed Text of Regulations, § 999.314(c).

[14] § 1798.140(d).

[15] *Id.*

Sincerely,

Gina Vetere
Senior Vice President and General Counsel
Entertainment Software Association

From: Hall, Britanie A.
To: Privacy Regulations
Subject: Comments to the California Attorney General"s CCPA Rulemaking
Date: Tuesday, February 25, 2020 3:50:00 PM
Attachments: Hogan Lovells US LLP Comments to CCPA Regulations (02.25.2020).pdf

Dear Privacy Regulations Coordinator,

Please find attached comments to the California Attorney General's CCPA Rulemaking, prepared by Hogan Lovells.

Sincerely,
Britanie Hall

Britanie Hall
Senior Associate

Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004

Tel: +1 202 637 5600
Direct: [redacted]
Fax: +1 202 637 5910
Email: [redacted]
www.hoganlovells.com

Please consider the environment before printing this e-mail.

Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

February 25, 2020

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

COMMENTS OF HOGAN LOVELLS US LLP
In connection with the Office of the Attorney General Rulemaking
Regarding the California Consumer Privacy Act of 2018

As a global law firm, Hogan Lovells counsels clients of all sizes across a range of industries. We are providing these comments after consultations with a number of our clients, many of whom are subject to the California Consumer Privacy Act ("CCPA") and are interested in the California Attorney General's efforts to provide clarity and sensible guidance through the rulemaking process.[1]

Our goal in providing the comments below is to encourage a set of standards that provides meaningful privacy protections for consumers and practical guidance for businesses seeking to comply with the CCPA. We appreciate the opportunity to provide input, and we respectfully request that the Attorney General consider these comments in the course of its rulemaking proceedings.

1. **§ 999.305(a)(4) — The obligation to provide just-in-time notices when collecting personal information from a mobile device should be removed because (1) it goes beyond the notice requirements in the statute, (2) it would create a vague standard of what constitutes "a purpose that the consumer would not reasonably expect," and (3) the new just-in-time notice is not narrowly tailored to highlight or provide meaningful information in addition to that required by the existing notice at collection requirement.**

Section 999.305(a)(4) proposes a novel requirement: if a business collects personal information from a consumer's mobile device for a purpose that "the consumer would not reasonably expect," the proposed regulation would require the business to provide a just-in-time notice. This obligation does not exist in the statute;[2] indeed, it goes beyond the existing § 1798.100(b) obligation to provide a "notice at collection" at *or before* the point at which personal information is collected given that a literal reading of the proposed regulation would require the business to display a new notice *during each session* the business collects certain information (rather than only once prior to collection). W236-1

Second, the proposed regulation would create a vague standard regarding what constitutes "a purpose that the consumer would not reasonably expect." The regulations provide an example of a flashlight app that collects geolocation information (a reference to the FTC's settlement with

[1] These comments are not intended to represent the views of any specific client.
[2] *See* Cal. Civ. Code § 1798.100(b).

Goldenshores Technologies, LLC). But outside of innocuous-seeming applications like the flashlight app collecting highly sensitive information like geolocation information, this creates incredible uncertainty regarding what types of information or purposes of collection would trigger the new notice requirement. For example, the average consumer may not know that mobile apps collect analytics to understand how the app is functioning, in order to improve the app. Under a plain reading of the proposed regulation, this relatively benign data use might trigger a "just-in-time" pop-up notice. And faced with this vague requirement and the possibility for significant penalties under the CCPA, companies may take a conservative approach and provide more just-in-time notices. Depending on the nature of a particular app, more frequent notices have the potential to negatively impact user privacy, safety, and experience in a number of ways, from minor distractions that users will just click through without reading to potentially dangerous interruptions (e.g., navigation apps used while driving).

W236-1 (cont.)

Third, the just-in-time notice required is not narrowly tailored to provide the consumer with meaningful information about the type of personal information collected or purpose of processing that they would not expect. Instead, the requirement appears to just introduce a requirement for a new, third type of CCPA notice covering information that must already be covered in the existing notice at collection requirement and the business's more detailed online privacy notice, with a single prescriptive example of how that additional notice might be provided. If just-in-time notice is required because of a consumer expectation gap, then it seems that the requirements for the contents of such notice should be narrowly tailored to close that expectation gap.

If this proposed § 999.305(a)(4) is retained, the Attorney General at minimum should clarify (1) that this is part of the § 1798.100(b) notice at collection requirement, (2) that such enhanced notice at collection must be provided (e.g., as a pop-up) only once before the personal information is collected, and (3) the purposes or types of personal information collected that trigger this just-in-time notice, including examples of what *is* reasonably expected.

2. § 999.305(d) — Businesses that do not collect information directly from consumers should not be required to provide a notice at collection, even if they are not registered data brokers.

The prior draft of § 999.305(d) provided a clear exception to the notice at collection requirement for businesses that do not collect personal information directly from consumers but do not sell personal information to third parties. The Attorney General should restore the previously proposed exception for such businesses that do not sell personal information to third parties.

W236-2

Otherwise, effectively requiring direct outreach by these businesses to consumers means consumers will receive that many more emails, letters, and phone calls with little practical benefit, especially considering this subset of businesses does not engage in sales (as they are not "data brokers" as defined by the statute[3] and already subject to an exemption from the direct notice requirement) and thus would not be providing the consumer a sale opt-out. In addition, businesses without a direct relationship to consumers and who do not engage in sales will be forced to engage in burdensome outreach to consumers in order to contact them directly and provide a notice at collection; counter-intuitively, this is more of an obligation than data brokers face. This would be

[3] *See* Cal. Civ. Code § 1798.99.80(d).

costly, time-consuming, and in some cases impossible, such as where the business does not have a consumer's contact details.

The most recent revisions to the draft regulations created an exemption from the notice requirement specifically for businesses who register as a "data broker." This is a reasonable exception, given that consumers can obtain information about businesses who sell their personal information without a direct relationship. However, the exception from having to directly notify consumers should extend to businesses that do *not* further sell information as well.

W236-2 (cont.)

3. **§ 999.308(c)(1)(e)(2) — The requirement to identify the categories of third parties to whom *each category* of personal information was disclosed or sold adds length and complexity to privacy notices without adding meaningful value to consumers.**

The proposed requirement to disclose a granular list of categories of third parties for each and every enumerated category of personal information collected by a business goes beyond the requirements of the statute.[4] More importantly, it would add length and complexity to privacy notices without providing meaningful value to consumers. For example, if even one category of personal information about a single consumer were disclosed to a particular category of recipient, the published privacy notice would have to reflect this. In practice, privacy notices will grow that much longer and be that much harder for consumers to parse.

W236-3

Thus the requirement to identify the categories of third parties to whom each category of personal information was disclosed or sold should be struck. Businesses should instead only be required to disclose the categories of third parties to whom all categories of personal information may be disclosed or sold, consistent with the requirement in the statute.[5]

4. **§ 999.312(a) — The Attorney General should clarify that businesses operating "exclusively online" should be interpreted to include businesses that may have non-online components, such as customer service or technology support, so long as substantially all other business is transacted online.**

Section 999.312(a) allows a business that operates "exclusively online" and has a direct relationship with a consumer from whom it collects personal information to offer only an email address as a designated method for submitting right to know requests, but the regulations provide no guidance on the meaning or scope of what it means to operate "exclusively online." The Attorney General should clarify that this designation should be interpreted to include businesses with some non-online components, so long as substantially all other business is transacted online.

W236-4

For example, many businesses do not have physical storefronts and conduct all or almost all transactions online, but they may provide certain minimal non-online services for the benefit of their consumers, like troubleshooting or providing support for purchases made online. Requiring these businesses to maintain a toll-free number to submit rights requests would necessitate engaging additional customer service teams or providing substantial additional training where consumers otherwise fully utilize the business's products or services online. This would undermine the policy behind allowing businesses that consumers transact with online to maintain an online-only method for receiving right-to-know requests.

[4] *See* Cal. Civ. Code § 1798.110(c)(4).
[5] *Id.*

5. **§ 999.312(b) — As with "right to know" requests, if a business operates exclusively online and has a direct relationship with consumers, the business should be required to provide only an email address for deletion requests.**

The policy of providing online businesses with an exception from the requirement to provide two designated methods for submitting right to know requests makes sense, as it recognizes a practical reality of the digital marketplace and acknowledges how consumers interact with online businesses. For purposes of consistency and operational efficiency, this same exception should be extended to deletion requests. Not only would this approach make it easier for online businesses to comply with the CCPA, it would substantially simplify the back-end process required to efficiently service rights requests. It also makes the process less confusing for consumers and helps minimize user error when submitting rights requests (i.e., mistakenly submitting a right to know request via the wrong method may lead to delays and frustrated consumer expectations). Finally, allowing for rights requests via a single email point of contact would align with international standards for submitting rights requests (such as data subject rights requests under the GDPR). W236-5

6. **§ 999.313(c)(3) — The previously proposed exception to responding to right to know requests for personal information that creates security risks should be reinstated, and the newly proposed exception for personal information that is not kept in a searchable format and maintained solely for legal or compliance purposes should be split into two separate exceptions.**

The modified regulation at § 999.313(c)(3) removed the previously proposed exception from disclosing specific pieces of personal information in response to requests to know where the disclosure would create a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account, or the security of the business's systems or network. It also added a new exception when four conditions are met: (a) the business does not maintain the personal information in a searchable format or reasonably accessible format; (b) the business maintains the personal information solely for legal or compliance purposes; (c) the business does not sell the personal information and does not use it for any commercial purpose; and (d) the business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the prior three conditions.

First, the Attorney General should reinstate the previously proposed security exception deleted from the October 2019 draft regulations. This exception is vital to maintaining the security of the digital economy and should be reinstated to protect personal information and provide additional clarity for consumers and businesses. Without it, there is increased risk to consumers where the disclosure of their information may lead to security risks, and businesses will no longer be put in the difficult position to decide between disclosing personal information or compromising their security. Businesses can, of course, be expected to bear the burden of proof that their assessment of the security risks posed by disclosure demonstrated a substantial, articulable, and unreasonable security risk. W236-6

Second, while the newly proposed exception is helpful in reducing compliance burdens and security risks to businesses without meaningfully impacting consumer privacy, the first two prongs at §§ 999.313(c)(3)(a) & (b) should be separate exceptions, provided that the current third and fourth conditions in §§ 999.313(c)(3)(c) & (d) are both met for each exception to apply. W236-7

Stated another way, the Attorney General should amend this section to create separate exceptions providing that, in responding to a request to know, a business is not required to search for personal information if:

(a) The personal information is not maintained in a format that is reasonably searchable or accessible—provided that the business (1) does not sell the personal information or use it for a commercial purpose and (2) describes to the consumer the categories of records that it did not search for this reason. Even where such information is not maintained solely for legal or compliance purposes, requiring businesses to attempt extensive searches of prohibitively difficult-to-search files (e.g., backup tapes, email inboxes of employees not involved in sales or customer service) will result in a time-consuming, expensive, and in many cases unproductive process, the costs of which will ultimately be passed down to consumers. In other cases where files are completely inaccessible, it may not be possible to conduct a search at all. Even a business that makes a good faith effort to comply with a request to know may find itself in violation of the CCPA, and for that reason the Attorney General should amend this section accordingly. W236-7 (cont.)

(b) The business maintains the personal information solely for legal or compliance purposes—provided that the business (1) does not sell the personal information or use it for a commercial purpose and (2) describes to the consumer the categories of records that it did not search for this reason. Because information maintained solely for legal or compliance purposes is not of particular value for a consumer's right to know how a business is processing their personal information for commercial or business purposes, it would reduce the production of less-meaningful information to consumers to exempt the production of this information even where it is in a format that is reasonably searchable or accessible. For example, businesses that segregate the personal information that they maintain solely for legal or compliance purposes outside of their operational/production systems—such as personal information that consumers request be deleted but which must still be maintained for legal or compliance purposes—would not have to search those systems.

7. § 999.313(c)(4) — Payment card numbers should be added to the list of types of personal information that cannot be disclosed in response to a request to know.

Highly sensitive personal information, such as a consumer's social security number, driver's license number, and financial account number, should not be disclosed in response to a request to know due to the particularly acute security risks posed to consumers and businesses alike, and the approach taken in the proposed regulations is generally reasonable. However, while the proposed regulation already covers financial account numbers, to eliminate any potential uncertainty and to ensure consumers are not subjected to unnecessary risk of fraud or tangible financial harm, § 999.313(c)(4) should be updated to expressly include payment card numbers to the list of personal information that should not be disclosed in response to a rights request. W236-8

8. § 999.313(d)(5) — The updated text should be amended to remove the implied obligation to ensure that a consumer's personal information remains deleted from the business's records, even if the business collects it a second time. W236-9

In the context of responding to a deletion request, the updated regulations state that a business may retain a record of the request "for the purpose of ensuring that the consumer's personal information

remains deleted from the business's records."[6] This introduces an implied obligation, not included in the statute,[7] to ensure that a consumer's personal information remains deleted from the business's records, even if the business collects it a second time, such as in the course of ongoing interactions with the consumer. This would change the fundamental nature of a deletion request into a perpetual opt-out from the collection or storage of a consumer's information, regardless of how the consumer chooses to interact with the business going forward. Essentially, this would be more akin to an obligation to create and maintain a "do not track" registry than a right for consumers to request that businesses delete their personal information.

W236-9 (cont.)

As such, the proposed regulation creates a requirement that in many cases may not align with consumer expectations about what it means to submit a deletion request. For example, if a consumer with an account with a business submits a deletion request but then decides to sign up for a new account, the proposed requirement could be interpreted to require the business to immediately delete the consumer's information. At minimum, the proposed requirement introduces significant uncertainty for consumers and businesses.

The implied requirement should instead be removed, and the second sentence of § 999.313(d)(5) should be amended to say, "A business may retain a record of the request for the purpose of demonstrating compliance with the request to delete."

9. **§§ 999.314(a), (b) — These subsections now use the word "business" but appear to refer to its general meaning, when that term is defined by the CCPA and carries a specific meaning; this should be revised to use a different term than "business" when not referring to the defined term.**

The additions of "business" to §§ 999.314(a) and (b) in place of the language "a person or entity" appear to refer to the dictionary definition of a "business"—i.e., as a legal entity—when in fact "business" is statutorily defined by the CCPA with the specific meaning of a for-profit entity with primary control and responsibility over the collection and processing of consumers' personal information.[8] By contrast, a "service provider" as defined by the CCPA processes personal information "on behalf of a business."[9]

W236-10

If the revised §§ 999.314(a) and (b) are read using the statutorily defined term "business," this introduces uncertainty as to how these sections should be interpreted and which "requirements and obligations of a 'service provider'" would trigger these provisions. For clarity, both §§ 999.314(a) & (b) should use a different term than "business" if not referring to the defined term—such as "legal entity."

10. **§ 999.315(d) — This subsection should be removed or revised to no longer require businesses to comply with third-party or browser privacy settings, which is currently unworkable and not required by the statute.**

The proposed revisions to § 999.315(d) still require businesses to comply with third-party or browser privacy controls and settings, which can proliferate and be difficult for businesses to integrate if there

W236-11

[6] California Consumer Privacy Act Regulations, Text of Modified Regulations, § 999.313(d)(5).
[7] *See* Cal. Civ. Code §§ 1798.105 & .130.
[8] Cal. Civ. Code 1798.140(c).
[9] Cal. Civ. Code 1798.140(v).

is not clarity as to a common standard or approved list of controls and settings. This requirement also does not exist in the statute, which requires businesses only to honor opt-out requests from consumers or their authorized agents.[10] As currently written, the proposed regulation introduces a requirement that very few, if any, businesses could comply with due to the number of possible privacy controls, device settings, browser plugins, and other theoretical third-party opt-out mechanisms. It also places an unrealistic burden on businesses to discern ambiguous actions taken by consumers, such as adjusting device settings that may or may not clearly align with a sale opt-out. This could lead to confusion for consumers and an inability for businesses to accurately respond to consumer requests.

W236-11 (cont.)

Rather than creating this new obligation that does not currently exist under the statute, the Attorney General should consider conducting further studies of various third-party opt-out solutions in order to craft regulations that approve specific standards for such signals, communications, or settings without creating a standard that will be functionally impractical to comply with, especially by small- and medium-sized businesses. Ideally, these regulations should also consider the practical issues inherent to third-party privacy controls, such as which entities need to respond to these signals (i.e., businesses, service providers, or both) and how to distinguish between signals from inside and outside California.

For the time being, § 999.315(d) should be removed or substantially revised to no longer require businesses to comply with third-party or browser privacy settings.

11. §§ 999.305(a)(2)(d), .306(a)(2)(d), .307(a)(2)(d) & .308(a)(2)(d) — The Web Content Accessibility Guidelines should be listed as an example of how businesses may address accessibility requirements, but they should not be expressly required for every website subject to the CCPA without any study on how it will impact businesses.

In several sections throughout the updated regulations, the Attorney General has incorporated a specific requirement that privacy notices posted online must comply with generally recognized industry standards for accessibility, such as the Web Content Accessibility Guidelines ("WCAG"). Given the relative lack of generally recognized industry standards for accessibility, this will become a de facto requirement that every CCPA-regulated business with a website will seek to comply with the very prescriptive requirements of the WCAG, absent a viable alternative.

W236-12

Considering that this requirement does not currently exist for most commercial websites and no studies have been undertaken to measure the potential impact to businesses and benefit to consumers of implementing the WCAG in lieu of other potential reasonable accessibility accommodations, requiring compliance with a specific standard for all websites will add significant compliance costs for these businesses, with a disproportionate impact on smaller businesses. This standard should be more flexible to account for the nature and context of particular websites and online services.

Instead of strongly implying that the WCAG will be the de facto standard, the requirement should revert to the flexible standard previously proposed: website privacy notices should "[b]e reasonably accessible to consumers with disabilities" and businesses shall, at minimum, provide information on how a consumer with a disability may access the notice in an alternative format. At the same time,

[10] *See* Cal. Civ. Code 1798.120 & .135(c).

the WCAG can instead be listed as an example of one way to satisfy the accessibility requirements, but they should not be functionally required for every website subject to the CCPA. W236-12 (cont.)

From: [redacted]
To: Privacy Regulations
Subject: Comments on Modified Regulations - CCPA
Date: Tuesday, February 25, 2020 3:44:58 PM
Attachments: myLetter.pdf

February 25, 2020

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

RE: Comments on Modified Regulations - CCPA

Dear Ms. Kim,

I am writing on behalf of SAFE Credit Union (SAFE), which serves 13 counties in Northern California. We have about 235,000 members and $3 billion in assets. SAFE respectfully submits the following comments to the California Department of Justice on its proposed modified regulations concerning the California Consumer Privacy Act (CCPA).

SAFE appreciates the efforts of the California Department of Justice to gather feedback on the Modified Proposed Regulations but opposes the applicability of the CCPA to credit unions. While we support the spirit of the law, we still have some concerns regarding the practicality and implementation of CCPA's Modified Proposed Regulations published on February 10, 2020. Credit unions in California are already subject to the Gramm-Leach-Bliley Act (GLBA) and the California Financial Information Privacy Act (CFIPA). SAFE takes great care to safeguard the integrity of members' personal data and provide notice regarding the sharing of that data. Although some relief was provided via the Modified Proposed Regulations, the CCPA remains burdensome, proposing costly compliance obligations for credit unions and confusion for consumers. The Modified Proposed Regulations do not address the variety of exceptions under the CCPA statute, including exceptions under the GLBA and CFIPA.

The Notification Process of a Consumer's Rights

The Modified Proposed Regulations do not establish sufficient rules and procedures for compliance with the CCPA's notice provisions. The privacy policy and notice requirements create confusion and additional burdens for covered credit unions and our members because the they: (1) do not address the exceptions for financial institutions under the GLBA and CFIPA, and (2) create multiple notice requirements for information they presently provide under the GLBA and CFIPA.

W237-1

Disclosure Requirements

The disclosures under the Modified Proposed Regulations would require credit unions to provide detailed notice about the information collected on consumers. Under the GLBA, a credit union is already subject to the following privacy requirements:

- Must provide initial and annual notice of its privacy policies to its customers, both members and nonmembers, and any other consumer if his or her data will be shared with nonaffiliated third parties; and

- Must allow the consumer to opt out of the disclosure of the consumer's nonpublic personal information to a nonaffiliated third party if the disclosure occurs outside of certain exceptions in the regulations.

Despite the fact that credit unions already provide detailed notice under the GLBA, Article 2 of the Modified Proposed Regulations still imposes an expanded disclosure requirement regarding information collection and privacy policies. The Modified Proposed Regulations do not offer any clarification as to how a credit union which is covered by GLBA that still collects information outside of the GLBA's scope should reconcile the detailed privacy notice required by that law with the additional, detailed notice required by the CCPA. Only information that is not already subject to the GLBA is covered by these notice provisions in the CCPA, therefore, it would appear that a credit union would be in compliance if it were to draft a Privacy Policy that only covered the information that falls outside of the GLBA. However, such a policy could hardly be called a comprehensive description of the credit union's privacy policies. As written, the proposed regulations do not give proper effect to the GLBA exemption in the CCPA and create notice and disclosure requirements that are confusing and ambiguous and will not serve to give consumers easily understandable information. W237-1 (cont.)

The CCPA allows the California Attorney General to add "any exceptions necessary" to ensure that notices provided to consumers are easily understood. The Modified Proposed Regulations should exempt credit unions subject to the GLBA from further disclosure requirements if they are in compliance with the GLBA and their existing annual privacy notice is posted on the credit union's website. The distinction between GLBA-covered information and CCPA-covered information is not one that consumers will instinctively identify and providing consumers with multiple, detailed privacy disclosures will only be confusing and frustrating for them.

If the California Attorney General is not willing to provide an exception for credit unions, it must provide guidance as to how we can comply without requiring duplicativenotices or unnecessarily burdening credit unions. For credit unions already providing detailed privacy policy disclosures, such a requirement should make reference to the inclusion or addition of information to existing notices, rather than requiring separate, free-standing disclosures which will only serve to confuse consumers and place unnecessary compliance burden on credit unions. A separate, free-standing notice would require covered businesses to undertake a separate and new disclosure process, creating additional compliance burdens.

Model Notices

It would be beneficial to have model language or forms for the required notices under the CCPA, as it pertains to financial institutions. In the financial industry, model forms or guides with specifics, which are provided to consumers, are particularly helpful for successful compliance. Like other model language or forms for privacy laws this could provide a safe harbor; and consumers will benefit by being able to recognize the uniformity of the different types of notices so they may better understand and exercise their privacy rights.

W237-2

Exemptions Under the CCPA

As a state-chartered credit union, engaging with consumers and handing financial data, we understand the importance of properly managing the sensitive information we obtain. As a result, we have built strong privacy programs that adhere to data privacy and security requirements including the GLBA, and CFIPA, and the National Credit Union Administration's (NCUA's) data security regulations (12 CFR Part 748 and its Appendices). We will be able to better serve consumers with clarity from the California Attorney General on how the GLBA and CFIPA exemptions specifically apply to the CCPA.

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

W237-3

In addition, the GLBA pertains to "personally identifiable financial information" collected in the course of a transaction or when providing a financial product or service. The CCPA pertains to personal information collected in basically any manner, including when there is no transaction. Due to inconsistent terminology, the exemption provided is unclear and can be interpreted several ways. We propose that all financial institutions, already subject to the strict requirements of GLBA and CFIPA, be expressly exempted from the CCPA. A clearly defined exemption will better manage consumer expectations about their privacy rights and eliminate confusion on what personal information is covered or not covered under the CCPA.

Despite the CCPA's failure to offer exemptions that apply to financial institutions, SAFE maintains the position that the CCPA should not apply to credit unions. In the alternative, the California Attorney General should establish implementing regulations that clarify that the requirements of the CCPA and its implementing regulations do not apply to organizations that solely collect GLBA-covered and CFIPA information. Implementing regulations should clarify that financial institutions can comply with CCPA through a regulatory regime that works in tandem with the GLBA and CFIPA, rather than have entirely separate requirements, which will be confusing for consumers and overly burdensome to credit unions.

There is also an opportunity to provide more guidance on non-written interactions with consumers that require the notice at collection, such as during the collection of

W237-4

applications for credit union membership accounts or loan applications via telephone. The Modified Proposed Regulations require a Notice at Collection, 999.305(a)(1) to "…provide consumers with timely notice, at or before the point of collection about the categories of personal information to be collected from them and the purposes for which the personal information will be used." This will translate into a lot of information that will need to be disclosed via this channel, but no guidance is given for how to properly provide the notice during this oral, non-written interaction. Since other solutions seem impractical and burdensome to the consumer, such as requiring them to open a link or go to a website to review a Notice at Collection, we would again, like to recommend an exemption for providing the Notice at Collection for non-written interactions with consumers. W237-4 (cont.)

Handling Consumer Requests

Responding to Requests to Know

As modified, when responding to a request to know, a business is not required to search for personal information if "all" of the specified conditions are met. We recommend that the exemption apply for "any" of the conditions listed within 999.313 (c)(3)(a.) through (c)(3)(c.), instead of "all." W237-5

Otherwise, we recommend additional clarification for 999.313 (c)(3)(a.)"The business does not maintain the personal information in a searchable or reasonably accessible format." We would ask for examples of what is considered "searchable" or "reasonably accessible format." W237-6

We support 999.313 (c)(3)(d.) noting that the business should describe, to the consumer, the categories of records it did not search because it met any number of the three conditions stated. W237-7

Responding to Requests for Opt-Out

Regarding requests to opt-out, credit unions are already required by the GLBA and CFIPA to provide consumers an opportunity to opt-out of information sharing practices. It would be easiest and most streamlined for consumers to make an opt-out request regarding the sharing or sale of their information at one time and in the same manner, rather than having a separate opt out process for CCPA. W237-8

Extension of Moratorium

SAFE understands that, per statute, the CCPA became operative on January 1, 2020 and there is a moratorium on enforcement by the California Attorney General until July 1, 2020. However, given ambiguities in the law, the need for additional guidance and the significant difficulties associated with reconciling the requirements for the GLBA and CFIPA-covered entities, warrants a delay in enforcement. Although SAFE objects to the applicability of theCCPA to credit unions, we request an additional delay in enforcement actions by the California Attorney General to help ease the burden of compliance. W237-9

If a credit union affords consumer privacy rights under GLBA and CFIPA to W237-1 (cont.)

consumers associated with business/commercial accounts, to whom we provide financial products and services, then the CCPA exemptions should be applied. We believe that the temporary exemption for consumers of business/commercial accounts should be made a permanent exemption, rather than expiring in January 1, 2021.

As an employer in California, we value and protect our employee's privacy and the provisions for employee privacy rights. However, CCPA presents a significant challenge to financial institutions as employers in California. We believe that the temporary exemption to providing an employee privacy notice given under AB 25, should be made a permanent exemption rather than expiring in January 1, 2021.

W237-1 (cont.)

Privacy of our consumers' information has and will always be a priority. We ask the California Attorney General for clear guidance to ensure we can fully and thoughtfully reinforce consumer privacy rights. We want to continue to protect members by following the robust privacy requirements set forth in the GLBA and CFIPA.

Thank you for the opportunity to comment on the CCPA Modified Proposed Regulations and for considering our views.

Sincerely,

Sun Park
Vice President, Enterprise Risk Management
SAFE CU

cc: CCUL

From: Jones, Erik
To: Privacy Regulations
Subject: CompTIA Comments - Revised CCPA Implementing Regulations
Date: Tuesday, February 25, 2020 3:43:47 PM
Attachments: CompTIA CCPA Comments 2.25.2020.pdf

Please find attached CompTIA's comments on the Department of Justice's revised California Consumer Privacy Act (CCPA) implementing regulations.

Let us know if you have any questions or issues accessing the document.

Sincerely,

Erik

Before the
CALIFORNIA DEPARTMENT OF JUSTICE
Los Angeles, CA 90013

In the Matter of	)
	)
Revised California Consumer Privacy Act	)
Implementing Regulations	)

COMMENTS OF THE COMPUTING TECHNOLOGY INDUSTRY ASSOCATION

Dileep Srihari
Vice President and Senior Counsel

Alexi Madon
Vice President, State Government Affairs

COMPUTING TECHNOLOGY
INDUSTRY ASSOCIATION
3500 Lacey Road, Suite 100
Downers Grove, IL 60515

February 25, 2020

INTRODUCTION

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 Department of Justice's revised California Consumer Privacy Act (CCPA) regulations. 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.

In these comments, we offer additional guidance to address concerns that remain in the revised version of the regulations. CompTIA appreciates the changes the Department made to the prior version in response to stakeholder feedback. While a number of these changes represent an improvement to the regulations, we believe that additional edits to the proposed regulations should be made. These edits are addressed below.[2]

DISCUSSION

I. § 999.301(a). Authorization Should Not Include Multiple Steps

The draft rules define "affirmative authorization" as:

> an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a child under 13, it means that the parent or guardian has provided

W238-1

[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.

[2] The proposed edits in these comments do not necessarily represent the only areas for improvement in the proposed regulations.

consent to the sale of the child's personal information in accordance with the methods set forth in section 999.330. For consumers 13 years and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

CCPA requires detailed notice concerning consumers' right to opt in to the sale of their information. This requirement, along with consumers having to affirmatively and "clearly request to opt-in," works to ensure that consumers are making informed choices.

It is therefore unclear why consumers would need to undertake an extra step concerning their affirmative and clear choice. Multiple pop-ups and other prominent notices can interrupt consumers' experiences and lead to confusion. The more notifications presented to consumers, the less likely consumers can comprehend or absorb any one particular notice and make informed choices about their data.

W238-1 (cont.)

The more notices that companies display, the greater the chance of creating "click fatigue," whereby consumers skip over the words and click through to continue using the service. To address this issue, we suggest striking the language mandating a two-step process.

II. § 999.305(d). The Indirect Collection Exception Should Apply Beyond Data Brokers.

As § 999.305(d) was previously written, businesses did not need to provide notice at collection if they did not collect information directly from consumers. The revised language now states that only registered data brokers do not need to provide notice at collection in instances of indirect collection:

W238-2

> If a ~~A~~ business that does not collect information directly from consumers is registered with the Attorney General as a data broker pursuant to Civil Code section 1798.99.80, *et seq.* it does not need to provide a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out. ~~to the consumer,~~

We do not believe notice at collection should be required when any business, and not just a registered data broker, indirectly collects publicly available data. For that reason, the prior exception should be reinstated to apply to all businesses.

W238-2 (cont.)

III. § 999.305(a)(4). The Just-In-Time Notification Obligation Should Be Removed.

The just-in-time requirement for mobile devices proposed in § 999.305(a)(4) does not exist in the CCPA and goes well beyond the obligations for notice at collection in the CCPA. Additionally, the proposed standard – a "purpose that the consumer would not reasonably expect" – is too vague. Facing such a vague requirement, companies may provide more just-in-time notices than is warranted or necessary. The resulting over-notification, depending upon the nature of the app, could negatively impact user privacy and experience. For these reasons, this proposed requirement should be removed.

W238-3

IV. § 999.306(f). The Opt-Out Button Graphic Should Be Deleted.

The draft rules have proposed an optional "Do Not Sell My Personal Information" and "Do Not Sell My Info" toggle button. We urge the Department to remove this toggle button as an option due to its unclear design, which inadvertently suggests it is an actual control, whereas it is intended to serve as a link so that consumers can obtain additional information. The button omits important nuances that each business might need to convey based on specific practices. Moreover, excessive standardization could lead to consumers ignoring notifications altogether. The draft requires privacy notices to be "reasonably accessible to consumers with disabilities," yet standardized notification requirements like the envisioned toggle button can fail consumers with disabilities and diverse needs. Businesses will be in the best position to craft notices appropriately tailored to help inform consumers with specific needs and abilities, as they are continuously conducting user interface (UI) and user experience (UX) research.

W238-4

V. § 999.307. The Value of Consumer Data Disclosure Requirements Should Be Deleted.

The section requires "[a]n explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including: a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and a description of the method the business used to calculate the value of the consumer's data."

W238-5

We recommend removing any requirements for providing an estimate of the value of consumer data. We propose:

> "[a]n explanation of how the financial incentive or price or service difference reasonably related to the value of the consumer's data~~, including: a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and a description of the method the business used to calculate the value of the consumer's data~~."

We also propose striking 999.37, which describes the methods in calculating the value of consumer data.

The perceived value of data is subjective, in flux, and depends on context. It does not have independent value. Because data lacks clear, objective value, academics have come up with various methods for estimating the value of certain services to people. Regarding free, ads-based, personalized services, people do not give up or exchange data for their experience. Rather, the experience is made possible by data. This distinction is important. Data enables ads-based services to provide the core of the service itself, which is personalized content. The reason certain businesses can offer their services for free is ***not*** that they are being compensated for an individual's data. They make money selling advertisements. These businesses sell advertisers the opportunity to present their messages to people. And advertisers pay the businesses based on

objective metrics such as the number of people who see their ads or the number of people who click on their ads.

W238-5 (cont.)

VI. § 999.308(c)(1)(e). The New Notification Requirement for Categories of Third Parties Should Be Removed.

The revised proposed regulations would require businesses to disclose "the categories of third parties to whom the information was disclosed or sold" for "each category of personal information identified." The requirement is needlessly burdensome. Disclosing additional categories of third parties will make the privacy policies less consumer-friendly and complicated, and will be burdensome for businesses. As a result, we suggest that this provision be removed.

W238-6

VII. § 999.312(b). The "Exclusively Online" Exception Should Be Extended to Deletion Requests.

We agree that business operating online should have an exception from the requirement to provide two methods for right to know requests. This same exception should be extended to deletion requests. A single email point of contact aligns with international standards for rights requests, would be simpler for consumers, and makes it easier for online businesses to comply with the CCPA.

W238-7

VIII. § 999.313(c)(1). Obligations for Unverified Requests Should Be Removed.

The obligations under § 999.313 for *unverified* requests conflicts with the CCPA. Understandably, the CCPA contemplates that unverified requests should be *discarded* because they are unverified: "A business is not obligated to provide information to the consumer pursuant to Sections … 1798.105 … if the business cannot verify … that the consumer making the request is the consumer about whom the business has collected information …" This approach protects the consumer, as a business should discard an unverified request. If a business is unable to verify the individual's identity, it should not act on requests related to that

W238-8

consumer's personal information. Additionally, the CCPA already has a mechanism for opting-out of the sale of information. Combining verification and opt-out procedures is contrary to the statute and creates the potential for abuse. As such, we recommend making the following edits:

W238-8 (cont.)

> 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).~~

IX. § 999.313(c)(3). The Security Risk Exception Should Be Reinstated.

We request that the eliminated language on "security risks" be reinstated. This language would have enabled a business to not provide specific pieces of information if it met a particular security risk threshold. It was intended to ensure that businesses would not have to compromise security to comply with the law. Accordingly, we request that this language be restored:

W238-9

> 999.313(c)(3) 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.

X. § 999.313(c)(3). Additional Clarification Should Be Provided on When Businesses Should Not Be Required to Search for Personal Information in Response to a Right to Know Request.

We suggest clarifications on conditions under which businesses should not be required to search for personal information in response to a right to know request. As currently written, the draft requires a business to meet enumerated conditions to excuse the business from conducting a search. However, operationally, the exceptions do not work together. For example, when a business maintains personal information solely for legal or compliance purposes (subsection b) it must maintain that information in a searchable or reasonably accessible format (subsection a) so that it can undertake its legal or compliance purposes.

W238-10

Further, the statute and draft regulations currently lack sufficient clarity regarding how far the access right extends. A clear regulation is necessary to draw outer lines around the information a business must make available. Many businesses possess data that may technically fall within the CCPA's broad definition of "personal information," but that is not used in the ordinary course of business, such as log data, is not readily accessible, or has not been "collected." This is particularly true with data that the business has derived, rather than collected, the data. Requiring a business to identify, compile, and then make accessible such information has the adverse effects of forcing a business to create new or more robust consumer profiles. This creates privacy and security concerns for consumers by associating more data with them than otherwise would be, as businesses will be required to build systems with more detailed consumer profiles and then send those profiles outside of the business. Accordingly, we recommend the following edits:

W238-10 (cont.)

> 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, networks, or consumers. In responding to a request to know, a business is not required to provide personal information ~~if all~~ that meets any of the following conditions ~~are met~~, provided the business describes to the consumer the categories of records that may contain personal information it did not provide because it meets one of the conditions stated ~~above~~ below:
>
> a. The business does not maintain the personal information in a searchable or reasonably accessible format;
>
> b. The business maintains the personal information solely for legal or compliance purposes;
>
> c. The business does not sell the personal information and does not use it for any commercial purpose;
>
> d. The business does not associate the personal information with a consumer in the ordinary course of business; or

e. The personal information was not collected from the consumer or a third party, but was instead derived internally by the business.

~~d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.~~

W238-10 (cont.)

XI. § 999.313(c)(4). Payment Card Numbers Should Be Included.

We agree that highly sensitive personal information, such as a consumer's Social Security number, driver's license number, and financial account number, should not be disclosed in response to a request to know. We recommend that § 999.313(c)(4) also include payment card numbers on the list of personal information that should not be disclosed in response to a rights request.

W238-11

XII. § 999.315(d)(1). An Opt-Out Inherently Includes Defaults.

The language in § 999.315(d)(1) is confusing because "shall not be designed with any pre-selected settings" suggests that there can be no default, when it is quite clear that the default would allow for sale of personal information. A consumer is required to select the "opt-out" and an opt-out inherently includes defaults. Accordingly, the language should be modified as follows:

W238-12

> 999.315(d)(1). Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a customer intends to opt-out of the sale of personal information. The privacy control shall require that the consumer affirmatively select their choice to opt-out and shall not be designed in a manner that would prevent the sale of personal information unless the customer affirmatively selects their choice to opt-out. ~~with any pre-selected settings~~.

XIII. § 999.316. The Two-Step Process for Opt-In Should Be Removed

The draft continues to envision a two-step process to opt in to the sale of data, where the consumer requests to opt in to the sale of data and then confirms the opt-in. Multiple pop-ups and other prominent notices are highly likely to be noticed, but can interrupt consumers'

W238-13

experiences. The more notifications presented to consumers, the less likely consumers are to comprehend or absorb any one particular notice and make informed choices about their data. The more notices that companies display, the greater the chance of creating "click fatigue," whereby consumers just skip over the words and click through to continue using the service. We therefore suggest striking the reference to a required "two-step" process.

W238-13 (cont.)

XIV. § 999.317(g). The Recordkeeping Requirements Should Be Deleted

The reporting and recordkeeping requirement presented in §999.317(g) does not exist in the statute itself and therefore has no support in the law. Additionally, the requirement is burdensome and provides little value to consumers. We believe this requirement should be deleted altogether, or at the very least, the requirement to have the metrics posted on the privacy policy should be removed. The percentages of approvals compared to denials for requests under the CCPA, for various reasons, could be very different for different organizations. These differences could be based upon legitimate reasons. However, the differences in these numbers could be misleading to consumers and needlessly cause reputational damages to businesses.

W238-14

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. While we believe the Department has made progress between its initial draft and most recent draft of the regulations, we believe additional changes should be made. 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/ Alexi Madon

Dileep Srihari
Vice President and Senior Counsel

Alexi Madon
Vice President, State Government Affairs

COMPUTING TECHNOLOGY
INDUSTRY ASSOCIATION
3500 Lacey Road, Suite 100
Downers Grove, IL 60515

From:	Ferber, Scott
To:	Privacy Regulations
Cc:	Farber, David; Chittenden, Kelley
Subject:	Modified Proposed California Consumer Privacy Act Regulations
Date:	Tuesday, February 25, 2020 3:36:51 PM
Attachments:	image001.png ACP-ltr-2-25-20.pdf ACP-ltr-12-6-19.pdf ACP-ltr-3-8-19.pdf

On behalf of the Association of Claims Professionals (ACP), we respectfully submit the attached comments to the modified proposed CCPA regulations, outlining one recommended adjustment to the regulations to provide greater consistency and clarity to the Act's application and to avoid consumer confusion over potential conflict with other California laws. The attached supplements and incorporates our preliminary rulemaking submission from December 6, 2019 and comments to the preliminarily proposed regulations from March 8, 2019.

Very truly yours,
Scott Ferber

Partner

T: [redacted] | M: [redacted] | E: [redacted] | www.kslaw.com

BIO | vCARD

King & Spalding LLP
1700 Pennsylvania Avenue, NW
Suite 200
Washington, D.C. 20006

KING & SPALDING

February 25, 2020

BY EMAIL

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

RE: **Proposed California Consumer Privacy Act Regulations**

Ladies and Gentlemen:

The Association of Claims Professionals (ACP) is pleased to respond to requests for comment on the modified proposed California Consumer Privacy Act (CCPA) regulations and writes to recommend one adjustment to the regulations to provide greater consistency and clarity to the Act's application and to avoid consumer confusion over potential conflict with other California laws. While ACP members are strong proponents of individual privacy rights, we remain concerned that the unintended application of the CCPA and the proposed regulations, as currently drafted, will sow confusion and discord among California consumers and result in conflicting regulatory standards for our members and the larger California business community writ large. Our proposed language is designed to avoid those consequences. This letter supplements and incorporates our preliminary rulemaking submission from December 6, 2019 and comments to the preliminarily proposed regulations from March 8, 2019 (attached for ease of reference).

ACP (formerly known as the American Association of Independent Claims Professionals or AAICP) was formed in 2002 as the only national association representing the interests of the nation's independent claims professionals. ACP members employ thousands of claims specialists and other professionals across the country and handle millions of property and casualty, workers' compensation, disability, and other liability claims annually. Membership is comprised of independent claims adjusters and third-party administrator organizations, many of whom handle claims administration responsibilities for California insureds and their carriers. ACP member companies employ thousands of adjusters in the State of California and manage billions of dollars of claims for California insurers and policyholders.

ACP companies respond every day to individuals and businesses who receive employee benefits or suffer a loss such as workplace injury, property or casualty damage, or liability. Insurance carriers and self-insured companies retain our member companies for expert advice and knowledge throughout the management of claims entrusted to their care. ACP companies provide a full range of claims services from claims adjusting to comprehensive claims management. ACP focuses on the importance of claims specialists as front line responders when an individual or business suffers a loss such as a workplace injury, property or casualty damage, or liability. For claimants, ACP companies help individuals and companies begin to recover from such a loss. For carriers and

self-insured customers, ACP companies are a strategic business partner and trusted advisor providing professional claims services integral to risk management. At each step of this process, important information is shared to facilitate effective and efficient claims management.

Given these important roles and responsibilities, and to ensure the most expedient claims management and administration, while avoiding consumer confusion and consternation, it is important that there be greater clarity on what is and is not covered by the CCPA. Based on the current language of the Act and proposed regulations, information collected as part of administering and managing employee benefits, workplace injury, property and casualty damage, and liability claims and benefits largely are exempted from the CCPA's provisions. See, e.g., Cal. Civ. Code §§1798.105(d),[i] 1798.140(t)(2)(A),[ii] 1798.140(t)(2)(C),[iii] 1798.145(a),[iv] 1798.145(b),[v] 1798.145(c)(1)(A),[vi] 1798.145(h)(1)(A),[vii] 1798.145(h)(1)(C),[viii] and 1798.145(n)(1);[ix] see also Modified Proposed CCPA Reg. § 999.313(c)(3).[x] To provide greater clarity and consistency with other laws, the proposed regulations should be revised to make it clear that the following information is exempted: W239-1

> This title shall not apply to any information collected, received, or shared for the purpose of administering or managing employee benefits or workplace injury, property and casualty damage, or liability claims or benefits.

This clarification, of course, makes good sense given that California has already specifically and comprehensively addressed transparency and privacy in the claims adjusting industry under the California Insurance Code, Labor Code, and health laws; the CCPA's preamble acknowledgement of existing law's providing protection in various other contexts; and the already existing exemptions in the CCPA itself, as noted above.

****

ACP appreciates the opportunity to provide comments on the proposed regulations. If you have any questions concerning our comments, or if we can be of further assistance, please contact Susan Murdock at [redacted]. We thank you for consideration of these comments and welcome any further questions you may have.

Sincerely,

w/e/p SRM

Susan R. Murdock
Executive Director
Association of Claims Professionals
1700 Pennsylvania Avenue, Suite 200
Washington, DC 20006
Phone: [redacted]
www.claimsprofession.org

[i] "A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal

information if it is necessary for the business or service provider to maintain the consumer's personal information in order to: (1) Complete the transaction for which the personal information was collected, … provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer. (2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity. (3) Debug to identify and repair errors that impair existing intended functionality. (4) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law… (7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business. (8) Comply with a legal obligation. (9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information."

[ii] "For purposes of this title, a business does not sell personal information when …: A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title."

[iii] "For purposes of this title, a business does not sell personal information when …: The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met: (i) The business has provided notice of 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."

[iv] "The obligations imposed on businesses by this title shall not restrict a business' ability to: (1) Comply with federal, state, or local laws. (2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities. (3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law. (4) Exercise or defend legal claims. (5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information. (6) Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California."

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

[vi] "This title shall not apply to … Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5)."

[vii] "This title shall not apply to … Personal information that is collected by a business about a natural person in the course of the natural person acting as … an employee of … that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a … an employee … of that business."

[viii] "This title shall not apply to … Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as … an employee of … that business to the extent that the personal information is collected and used solely within the context of administering those benefits."

[ix] "The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee … of a company … and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company…."

[x] "In responding to a request to know, a business is not required to search for personal information if all the following conditions are met: a. The business does not maintain the personal information in a searchable or reasonably accessible format; b. The business maintains the personal information solely for legal or compliance purposes; c. The business does not sell the personal information and does not use it for any commercial purpose; and d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above."

From:	Garrett Hohimer
To:	Privacy Regulations
Cc:	Tola Sobitan
Subject:	Alight Solutions LLC Comments to CCPA Modified Proposed Regulations - Submitted 2.25.2020
Date:	Tuesday, February 25, 2020 3:36:18 PM
Attachments:	Alight Solutions LLC Comments to CCPA Modified Proposed Regulations 2.25.2020.pdf

Dear Sir or Madam,

Attached are Alight Solutions LLC's Comments on the California Attorney General's modifications to the text of proposed 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) (Published January 10, 2020)

Garrett Hohimer
Assistant General Counsel &
Director, Government Relations

Alight Solutions
4 Overlook Point
Lincolnshire, IL 60069
O [redacted] | M [redacted]
alightsolutions.com

alight

February 25, 2020

Submitted electronically in reference to the matter identified below, via PrivacyRegulations@doj.ca.gov

Subject: Alight Solutions LLC's Comments on:

- **The California Attorney General's modifications to the text of proposed 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) (Published January 10, 2020)**

To Whom It May Concern:

Alight Solutions LLC ("Alight") is a leader in benefits, payroll and cloud solutions, supporting more than 3,250 clients, including 50% of the Fortune 500. On behalf of its clients, Alight serves 26 million people and their family members including more than 5.5 million defined benefit participants, nearly 5 million defined contribution participants, and over 11 million health and welfare plan participants.

We again appreciate the Attorney General's effort to provide detailed regulations related to the California Consumer Privacy Act of 2018 (CCPA), and the opportunity to submit comments on the proposed modifications to the initial, proposed regulations. We support the inclusion of definitions of "employment benefits" and "employment-related information" (Section 999.301(h) & (i), respectively) as well as the related changes at Section 999.305(e). We encourage the Attorney General to continue to acknowledge and approach employment-related information, including that involving employment benefits, with flexibility, and tailored guidance. Additionally, the Attorney General should continue the applicability of Section 999.305(e) by extending the "sunset" provision in Section 999.305(f) to the greatest degree possible to provide consistent, reliable guidance while the legislature considers any additional legislative action, as referenced therein. We furthermore support legislative action consistent with Section 999.305(f) to create additional flexibility and CCPA relief for employers and their employment benefit programs, which are generally heavily regulated already, including with regards to record keeping requirements and data privacy and security.

W240-1

W240-2

W240-3

Although the modifications provide certain changes to Section 999.314(a), it appears that the modified proposed regulation continues to stretch the applicability of the CCPA beyond its statutory definitions in contravention of California's Administrative Procedure Act ("APA"), CA Gov't Code Sec. 11340 *et seq.* For this reason we reiterate our comments of December 6, 2019, related to this provision. As proposed we expect that Section 999.314(a) could at minimum have unintended negative consequences on businesses, service providers, and consumers.

I. We urge the Attorney General to strike or clarify Section 999.314(a) related to service providers, which appears to significantly expand who is a covered service provider, create a direct conflict between service providers and any non-"business" client otherwise not covered by CCPA, and potentially subject such non-"business" clients to CCPA's requirements indirectly.

W240-4

The definition of "service provider" set forth in Section 1798.140(v) is a person or entity that processes "information on behalf of a **business**…." (emphasis added). Additionally, the term "business" is defined in Section 1798.140(c) to mean a for-profit entity that is covered by CCPA. As a result, an entity providing services to a company that is not a "business" will not be subject to CCPA's service provider requirements. Proposed regulation 999.314(a), however, does away with the "business" limitation in the express terms of the CCPA. As a result, entities not contemplated as "service providers" under the

CCPA statute itself may nonetheless be deemed "service providers" for purposes of the regulations. We expect many entities that, for example, provide services to not-for-profits (or state, municipal, or other governmental units), will not be prepared to meet the service provider requirements of CCPA and that there will be conflict and confusion about this expansion. Additionally, the APA, does not grant the AG the authority to enlarge the scope of the CCPA through regulation.

For entities that would not be service providers but for proposed regulation 999.314(a), or entities that are service providers, but have clients that are a mix of "business" and non-"business" companies, this provision will either create a conflict with the non-"business" client over the need to comply regarding such client's population, or effectively subject the non-"business" client to CCPA's requirements by virtue of the deemed service provider status.

For example, in the event an entity was servicing clients that were not-for-profit companies, those clients may assert that they are not subject to CCPA; which would be accurate under both the text of the CCPA as well as the proposed regulations. The service provider entity would be holding the data of the non-profit clients, but does not own that data and generally would not take independent action regarding that data. However, if the service provider entity were to be deemed a "service provider" under CCPA with regards to, in this example, non-profit clients, there may be a conflict between the responsibilities of a service provider under the CCPA and the direction provided by a non-profit client that is not subject to the CCPA. The service provider entity would be caught between its own responsibilities under the CCPA and the non-profit client's position that the CCPA does not apply to the client's data. If the client directed, for example, that the service provider not respond or take any action on requests related to personal data obtained from that client's employees, it is unclear how the service provider could assert that such action was required if the CCPA does not apply to the client who owns the data.

W240-4 (cont.)

In addition to the deemed service provider's conflicted position, a non-"business" client would be essentially forced to choose between voluntarily following the CCPA requirements despite it not applying or contending with the conflict and challenges described above.

For these reasons, we urge the AG to strike Section 999.314(a) from the proposed regulations and allow the statutory definitions of "business" and "service provider" to control. Although we believe this section should be struck and that failing to do so will have negative consequences, as an alternative, we suggest the AG, at minimum, clarify that when a service provider performs services for an entity that is not a "business" and to which the CCPA does not apply, the service provider may follow such entity's otherwise lawful direction deviating from the CCPA with regards to any action otherwise required under the CCPA.

* * * * *

Thank you for the opportunity to submit these comments on the proposed regulations. Alight would welcome the opportunity to meet and discuss our comments in greater detail or to answer any questions that you may have.

Respectfully submitted,
Alight Solutions LLC

M. Garrett Hohimer
Asst. General Counsel & Dir, Government Relations
[redacted]

Tola Sobitan
Chief Privacy Officer & Senior Counsel
[redacted]

From: Joseph W Guzzetta
To: Privacy Regulations
Subject: CCPA Draft Regulation Comments
Date: Tuesday, February 25, 2020 3:35:48 PM
Attachments: CCPA Proposed Regs Letter.pdf

Dear Attorney General Becerra,

Please find attached a letter containing comments on the proposed CCPA regulations that were released on February 10, 2020.

Very truly yours,

Joseph W. Guzzetta
[redacted]

February 25, 2020

VIA ELECTRONIC MAIL

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

Re: Proposed Amended California Consumer Privacy Act Regulations

Dear Attorney General Becerra,

I write as a private citizen to submit comments on the proposed regulations issued on February 14, 2020 by the Office of the Attorney General under the California Consumer Privacy Act of 2018 (the "CCPA") pursuant to the authority granted to him in California Civil Code Section 1798.185. I write to note a number of potential contradictions, ambiguities and typographical errors in the proposed regulations. Because it is critically important that CCPA regulations be as clear and understandable as possible, and I urge the Attorney General to further amend the proposed regulations before they become final.

Contradiction in Regulations Regarding Notices at Collection: First, under draft 11 CCR §999.305(a), notices at collection required under Civil Code §1798.100(b) are required only for "the categories of personal information ***to be collected from them***" (emphasis added). The regulation strongly suggests that "them" means "the consumer." In other words, notices at collection are only required for information collected ***from the consumer***. This makes perfect sense how could a business possibly provide a consumer notice at collection when the collection of personal information is from sources that are not the consumer him or herself?

But, draft 11 CCR §999.305(d) implies that a business that is registered as a data broker that does not include instructions on how a consumer may opt out of sales of his or her personal information in its data broker registration submission is required to provide a notice at collection even when the business "does not collect information directly from consumers." This makes no sense and contracts draft subsection (a). W241-1

Which is it? Are notices at collection required only in the case of collection of personal information ***from*** consumers? Are notices at collection required for any collection from any source (in which case, how could a business possibly provide consumers with notice at collection when they collect personal information about those consumers from third party sources?)? Or, are notices at collection only required ***of data brokers*** in the case of personal information collected from sources other than the consumer (provided the data broker did not include the required information in its submission to the Attorney General when registering as a data broker)? This is an apparent contradiction in the regulations that needs clarification.

Typographical errors: Second, there is a typographical error in draft 11 CCR §999.307(b)(2) "A description of the material terms of the financial incentive or price of service difference" should read "A description of the material terms of the financial incentive or price **or** service difference". In other words, change the second "of" in this sentence to an "or" to remain consistent with the remainder of the draft regulation. W241-2

Contradiction with statute: Third, draft 11 CCR §999.313(b) permits businesses to extend the 45 day period in which to respond to requests to know and requests to delete. The version of the CCPA enacted by the Legislature and approved by the Governor, however, directly contradicts this draft regulation. It is true that Cal. Civ. Code §1798.130(a)(2) allows businesses to take a 45 day extension of the initial 45 day time period in which to respond to verifiable consumer requests if the extension is "reasonably necessary." However, California Civil Code Section 1798.145(i)(1) provides that a business's obligation to "respond to and honor consumer rights requests" under the CCPA may be extended "by up to 90 ***additional*** days where necessary, taking into account the complexity and number of the requests" (emphasis added). In other words, the draft regulation in draft 11 CCR §999.313 directly contradicts the CCPA as enacted by the Legislature. W241-3

As you know, the Attorney General lacks the authority to amend a statutory deadline or extension, and if there is any contradiction between the terms of the CCPA, and the terms of the Attorney General's regulations, the statute must prevail. Accordingly, the Attorney General should amend the extension in draft 11 CCR §999.313 to 90 days (for a total of 135 days).

Lack of clarity regarding methods for submitting verifiable consumer requests: Finally, proposed 11 CCR §999.312(c) requires businesses that interact with consumers in person to "consider" certain methods for permitting consumers to submit verifiable consumer requests. What does the Attorney General mean by this proposed regulation? If a business considers, but decides against, those listed methods, will the business be safe from an enforcement action? Or will the Attorney General bring an enforcement action against a business that interacts with consumers in person that does not use one of the listed methods? The Attorney General should consider using a different, less ambiguous word than "consider" in proposed 11 CCR §999.312(c) in order to help businesses comply with the CCPA. W241-4

Thank you for considering these comments.

Very truly yours,

/s/

Joseph W. Guzzetta

From:	Mihir E. Kshirsagar
To:	Privacy Regulations
Subject:	Princeton CITP CCPA Comments
Date:	Tuesday, February 25, 2020 3:31:31 PM
Attachments:	Dark Patterns at Scale.pdf CITP Clinic CCPA Comments-2.pdf

Dear Ms. Kim,

I attach comments on the proposed CCPA regulations and an academic article we authored that is relevant to the Department's rulemaking.

Sincerely,
Mihir Kshirsagar

Mihir Kshirsagar
Center for Information Technology Policy
[redacted]y
[redacted]

PRINCETON UNIVERSITY

CENTER FOR INFORMATION TECHNOLOGY POLICY
PRINCETON UNIVERSITY

February 25, 2020

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

Comments on Revised Proposed Regulations
Implementing the California Consumer Privacy Act

Thank you for the opportunity to provide comments to the California Department of Justice on the February 10, 2020 revised proposed regulations implementing the California Consumer Privacy Act.

We are academic researchers associated with the Center for Information Technology Policy (CITP) at Princeton University, with expertise in computer science, law, and policy.[1] We write to offer three specific recommendations that advance the Department's goal of protecting consumer privacy. We look forward to further opportunities to engage with the Department to provide additional analysis as the CCPA regulations evolve.

1. **Consent notices should avoid using dark patterns that burden consumer decision making.**

Dark patterns are user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions. Mathur et al, Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites, Proc. ACM Hum. Comput. Interact. 3, CSCW, Article 81 (Nov. 2019) (attached). We have studied these user interface designs extensively. Recently, we published a study based on a crawl of over 11,000 shopping websites using automated techniques that detected a variety of dark patterns on over 10% of those sites that could

W242-1

[1] In keeping with Princeton's tradition of service, CITP's Technology Policy Clinic provides nonpartisan research, analysis, and commentary to policy makers, industry participants, journalists, and the public. These comments are a product of that Clinic and reflect the independent views of the undersigned scholars.

mislead or confuse consumers. *Id.* Various academic studies have also examined the use of dark patterns around obtaining consumer consent to information collection. *See* Nouwens et al, Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence, CHI '20 CHI Conference on Human Factors in Computing Systems; Jamie Luguri and Lior Strahilevitz, Shining a Light on Dark Patterns, U of Chicago, Public Law Working Paper No. 719. A recent academic study reported on the use of dark patterns in obfuscating the consent notices required by the European Union's General Data Protection Regulation (GDPR). Utz et al, (Un)informed Consent: Studying GDPR Consent Notices in the Field, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19); *see also* Norwegian Consumer Council, Deceived by Design (2018).[2]

W242-1 (cont.)

The Department's design of a standardized opt-out button in §999.306(f) helps bring consistency across different providers and improves the ability of consumers to make informed choices. But the proposed design has a flaw that risks impairing a consumer's decision making because the button presents consumers with a pre-selected double negative choice by using a red cross next to the phrase "do not sell." As a result, consumers might be confused about whether or not the site has the ability to sell their information. We suggest that the Department adopt the design recommended in the study by Cranor et al., Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA (Feb. 4, 2020), which includes a check and a cross in the design and presents the choices in a neutral blue color. (*Id.* at p.32, shown below.)

The best icon to pair with current CCPA taglines to convey a "do not sell" opt-out is a *toggle* icon. This combination effectively communicates the presence of a choice, particularly one related to the sale of personal information.

Do Not Sell My Personal Information

More generally, the Department could assess whether providers make it equally easy for users to select among the choice to opt in or opt out of information sharing. For example, Facebook's GDPR consent flow opt in takes 3 clicks, while the opt out takes 11 clicks. *See* Deceived by Design. This suggests that consumers may not be presented with a fair choice.

W242-2

[2] https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

A key finding from the research literature is that service providers use a variety of design elements, including color, placement, size and language to obscure choices that consumers are likely to select if fairly presented. As a result, we support the new language in §999.315(c) that responds to such concerns by prohibiting user interface designs that have "the purpose or substantial effect of subverting or impairing a consumer's decision to opt-out."

W242-2 (cont.)

The Department might consider developing a process to monitor how providers are presenting information choices after the CCPA regulations come into effect and provide additional guidance, as necessary, to prevent tactics that subvert or impair a consumer's decision making process. The Department could also provide more explicit guidance that explains how it will not simply evaluate business practices in a vacuum, but will examine how certain choices that enhance consumer privacy are presented relative to other options that may benefit the business.

2. The Department should clarify how the definitions of "personal information" and "sell" apply to common practices.

The Department's decision to provide additional guidance about how the CCPA applies to common practices helps clarify how the law will be interpreted. But we urge the Department to reconsider its analysis of Internet Protocol (IP) addresses and to offer guidance on cookies and similar tracking technologies.

a. Internet Protocol addresses are "personal information."

W242-3

In the revised proposed regulations, the Department offers the following guidance on IP addresses: "For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be 'personal information.'" This guidance is problematic for several reasons.

First, IP addresses are used for identification. The purpose of an IP address is to route data to a particular user device or household. IP addresses can be—and often are—used as identifiers for linking individual-level or household-level information over time and across online services. Indeed, with the latest version of IP (IPv6) there may be additional information embedded in the address such as a device (MAC) address. Thus, IP addresses enable user or household tracking and singling out a user or device for contact, and may inherently contain some identifiable information.

Furthermore, associating an IP address with other forms of "personal information" is often technically trivial. Information that matches an IP address with an individual or a precise location is often publicly available on the internet, and commercial services offer precise IP address geolocation. Moreover, there are a number of businesses that possess a reliable mapping between individual user identities and IP addresses, including services that users log into, many third-party tracking and analytics services, and internet service providers. And even in a circumstance where an association between a user or household and an IP address is not already readily available, it is technically trivial to create that association by just sending an email to the user that includes invisible tracking content or induces the user to click a link. *See* Steven Englehardt, Jeffrey Han, and Arvind Narayanan, I never signed up for this! Privacy implications of email tracking, Proceedings on Privacy Enhancing Technologies; 2018 (1):109–126.

Second, the CCPA's statutory language recognizes that IP addresses are an example of "personal information." § 1798.140(o)(1) begins with setting forth the criteria for what constitutes personal information. The next subsection (o)(1)(A) identifies specific examples of identifiers that unambiguously constitute personal information, including "real name," "social security number," and "internet protocol address." That definition concludes with a catchall to capture "other similar identifiers" that satisfy the same criteria. Thus, there is no reason for treating an IP address any differently from identifiers such as a person's name or social security number.

W242-3 (cont.)

Third, other regulatory agencies have concluded that IP addresses are indeed personal information. For example, the Federal Communications Commission concluded in a 2016 rulemaking that IP addresses were "personally identifiable information." The FCC explained:

> We disagree with commenters that argue that we should not consider MAC addresses, IP addresses, or device identifiers to be [personally identifiable information (PII)]. First, as discussed above, a customer's IP address and MAC address each identify a discrete customer and/or customer device by routing communications to a specific endpoint linked to the customer. Information does not need to reveal an individual's name to be linked or reasonably linkable to that person. A unique number designating a discrete individual—such as a Social Security number or persistent identifier—is at least as specific as a name. Second, MAC addresses, IP addresses, and other examples of PII do not need to be able

> to identify an individual in a vacuum to be linked or reasonably linkable. [Broadband internet access service (BIAS)] providers can combine this information with other information to identify an individual (e.g., the BIAS provider's records of which IP addresses were assigned to which customers, or traffic statistics linking MAC addresses with other data). As the Supreme Court has observed, "[w]hat may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context."[3]

The FCC offered this guidance when elaborating on a "reasonably linkable" standard, nearly identical to the standard in the CCPA. We see no reason for the Department to reach a different technical conclusion about networking technology than that reached by the federal telecommunications regulatory agency.

Regulators in the European Union have similarly concluded that IP addresses should be treated as personal information because they are reasonably linkable to individuals or households. In *Breyer v Bundesrepublik Deutschland* (2016), the Court of Justice of the European Union ("CJEU") explained that "a dynamic IP address registered by an online media services provider . . . constitutes personal data within the meaning of that provision . . . where the latter **has the legal means** which enable it to identify the data subject with additional data which the internet service provider has about that person." (Emphasis added.)

W242-3 (cont.)

Fourth, the proposed guidance about the circumstances when IP address data can be linked to particular consumers or households could be read to only consider the data collected and maintained by a business. But the text of the CCPA does not contain either of these limitations; it provides an *objective* linkability standard, alternately phrased as "reasonably capable of being associated with" and "reasonably linked." We urge the Department to redraft the guidance to clarify that the linkability analysis is not simply confined to a business's own practices and data holdings and that information from third parties that could be obtained to identify consumers or households is relevant to the analysis.

Fifth, there is a practical concern that if the Department offers ambiguous guidance about when and how IP addresses are "personal information," that will detract from a predictable and uniform application of the law. Businesses of course

[3] https://www.fcc.gov/document/fcc-releases-rules-protect-broadband-consumer-privacy.

have significant commercial incentives to take the position that IP addresses are not subject to CCPA's privacy protections. Offering clarity on IP addresses now avoids foreseeable policy disputes in future about the circumstances when IP addresses are treated as personal information.

W242-3 (cont.)

b. Third-party consumer tracking using cookies and similar technologies constitutes a "sale" of "personal information."

We recommend that the Department offer guidance on how CCPA applies to third-party consumer tracking using cookies and similar technologies (e.g., "supercookies" and "fingerprinting"), a pervasive business practice on the web and in mobile applications. *See e.g.*, Jonathan R. Mayer and John C. Mitchell, Third-Party Web Tracking: Policy and Technology;[4] Steven Englehardt and Arvind Narayanan, Online Tracking: A 1-million-site Measurement and Analysis, ACM CCS 2016.[5]

W242-4

Like with the analysis of IP addresses, a tracking technology like cookies involves "personal information" because the data "is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

Tracking technologies that operate across online services also constitute a "sale" of personal information because such technologies are placed on sites in exchange for value. For example, when a third-party service collects consumer tracking information, it typically does so via content embedded in another business's site and offers an incentive for that business to host the tracking content. In other words, third-party tracking inherently involves personal information "[made] available . . . by [a] business to another business or a third party for monetary or other valuable consideration."

We recommend the Department offer guidance on the use of such technologies in the next round of proposed rulemaking.

3. If a consumer maintains a password-protected account with a business, logging into the account should be necessary and presumptively sufficient for verifying a consumer request.

W242-5

[4] Available at https://jonathanmayer.org/publications/trackingsurvey12.pdf
[5] Available at https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf

Recent research has highlighted security risks associated with GDPR data request processes, because businesses are implementing new processes for customer authentication rather than using existing processes that have been vetted extensively. *See* Martino et al, Personal Information Leakage by Abusing the GDPR Right of Access.[6] These studies raise a concern for how businesses will respond to the access rights under the CCPA. The problem is that the new authentication methods add a whole class of newly recognized security risks, where attackers can circumvent established authentication protections by using weaker GDPR request processes.

We recommend that the Department specify that, if a consumer maintains a password-protected account with a business, logging into the account is a necessary step for verifying a consumer request. This is a technically simple precaution for businesses to implement, including in coordination with a third-party identity verification service. This step is also trivial for consumers—just one simple login to an existing account. Adding this step avoids creating new and often insecure authentication methods. It also reduces the risk of data leaks in which businesses respond to requests with extraneous data that does not pertain to the consumer making the request. *See* James Pavur and Casey Knerr. GDPArrrrr: Using Privacy Laws to Steal Identities. Black Hat USA 2019. W242-5 (cont.)

We also recommend that the Department specify that logging into a password-protected account is presumptively sufficient for verifying a consumer request. In many contexts, a user already has full access to and control over their data after logging into an account and there is no need to add unnecessary friction for consumers seeking to exercise their CCPA rights.

We acknowledge that there are circumstances where additional authentication beyond a login is appropriate, especially when the CCPA gives the end user access to more data than they would have in the ordinary course. We recommend setting a presumption that businesses can overcome in appropriate contexts (e.g., considering the factors that the Department proposes to articulate in § 999.323).

* * *

We appreciate the opportunity to participate in the rulemaking process and remain available to answer any questions the staff may have.

Respectfully submitted,

[6] https://www.usenix.org/conference/soups2019/presentation/dimartino

Marshini Chetty
Assistant Professor, Department of Computer Science, University of Chicago

Shaanan Cohney
Postdoctoral Research Associate, Center for Information Technology Policy, Princeton University

Mihir Kshirsagar*
Technology Policy Clinic Lead, Center for Information Technology Policy, Princeton University

Arunesh Mathur
Graduate Student, Department of Computer Science, Princeton University

Jonathan Mayer*
Assistant Professor of Computer Science and Public Affairs, Princeton University

Arvind Narayanan
Associate Professor of Computer Science, Princeton University

Ross Teixeira
Graduate Student, Department of Computer Science, Princeton University

Ari Ezra Waldman
Microsoft Visiting Professor of Information Technology Policy, Princeton University

* denotes principal comment authors.

Contact:

Website: https://citp.princeton.edu
Phone: [redacted]
Email: [redacted]

Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites

ARUNESH MATHUR, Princeton University, USA
GUNES ACAR, Princeton University, USA
MICHAEL J. FRIEDMAN, Princeton University, USA
ELENA LUCHERINI, Princeton University, USA
JONATHAN MAYER, Princeton University, USA
MARSHINI CHETTY, University of Chicago, USA
ARVIND NARAYANAN, Princeton University, USA

Dark patterns are user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions. We present automated techniques that enable experts to identify dark patterns on a large set of websites. Using these techniques, we study shopping websites, which often use dark patterns to influence users into making more purchases or disclosing more information than they would otherwise. Analyzing ~53K product pages from ~11K shopping websites, we discover 1,818 dark pattern instances, together representing 15 types and 7 broader categories. We examine these dark patterns for deceptive practices, and find 183 websites that engage in such practices. We also uncover 22 third-party entities that offer dark patterns as a turnkey solution. Finally, we develop a taxonomy of dark pattern characteristics that describes the underlying influence of the dark patterns and their potential harm on user decision-making. Based on our findings, we make recommendations for stakeholders including researchers and regulators to study, mitigate, and minimize the use of these patterns.

CCS Concepts: • **Human-centered computing** → **Empirical studies in HCI**; *HCI theory, concepts and models*; • **Social and professional topics** → **Consumer products policy**; • **Information systems** → *Browsers.*

Additional Key Words and Phrases: Dark Patterns; Consumer Protection; Deceptive Content; Nudging; Manipulation

ACM Reference Format:
Arunesh Mathur, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 81 (November 2019), 32 pages. https://doi.org/10.1145/3359183

Authors' addresses: Arunesh Mathur, Princeton University, 304 Sherrerd Hall, Princeton, NJ, 08544, USA, amathur@cs.princeton.edu; Gunes Acar, Princeton University, 320 Sherrerd Hall, Princeton, NJ, 08544, USA, gunes@princeton.edu; Michael J. Friedman, Princeton University, 35 Olden Street, Princeton, NJ, 08544, USA, mjf4@princeton.edu; Elena Lucherini, Princeton University, 312 Sherrerd Hall, Princeton, NJ, 08544, USA, elucherini@cs.princeton.edu; Jonathan Mayer, Princeton University, 307 Sherrerd Hall, Princeton, NJ, 08544, USA, jonathan.mayer@princeton.edu; Marshini Chetty, University of Chicago, 355 John Crerar Library, Chicago, IL, 60637, USA, marshini@uchicago.edu; Arvind Narayanan, Princeton University, 308 Sherrerd Hall, Princeton, NJ, 08544, USA, arvindn@cs.princeton.edu.

2573-0142/2019/11-ART81 $15.00
https://doi.org/10.1145/3359183

1 INTRODUCTION

Dark patterns [32, 48] are user interface design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make. Such interface design is an increasingly common occurrence on digital platforms including social media websites [46], shopping websites [32], mobile apps [5, 31], and video games [85]. At best, dark patterns annoy and frustrate users. At worst, they can mislead and deceive users, e.g., by causing financial loss [1, 2], tricking users into giving up vast amounts of personal data [46], or inducing compulsive and addictive behavior in adults [74] and children [21].

While prior work [31, 32, 38, 48] has provided taxonomies to describe the existing types of dark patterns, there is no large-scale evidence documenting their prevalence, or a systematic and descriptive investigation of how the different types of dark patterns harm users. Collecting this information would allow us to first examine where, how often, and the technical means by which dark patterns appear; second, it would allow us to compare and contrast how various dark patterns influence users. In doing so, we can develop countermeasures against dark patterns to both inform users and protect them from such patterns. Further, given that many of these patterns are potentially unlawful, we can also aid regulatory agencies in addressing and mitigating their use.

In this paper, we present an automated approach that enables experts to identify dark patterns at scale on the web. Our approach relies on (1) a web crawler, built on top of OpenWPM [25, 40]—a web privacy measurement platform—to simulate a user browsing experience and identify user interface elements; (2) text clustering to extract all user interface designs from the resulting data; and (3) inspecting the resulting clusters for instances of dark patterns. We also develop a taxonomy so that researchers can share descriptive and comparative terminology to explain how dark patterns subvert user decision-making and lead to harm. We base this taxonomy on the characteristics of dark patterns as well as the cognitive biases they exploit in users.

While our automated approach generalizes, we focus this study on shopping websites, which are used by an overwhelming majority of people worldwide [41]. Dark patterns found on these websites trick users into signing up for recurring subscriptions and making unwanted purchases, resulting in concrete financial loss. We use our web crawler to visit the ~11K most popular shopping websites worldwide, create a large data set of dark patterns, and document their prevalence. Our data set contains several new instances and variations of previously documented dark patterns [32, 48]. Finally, we use our taxonomy of dark pattern characteristics to classify and describe the patterns we discover. We have five main findings:

- We discovered 1,818 instances of dark patterns on shopping websites, which together represent 15 types of dark patterns and 7 broad categories.
- These 1,818 dark patterns were found on 1,254 of the ~11K shopping websites (~11.1%) in our data set. Shopping websites that were more popular, according to Alexa rankings [9], were more likely to feature dark patterns. These numbers represent a lower bound on the total number of dark patterns on these websites, since our automated approach only examined text-based user interfaces on a sample of product pages per website.
- In using our taxonomy to classify the dark patterns in our data set, we discovered that the majority are *covert*, *deceptive*, and *information hiding* in nature. Further, many patterns exploit cognitive biases, such as the default and framing effects. These characteristics and biases collectively describe the consumer psychology underpinnings of the dark patterns we identified.
- We uncovered 234 instances of dark patterns—across 183 websites—that exhibit deceptive behavior. We highlight the types of dark patterns we encountered that rely on deception.

- We identified 22 third-party entities that provide shopping websites with the ability to create and implement dark patterns on their sites. Two of these entities openly advertised practices that enable deceptive messages.

Through this study, we make the following contributions:

- We contribute automated measurement techniques that enable expert analysts to discover new or revisit existing instances of dark patterns on the web. As part of this contribution, we make our web crawler and associated technical artifacts available on GitHub[1]. These can be used to conduct longitudinal measurements on shopping websites or be re-purposed for use on other types of websites (e.g., travel and ticket booking websites).
- We create a data set and measure the prevalence of dark patterns on 11K shopping websites. We make this data set of dark patterns and our automated techniques publicly available[2] to help researchers, journalists, and regulators raise awareness of dark patterns [21], and to help develop user-facing tools to combat these patterns.
- We contribute a novel descriptive taxonomy that provides precise terminology to characterize how each dark pattern works. This taxonomy can aid researchers and regulators to better understand and compare the underlying influence and harmful effects of dark patterns.
- We document the third-party entities that enable dark patterns on websites. This list of third parties can be used by existing tracker and ad-blocking extensions (e.g., Ghostery,[3] Adblock Plus[4]) to limit their use on websites.

2 RELATED WORK

2.1 Online Shopping and Influencing User Behavior

Starting with Hanson and Kysar, numerous scholars have examined how companies abuse users' cognitive limitations and biases for profit, a practice they call market manipulation [50]. For instance, studies have shown that users make different decisions from the same information based on how it is framed [80, 81], giving readily accessible information greater weight [79], and becoming susceptible to impulsively changing their decision the longer the reward from their decision is delayed [28]. Some argue that because users are not always capable of acting in their own best interests, some forms of 'paternalism'—a term referring to the regulation or curation of the user's options—may be acceptable [78]. However, determining the kinds of curation that are acceptable is less straightforward, particularly without documenting the practices that already exist.

More recently, Calo has argued that market manipulation is exacerbated by digital marketplaces since they posses capabilities that increase the chance of user harm culminating in financial loss, loss of privacy, and the ability to make independent decisions [34]. For example, unlike brick-and-mortar stores, digital marketplaces can capture and retain user behavior information, design and mediate user interaction, and proactively reach out to users. Other studies have suggested that certain elements in shopping websites can influence impulse buying behavior [60, 86]. For instance, perceived scarcity, social influence (e.g., 'social proof'—informing users of others' behavior—and shopping with others [33, 61]) can all lead to higher spending. More recently, Moser et al. conducted a study [65] to measure the prevalence of elements that encourage impulse buying. They identified 64 such elements—e.g., product reviews/ratings, discounts, and quick add-to cart buttons—by manually scraping 200 shopping websites.

[1]https://github.com/aruneshmathur/dark-patterns
[2]https://webtransparency.cs.princeton.edu/dark-patterns
[3]https://ghostery.com
[4]https://adblockplus.com

2.2 Dark Patterns in User Interface Design

Coined by Brignull in 2010, dark patterns is a catch-all term for how user interface design can be used to adversely influence users and their decision-making abilities. Brignull described dark patterns as 'tricks used in websites and apps that make you buy or sign up for things that you didn't mean to', and he created a taxonomy of dark patterns using examples from shopping and travel websites to help raise user awareness. The taxonomy documented patterns such as 'Bait and Switch' (the user sets out to do one thing, but a different, undesirable thing happens instead), and 'Confirmshaming' (using shame tactics to steer the user into making a choice).

2.2.1 Dark Pattern Taxonomies. A growing number of studies have expanded on Brignull's original taxonomy more systematically to advance our understanding of dark patterns. Conti and Sobiesk [38] were the first to create a taxonomy of malicious interface design techniques, which they defined as interfaces that manipulate, exploit, or attack users. While their taxonomy contains no examples and details on how the authors created the taxonomy are limited, it contains several categories that overlap with Brignull's dark patterns, including 'Confusion' (asking the user questions or providing information that they do not understand) and 'Obfuscation' (hiding desired information and interface elements). More recently, Bösch et al. [31] presented a similar, alternative breakdown of privacy-specific dark patterns as 'Dark Strategies', uncovering new patterns: 'Forced Registration' (requiring account registration to access some functionality) and 'Hidden Legalese Stipulations' (hiding malicious information in lengthy terms and conditions). Finally, Gray et al. [48] presented a broader categorization of Brignull's taxonomy and collapsed many patterns into categories such as 'Nagging' (repeatedly making the same request to the user) and 'Obstruction' (preventing the user from accessing functionality).

While these taxonomies have focused on the web, researchers have also begun to examine dark patterns in specific application domains. For instance, Lewis [57] analyzed design patterns in the context of web and mobile applications and games, and codified those patterns that have been successful in making apps 'irresistible', such as 'Pay To Skip' (in-app purchases that skip levels of a game). In another instance, Greenberg et al. [49] analyzed dark patterns and 'antipatterns'—interface designs with unintentional side-effects on user behavior—that leverage users' spatial relationship with digital devices. They introduced patterns such as 'Captive Audience' (inserting unrelated activities such as an advertisement during users' daily activities) and 'Attention Grabber' (visual effects that compete for users' attention). Finally, Mathur et al. [63] discovered that most affiliate marketing on social media platforms such as YouTube and Pinterest is not disclosed to users (the 'Disguised Ads' dark pattern).

2.2.2 Dark Patterns and User Decision-making. A growing body of work has drawn connections between dark patterns and various theories of human decision-making in an attempt to explain how dark patterns work and cause harm to users. Xiao and Benbasat [84] proposed a theoretical model for how users are affected by deceptive marketing practices in online shopping, including affective mechanisms (psychological or emotional motivations) and cognitive mechanisms (perceptions about a product). In another instance, Bösch et al. [31] used Kahneman's Dual process theory [79] which describes how humans have two modes of thinking—'System 1' (unconscious, automatic, possibly less rational) and 'System 2' (conscious, rational)—and noted how 'Dark Strategies' exploit users' System 1 thinking to get them to make a decision desired by the designer. Lastly, Lewis [57] linked each of the dark patterns described in his book to Reiss's Desires, a popular theory of psychological motivators [72]. Finally, a recent study by the Norwegian Consumer Council (Frobrukerrådet) [46] examined how interface designs on Google, Facebook, and Windows 10 make

it hard for users to exercise privacy-friendly options. The study highlighted the default options and framing statements that enable such dark patterns.

2.3 Comparison to Prior Work

Our study differs from prior work in two ways. First, while prior work has largely focused on creating taxonomies of the types of dark patterns either based on anecdotal data [31, 32] or data collected from users' submissions [38, 48], we provide large-scale evidence documenting the presence and prevalence of dark patterns in the wild. Automated measurements of this kind have proven useful in discovering various privacy and security issues on the web—including third-party tracking [25, 40] and detecting vulnerabilities of remote third-party JavaScript libraries [68]—by documenting how and on which websites these issues manifest, thus enabling practical solutions to counter them. Second, we expand on the insight offered by prior work about how dark patterns affect users. We develop a comprehensive taxonomy of dark pattern characteristics (Section 3) that concretely explains the underlying influence and harmful effects of each dark pattern.

Finally, while prior work has shed light on impulse buying on shopping websites, the focus of our work is on dark patterns. While there is some overlap between certain types of dark patterns and impulse buying features of shopping websites [65], the majority of impulse buying elements are not dark patterns. For instance, offering returns and exchanges for products, or showing multiple images of a product [65] do not constitute dark patterns: even though they play a role in persuading users into purchasing products, they do not fundamentally subvert user decision-making in a manner that benefits shopping websites and retailers.

3 A TAXONOMY OF DARK PATTERN CHARACTERISTICS

Our taxonomy explains how dark patterns affects user decision-making based on their characteristics as well as the cognitive biases in users—deviations from rational behavior justified by some 'biased' line of reasoning [51]—they exploit to their advantage. We ground this taxonomy in the literature on online manipulation [34, 77, 83] and by studying the types of dark patterns highlighted in previous work [32, 48]. Our taxonomy consists of the following five dimensions:

- **Asymmetric**: Does the user interface design impose unequal weights or burdens on the available choices presented to the user in the interface?[5] For instance, a website may present a prominent button to accept cookies on the web but make the opt-out button less visible, or even hide it in another page.
- **Covert**: Is the effect of the user interface design choice hidden from users? That is, does the interface design to steer users into making specific purchases without their knowledge? For instance, a website may leverage the decoy effect [52] cognitive bias, in which an additional choice—the decoy—is introduced to make certain other choices seem more appealing. Users may fail to recognize the decoy's presence is merely to influence their decision making, making its effect covert.
- **Deceptive**: Does the user interface design induce false beliefs either through affirmative misstatements, misleading statements, or omissions? For instance, a website may offer a discount to users that appears to be limited-time, but actually repeats when the user refreshes the website's page. Users may be aware that the website is trying to offer them a discount; however, they may not realize that they do not have a limited time to take advantage of the deal. This false belief affects users' decision-making i.e., they may act differently if they knew that the sale is recurring.

[5]We narrow the scope of asymmetry to only refer to explicit choices in the interface.

- **Hides Information**: Does the user interface obscure or delay the presentation of necessary information to the user? For instance, a website may not disclose additional charges for a product to the user until the very end of their checkout.
- **Restrictive**: Does the user interface restrict the set of choices available to users? For instance, a website may only allow users to sign up for an account with existing social media accounts so they can gather more information about them.

Many types of dark patterns operate by exploiting cognitive biases in users. In Section 5, we draw an explicit connection between each type of dark pattern we encounter and the cognitive biases it exploits. The biases we refer to in our findings are:

(1) Anchoring Effect [79]: The tendency of individuals to overly rely on an initial piece of information—the 'anchor'—in future decisions.
(2) Bandwagon Effect [75]: The tendency of individuals to value something more because others seem to value it.
(3) Default Effect [54]: The tendency of individuals to stick with options that are assigned to them by default due to inertia.
(4) Framing Effect [80]: The tendency of individuals to reach different decisions from the same information depending on how it is presented.
(5) Scarcity Bias [64]: The tendency of individuals to place a higher value on things that are scarce.
(6) Sunk Cost Fallacy [29]: The tendency of individuals to continue an action if they have invested resources into it, even if that action might make them worse off.

4 METHOD

Dark patterns may manifest in several different locations inside websites, and they can rely heavily upon interface manipulation, such as changing the hierarchy of interface elements or prioritizing certain options over others using different colors. However, many dark patterns are often present on users' *primary interaction paths* in an online service or website (e.g., when purchasing a product on a shopping website, or when a game is paused after a level is completed). Further, multiple instances of a type of dark pattern share common traits such as the text they display (e.g., in the 'Confirmshaming' dark pattern—which tries to shame the user into making a particular choice—many messages begin with *No thanks*). Our technique relies on automating the primary interaction path of websites, extracting textual interface elements present in this path, and finally, grouping and organizing these—using clustering—for an expert analyst to sift through.

While our method generalizes to different types of websites, we focus on shopping websites in this study. We designed a web crawler capable of navigating users' primary interaction path on shopping websites: making a product purchase. Our crawler aligned closely with how an ordinary user would browse and make purchases on shopping websites: discover pages containing products on a website, add these products to the cart, and check out. We describe these steps, and the data we collected during each visit to a website below. Figure 1 illustrates an overview of our method.

We note that only analyzing textual information in this manner restricts the set of dark patterns we can discover, making our findings a lower bound on the dark patterns employed by shopping websites. We leave detecting other kinds of dark patterns—those that are enabled using style, color, and other non-textual features—to future work, and we discuss possible approaches in Section 6.

4.1 Creating a Corpus of Shopping Websites

We used the following criteria to evaluate existing lists of popular shopping websites, and, eventually, construct our own: (1) the list must be representative of the most popular shopping websites globally,

and (2) the list must consist of shopping websites in English so that we would have the means to analyze the data collected from the websites.

We retrieved a list of popular websites worldwide from Alexa using the Top Sites API [9]. Alexa is a web traffic analysis company that ranks and categorizes websites based on statistics it collects from users of its toolbar. We used the Top Sites list because it is more stable and is based on monthly traffic and not daily rank, which fluctuates often [73] The list contained 361,102 websites in total, ordered by popularity rank.[6]

We evaluated two website classification services to extract shopping websites from this list of the most popular websites: Alexa Web Information Service [10] and WebShrinker [23]. We evaluated the classification accuracy of these services using a random sample of 500 websites from our list of 361K websites, which we manually labeled as 'shopping' or 'not shopping'. We considered a website to be a shopping website if it was offering a product for purchase. Of the 500 websites in our sample, we labeled 57 as 'shopping' and 443 as 'not shopping'. We then evaluated the performance of both classifiers against this ground truth.

Table 3 in the Appendix summarizes the classifiers' results. Compared to Webshrinker, Alexa's classifications performed poorly on our sample of websites (classification accuracy: 89% vs. 94%), with a strikingly high false negative rate (93% vs. 18%). Although Webshrinker had a slightly higher false positive rate (0.2% vs. 0.4%), we used methods to determine and remove these false positives as we describe in Section 4.2.1.

We subsequently used Webshrinker to classify our list of 361K websites, obtaining a list of 46,569 shopping websites. To filter out non-English websites, we downloaded home pages of each site using Selenium [8] and ran language detection on texts extracted from the pages using the `polyglot` Python library [4]. Our final data set contained 19,455 English language shopping websites. We created this filtered list in August 2018.

4.2 Data Collection with a Website Crawl

We conducted all our crawls from the Princeton University campus using two off-the-shelf computers, both equipped with 16G of memory and quad-core CPUs. Our crawler's exploration of each shopping website mimicked a typical user's primary interaction path on a shopping website—starting with one of its product pages. Therefore, the first step in our website crawl was to determine ways to automatically identify product URLs from shopping websites.

4.2.1 Discovering Product URLs on Shopping Websites. To effectively extract product URLs from shopping websites, we iteratively designed and built a Selenium-based web crawler that contained a classifier capable of distinguishing product URLs from non-product URLs.

At first, we build a naïve depth-first crawler that, upon visiting a website's home page, determined the various URLs on the page, selected one URL at random, and then repeated this process from the selected URL. Using this crawler, we assembled a data set of several thousand URLs from visiting a random sample of 100 websites from our data set of 19K shopping websites. We manually labeled a sample of these URLs either as 'product' or 'non-product' URLs, and created a balanced data set containing 714 labeled URLs in total.

We trained a Logistic Regression classifier on this data set of labeled URLs using the `SGDClassifier` class from scikit-learn [71]. We extracted several relevant features from this data set of URLs, including the length of a URL, the length of its path, the number of forward slashes and hyphens in

[6]We did not use Alexa's list of Top/Shopping websites [22] because of two issues. First, its criteria of categorization are not fully disclosed. Second, most of the websites in the list had an average monthly rank > 500,000, which we did not consider to be representative of the most popular websites worldwide.

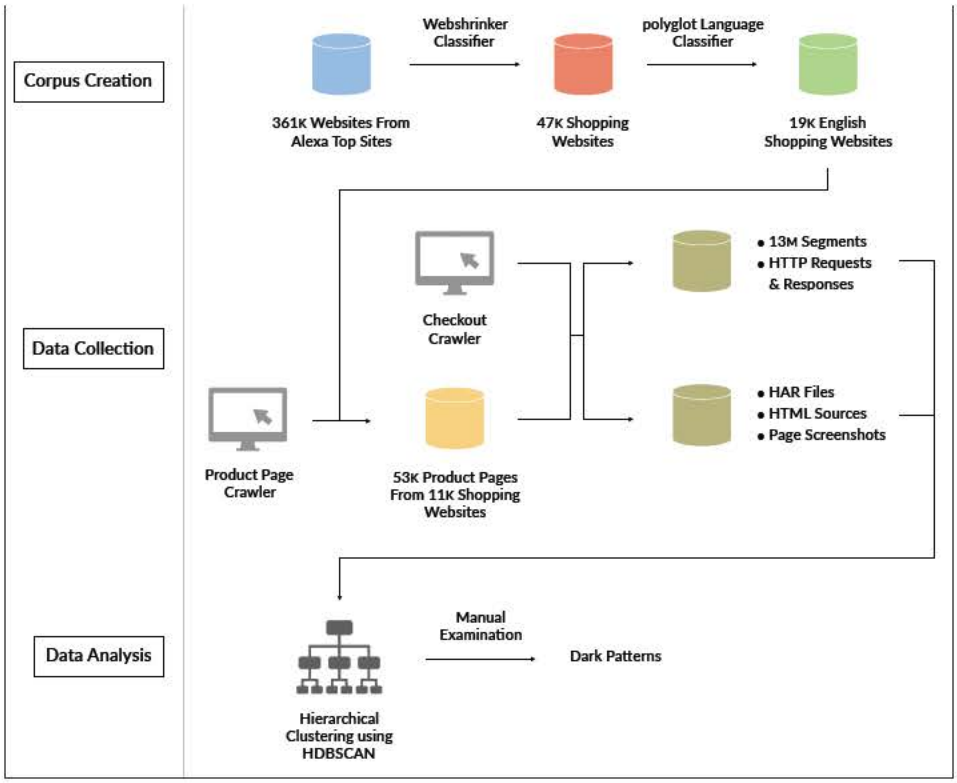


Fig. 1. Overview of the shopping website corpus creation, data collection using crawling, and data analysis using hierarchical clustering stages.

its path, and whether its path contained the words 'product' or 'category'. We used 90% of the URLs for training and obtained an 83% average classification accuracy using five-fold cross validation.

We embedded this classifier into our original Selenium-based web crawler to help guide its crawl. As a result, rather than selecting and visiting URLs at random, the crawler first used the classifier to rank the URLs on a page by likelihood of being product URLs, and then visited the URL with the highest likelihood. The crawler declared a URL as product if its page contained an 'Add to cart' or similar button. We detected this button by assigning a weighted score to visible HTML elements on a page based on their size, color, and whether they matched certain regular expressions (e.g., 'Add to bag|cart|tote|…'). This check also helped us weed out any false positives that may have resulted from the classification of shopping websites using Webshrinker (Section 4.1).

We tuned the crawler's search process to keep its crawl tractable. The crawler returned to the home page after flagging a product URL. It did not visit a given URL more than two times to avoid exploring the same URLs, and it stopped after visiting 100 URLs or spending 15 minutes on a site. We determined these termination limits by running test crawls on random samples of shopping websites. Finally, we opted to extract no more than five product pages from each shopping website.

To evaluate our crawler's performance, we randomly sampled 100 shopping websites from our corpus of 19K shopping websites and examined the product URLs the crawler returned for each of these websites. For 86 of those 100 websites, our crawler successfully extracted and returned legitimate product pages where they were present, and it returned no product pages where there

were not any. For the remaining 14 websites, the crawler either timed out because the website was no longer reachable, the website included a step that the crawler could not handle (e.g., the website required selecting a country of origin), or the 'Add to cart' button was incorrectly detected. We then used the crawler on all of the 19K shopping websites, and in total we gathered 53,180 product pages from 11,286 shopping websites.

4.2.2 Simulating Product Purchase Flows. To simulate a user's typical shopping flow—which included selecting certain product options (e.g., size or color), adding the product to the cart, viewing the cart, and checking out—we designed and built an interactive 'checkout crawler'.

We based our checkout crawler on OpenWPM, a fully instrumented browser platform that is designed to conduct large-scale privacy and web-tracking measurement studies [40]. We extended OpenWPM in a number of ways to interact with the product pages we collected previously, including identifying various interface elements using scoring functions similar to the ones we described in Section 4.2. Each of these functions would output the most likely 'Add to cart' buttons, 'View cart' buttons, and 'Checkout' buttons, which the crawler would click in–order across multiple pages. Because websites do not follow uniform HTML markup and design, our crawler needed to account for a variety of design alternatives and edge cases to simulate user interaction, such as dismissing popup dialogs, and identifying and interacting with product options (e.g., selecting a size and color for a t-shirt) to add a product to cart.

We collected three types of data during this crawl for each product page. First, we saved the page source on visit. Second, we took screenshots each time the state of the page changed (e.g., clicking a button or selecting a product option). Third, we extended OpenWPM's HTTP instrumentation to store HTTP Archive (HAR) [13]) files for each crawled page since HAR files are not limited to HTTP headers and contain full response contents that can be used for further analysis.

To evaluate our crawler's performance, we randomly sampled 100 product pages from the crawl in Section 4.2.1 and examined whether our crawler was able to simulate a user's shopping flow. In 66 of the 100 pages, our crawler reached the checkout page successfully. In 14 of the remaining 34, the crawler was able to add the product to cart but it was unable to proceed to the cart page; most often this was the result of complex product interaction (e.g., selecting the dimensions of a rug), which our crawler was not designed to perform. In the remaining 20 cases, either we produced Selenium exceptions, or failed to discover cart and checkout buttons. We then used the crawler on all of the 53K product pages. We divided the 53K product URLs into two equal-length lists to reduce the total crawling time. These crawls took approximately 90 hours to complete.

4.2.3 Capturing Meaningful Text Using Page Segmentation. The checkout crawler divided all the pages it visited into meaningful page segments to help discover dark patterns. These segments can be thought of as 'building blocks' of web pages, representing meaningful smaller sections of a web page. These formed the basic units for our data analysis and clustering.

We defined segments as *visible* HTML elements that contained no other block-level elements [6] and contained at least one text element—that is, elements of type `TEXT_NODE` [19]. However, since websites may use a virtually endless variety of markup and designs, we iteratively developed our segmentation algorithm, testing it on samples of shopping websites and accounting for possible edge cases. Algorithm 1 and Figure 11 in the Appendix detail the segmentation algorithm and illustrate its output for one web page, respectively.

Before segmenting each web page, the crawler waited for the page to load completely, also accounting for the time needed for popup dialogs to appear. However, web pages may also display text from subsequent user interactions, and with dynamically loaded content (e.g., a countdown timer). To capture possible segments from such updates to the web page during a crawl—no matter how minor or transient—we integrated the Mutation Summary [3] library into our checkout crawler.

The Mutation Summary library combines DOM `MutationObserver` events [18] into compound event summaries that are easy to process. When the checkout crawler received a new Mutation Summary representing updates to the page, it segmented (Algorithm 1) this summary and stored the resulting segments.

For each segment, we stored its HTML Element type, its element text (via `innerText`), its dimensions and coordinates on the page, and its style including its text and background colors. Our crawls resulted in ~13 million segments across the 53K product URL pages.

4.3 Data Analysis with Clustering

We employed hierarchical clustering to discover dark patterns from the data set of segments. Our use of clustering was not to discover a set of latent constructs in the data but rather to organize the segments in a manner that would be conducive to scanning, making it easier for an expert analyst to sift through the clusters for possible dark patterns.

4.3.1 Data Preprocessing. Many of the ~13 million segments collected during our crawls were duplicates, such as multiple 'Add to cart' segments across multiple websites. Since we only used text-based features for our analyses, we retained unique pieces of text across the websites in our data set (e.g., one segment containing the text 'Add to cart' across all the websites in our data set). We also replaced all numbers with a placeholder before performing this process to further reduce duplicates. This preprocessing reduced the set of segments by 90% to ~1.3 million segments.

4.3.2 Feature Representations and Hierarchical Clustering. Before performing clustering, we transformed the text segments into a Bag of Words (BoW) representation. Each entry in the resulting BoW matrix (M_{ij}) indicated the number of times token j appeared in segment i.[7] We filtered all stop words[8] and punctuation—except currency symbols, since these are indicative of product price—from the list of tokens, and further only retained tokens that appeared in at least 100 segments. This resulted in a vocabulary of 10,133 tokens.

Given this large size of our vocabulary—and thus the dimensions of the segment-token matrix—we performed Principal Component Analysis (PCA) on the BoW matrix. We retained 3 components from the PCA, which together captured more than 95% of the variance in the data.

We used the Hierarchical Density-Based Spatial Clustering of Applications with Noise (HDBSCAN) algorithm [35] implemented in the `HDBSCAN` Python library [14] to extract clusters from this data. We chose HDBSCAN over other clustering algorithms since it is robust to noise in the data, and it allows us to vary the minimum size of the clusters (`min_cluster_size`). We varied a total of four passes at clustering: two `min_cluster_size` values (5 and 10) × two distance metrics (Manhattan distance or L1 norm, and Euclidean distance or L2 norm). We picked sufficiently small values for the `min_cluster_size` parameter to keep the size of the noise cluster small and to avoid coercing segments into one cluster.

The clustering output across the BoW input was nearly the same. As expected, a `min_cluster_size` of 10 resulted in a larger noise cluster compared to a `min_cluster_size` of 5—but only marginally larger regardless of the distance metric. However, since the `min_cluster_size` of 10 produced significantly fewer clusters, we picked its output over the others. It contained 10,277 clusters.

[7] We did not use the Term Frequency-Inverse Document Frequency (TF-IDF) representation as upon clustering, it resulted in anywhere between 70%-75% of the segments being classified as noise. We believe this may have been because of the incorrect IDF scaling factor since the segments were not all drawn from a pool of independent observations—i.e., multiple segments originated from the same website

[8] Using Python `NLTK` [30]

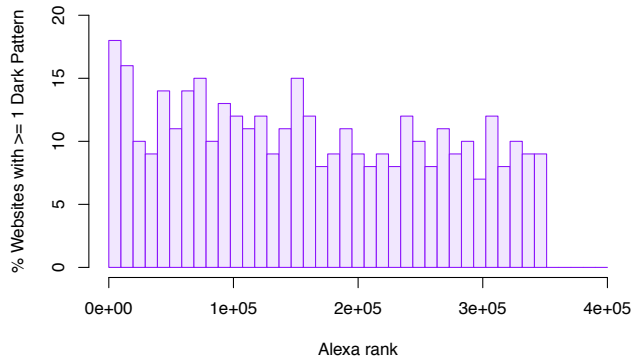


Fig. 2. Distribution of the dark patterns we discovered over the Alexa rank of the websites. Each bin indicates the percentage of shopping websites in that bin that contained at least one dark pattern.

4.3.3 Examining and Analyzing the Clusters. Once the clustering was complete, we made two passes through the data. The goal of pass one was to include clusters that contained any segments that might manifest as dark patterns. In this pass, one researcher scanned the clusters and identified possible clusters of interest, recording all those clusters that represented specific types of user interfaces (e.g., login choices, cart totals), website characteristics (e.g., stock notifications), and product options (e.g., small/medium/large) that generally appear on shopping websites. This step filtered down the clusters from 10,277 to 1,768.

In pass two, we extracted all the websites that corresponded to these segments for further examination. The research team used the literature on dark patterns [32, 48, 69] and impulse buying [65], and media coverage of high-pressure sales and marketing tactics (e.g., [15]) to create a shared understanding of possible dark patterns using the examples cited in these works to guide our thinking. In order to validate the coding of clusters, two researchers examined a sample of 200 of the 1,768 clusters, and recorded any dark patterns they encountered. The researchers also examined each website's set of screenshots and visited the websites to gain context and additional information surrounding the segments (e.g., discovering practices associated with the flagged pattern). To measure agreement between the researchers, we computed Cohen's kappa between the segments that were recorded—resulting in a score of 0.74. The team discussed and resolved all disagreements, and one researcher then examined the remaining clusters in the same manner. The team then discussed the resulting dark patterns, and iteratively grouped them into types and broader categories.

4.4 Detecting Deceptive Dark Patterns

We further examined many of the dynamic dark patterns—those patterns that displayed transient values (e.g., a countdown timer)—for deceptive practices. To this end, we used our checkout crawler to 'monitor' the websites containing dark patterns of interest once every four hours for a period of five days. We combined this data with several dark pattern-specific heuristics—which we describe in the following sections—to uncover instances of deceptive practices.

5 FINDINGS

In total, we discovered 1,818 instances of dark patterns from 1,254 (~11.1%) websites in our data set of 11K shopping websites. Given that (1) our crawler only explored the product pages, cart pages, and checkout pages of websites, (2) our analyses only took text-based user interfaces into

Table 1. Categories and types of dark patterns along with their description, prevalence, and definitions. Legend: ●= Always, ◐= Sometimes, ○= Never

Category	Type	Description	# Instances	# Websites	Asymmetric?	Covert?	Deceptive?	Hides Info?	Restrictive?	Cognitive Biases
Sneaking	Sneak into Basket	Adding additional products to users' shopping carts without their consent	7	7	○	○	◐	●	○	Default Effect
	Hidden Costs	Revealing previously undisclosed charges to users right before they make a purchase	5	5	○	○	◐	●	○	Sunk Cost Fallacy
	Hidden Subscription	Charging users a recurring fee under the pretense of a one-time fee or a free trial	14	13	○	○	◐	●	○	None
Urgency	Countdown Timer	Indicating to users that a deal or discount will expire using a counting-down timer	393	361	○	◐	◐	○	○	Scarcity Bias
	Limited-time Message	Indicating to users that a deal or sale will expire will expire soon without specifying a deadline	88	84	○	◐	○	●	○	Scarcity Bias
Misdirection	Confirmshaming	Using language and emotion (shame) to steer users away from making a certain choice	169	164	●	○	○	○	○	Framing Effect
	Visual Interference	Using style and visual presentation to steer users to or away from certain choices	25	24	◐	●	◐	○	○	Anchoring & Framing Effect
	Trick Questions	Using confusing language to steer users into making certain choices	9	9	●	●	○	○	○	Default & Framing Effect
	Pressured Selling	Pre-selecting more expensive variations of a product, or pressuring the user to accept the more expensive variations of a product and related products	67	62	◐	◐	○	○	○	Anchoring & Default Effect, Scarcity Bias
Social Proof	Activity Message	Informing the user about the activity on the website (e.g., purchases, views, visits)	313	264	○	◐	◐	○	○	Bandwagon Effect
	Testimonials	Testimonials on a product page whose origin is unclear	12	12	○	○	◐	○	○	Bandwagon Effect
Scarcity	Low-stock Message	Indicating to users that limited quantities of a product are available, increasing its desirability	632	581	○	◐	◐	◐	○	Scarcity Bias
	High-demand Message	Indicating to users that a product is in high-demand and likely to sell out soon, increasing its desirability	47	43	○	◐	○	○	○	Scarcity Bias
Obstruction	Hard to Cancel	Making it easy for the user to sign up for a service but hard to cancel it	31	31	○	○	○	◐	●	None
Forced Action	Forced Enrollment	Coercing users to create accounts or share their information to complete their tasks	6	6	●	○	○	○	●	None

account, this number represents a lower-bound estimate of the prevalence of dark patterns. We divide our discussion of the findings by first illustrating the categories of dark patterns revealed by our analyses, and then by describing our findings on the ecosystem of third-parties that enable dark patterns.

5.1 Categories of Dark Patterns

Our analyses revealed 15 types of dark patterns contained in 7 broader categories. Where applicable, we use the dark pattern labels proposed by Gray et al. [48] and Brignull [32] to describe these types and categories. Table 1 summarizes our findings, highlighting the number of separate instances of dark patterns found for each type.

Figure 2 shows the distribution of the websites containing dark patterns over their Alexa ranks. The distribution suggests that dark patterns are more likely to appear on popular websites (Spearman's Rho = -0.62, $p < 0.0001$). In the following sections, we describe the various categories and types of dark patterns we discovered.

5.1.1 Sneaking. Coined by Gray et al. in their taxonomy [48], 'Sneaking' refers to the category of dark patterns that attempt to misrepresent user actions, or hide/delay information that, if made available to users, they would likely object to. We observed three types of the Sneaking dark pattern: Sneak into Basket [32], Hidden Costs [32], and Hidden Subscription (Brignull's Forced Continuity [32]) on 23 shopping websites. Figure 3 highlights instances of these three types.

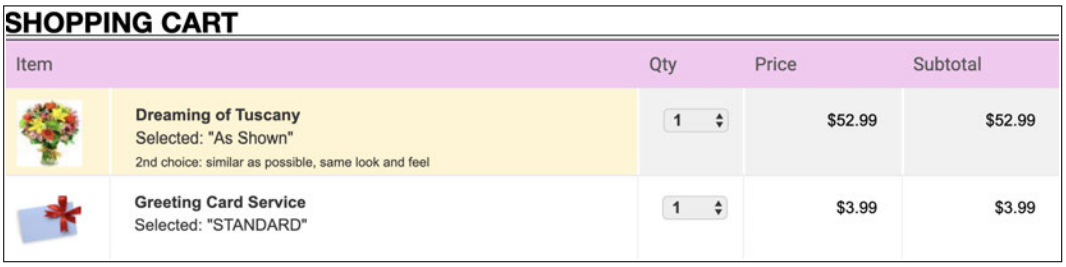
Sneak into Basket. The 'Sneak into Basket' dark pattern adds additional products to users' shopping carts without their consent, often promoting the added products as 'bonuses' and 'necessary'. Sneak into Basket exploits the default effect cognitive bias in users, with the website behind it hoping that users will stick with the products it adds to cart. One instance of Sneak into Basket is shown in Figure 3a, where adding a bouquet of flowers to the shopping cart on `avasflowers.net` also adds a greeting card. In another instance on `laptopoutlet.co.uk` —not shown in the figure— adding an electronic product, such as a laptop, to the shopping cart also adds product insurance. Other websites, such as `cellularoutfitter.com`, add additional products (e.g., a USB charger) to the shopping cart using pre-selected checkboxes. While such checkboxes could be deselected by a vigilant user, the additional products would be added by default in the absence of any intervention. In our data set, we found a total of 7 instances of the Sneak into Basket dark pattern.

Using our taxonomy of dark pattern characteristics, we classify Sneak into Basket as at least partially *deceptive* (it incorrectly represents the nature of the action of adding an item to the shopping cart) and *information hiding* (it deliberately disguises how the additional products were added to cart from users) in nature. However, it is not *covert*: users can visibly see and realize that the website included additional products to their shopping carts.

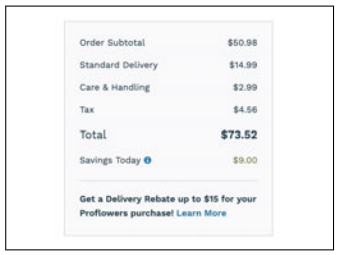
Hidden Costs. The 'Hidden Costs' dark pattern reveals new, additional, and often unusually high charges to users just before they are about to complete a purchase. Examples of such charges include 'service fees' or 'handling costs'. Often these charges are only revealed at the end of a checkout process, after the user has already filled out shipping/billing information, and consented to terms of use. The Hidden Costs dark pattern exploits the sunk cost fallacy cognitive bias: users are likely to feel so invested in the process that they justify the additional charges by completing the purchase to not waste their effort. Figure 3b shows the Hidden Costs dark pattern on `proflowers.com`, where the 'Care & Handling' charge of $2.99 is revealed immediately before confirming the order. In our data set, we found a total of 5 instances of the Hidden Costs dark pattern.

Using our taxonomy of dark pattern characteristics, we classify Hidden Costs as at least partially *deceptive* (it relies on minimizing and delaying information from users), and thus also *information hiding* in nature. Like Sneak into Basket, Hidden Costs is not *covert*: users can visibly see and realize that the website included additional charges.

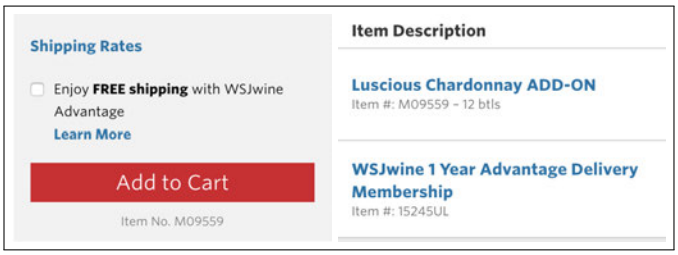
Hidden Subscription. The 'Hidden Subscription' dark pattern charges users a recurring fee under the pretense of a one-time fee or a free trial. Often, if at all, users become aware of the



(a) Sneak into Basket on `avasflowers.net`. Despite requesting no greeting cards, one worth $3.99 is automatically added.



(b) Hidden Costs on `proflowers.com`. The Care & Handling charge ($2.99) is disclosed on the last step.



(c) Hidden Subscription on `wsjwine.com`. Left: The website fails to disclose that the *Advantage* service is an annual subscription worth $89 unless the user clicks on *Learn More*. Right: The service in cart.

Fig. 3. Three types of the Sneaking category of dark patterns.

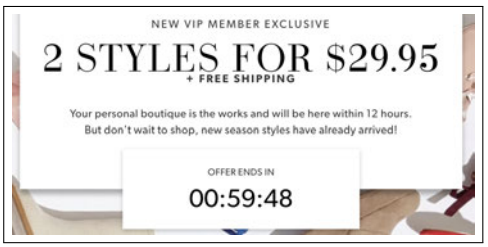
recurring fee once they are charged several days or months after their purchase. For instance, we discovered that `wsjwine.com` offers users an *Advantage* service which appears to be a one-time payment of $89 but renews annually, as shown in Figure 3c. Further, Hidden Subscription often appears with the 'Hard to Cancel' dark pattern—which we describe in Section 5.1.6—thereby making the recurring charges harder to cancel than signing up for them. In our data set, we found a total of 14 instances of Hidden Subscription dark pattern.

Using our taxonomy of dark pattern characteristics, we classify Hidden Subscription as at least partially *deceptive* (it misleads users about the nature of the initial offer) and *information hiding* (it withholds information about the recurring fees from users) in nature.

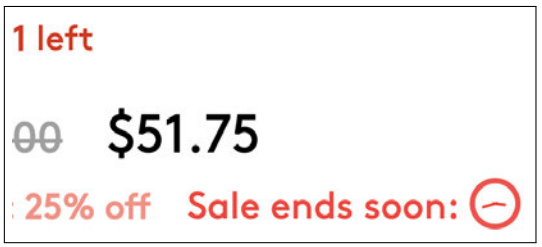
5.1.2 Urgency. 'Urgency' refers to the category of dark patterns that impose a deadline on a sale or deal, thereby accelerating user decision-making and purchases [27, 37, 53, 69]. Urgency dark patterns exploit the scarcity bias in users—making discounts and offers more desirable than they would otherwise be, and signaling that inaction would result in losing out on potential savings. These dark patterns create a potent 'fear of missing out' effect particularly when combined with the Social Proof (Section 5.1.4) and Scarcity (Section 5.1.5) dark patterns.

We observed two types of the Urgency dark pattern: Countdown Timers and Limited-time Messages on 437 shopping websites across their product, cart, and checkout pages. In product pages, these indicated deadlines about site-wide sales and coupons, sales on specific products, or shipping deadlines; in cart pages, they indicated deadlines about product reservation (e.g., 'Your cart will expire in 10:00 minutes, please check out now') and coupons, urging users to complete their purchase. Figure 4 highlights instances of these two types.

(a) Countdown Timer on mattressfirm.com. The header displays a *Flash Sale* where the majority of discounted products remain the same on a day-to-day basis.



(b) Countdown Timer on justfab.com. The offer is available even after the timer expires.



(c) Limited-time Message on chicwish.com. The website claims the sale will end 'soon' without stating a deadline.

Fig. 4. Two types of the Urgency category of dark patterns.

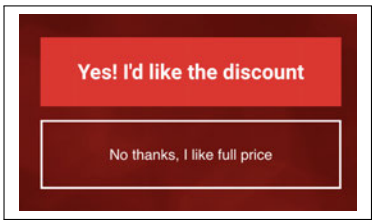
Countdown Timers. The 'Countdown Timer' dark pattern is a dynamic indicator of a deadline, counting down until the deadline expires. Figures 4a and 4b show the Countdown Timer dark pattern on mattressfirm.com and justfab.com, respectively. One indicates the deadline for a recurring *Flash Sale*, the other a *Member Exclusive*. In our data set, we found a total of 393 instances of the Countdown Timer dark pattern.

Deceptive Countdown Timers. Using the visit-and-record method described in Section 4.4, we examined the countdown timers in our data set for deceptive practices. We stitched the screenshots of each countdown timer from the repeated visits of our crawler to a website into a video, and viewed the resulting videos to observe the behavior of the timers. We considered a countdown timer deceptive if (1) the timer reset after timeout with the same offer still valid, or (2) the timer expired but the offer it claimed was expiring was still valid even following expiration.

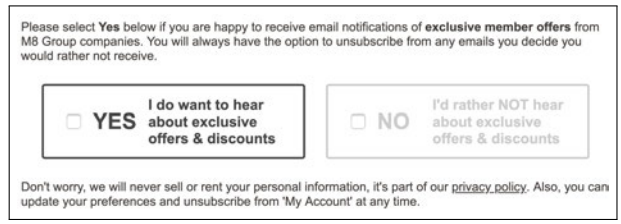
In our data set, we discovered a total of 157 instances of deceptive Countdown Timers on 140 shopping websites. One such example is shown in Figure 4b on justfab.com, where the advertised offer remains valid even after the countdown timer of 60 minutes expires.

Using our taxonomy of dark pattern characteristics, we classify Countdown Timers as partially *covert* (it creates a heightened sense of immediacy, unbeknownst to at least some users), and sometimes *deceptive* (it can mislead users into believing an offer is expiring when in reality it is not) in nature.

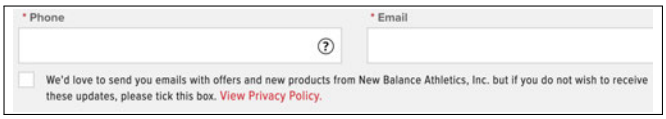
Limited-time Messages. Unlike Countdown Timers, the 'Limited-time Message' dark pattern is a static urgency message without an accompanying deadline. By not stating the deadline, websites withhold information from users, and thus misrepresent the nature of the offer [20]. Figure 4c shows an instance of the Limited-time Message dark pattern on chicwish.com, where the advertised sale is stated to end 'soon' with no mention of the end date. For every such instance we discovered, we verified that the shopping website made no disclosure about the accompanying deadline (e.g., in



(a) Confirmshaming on radioshack.com. The option to dismiss the popup is framed to shame the user into avoiding it.



(b) Visual Interference on greenfingers.com. The option to opt out of marketing communication is grayed, making it seem unavailable even though it can be clicked.



(c) Trick Questions on newbalance.co.uk. Opting out of marketing communication requires ticking the checkbox.

(d) Pressured Selling on 1800flowers.com. The most expensive product is the default.

Fig. 5. Four types of the Misdirection category of dark patterns.

the fine print and in the terms of sale pages). In our data set, we discovered a total of 88 instances of the Limited-time Message dark pattern.

Using our taxonomy of dark pattern characteristics, we classify Limited-time Messages as at least partially *covert* (similar to Countdown Timers), and *information hiding* (unlike Countdown Timers, they do not reveal the deadline in their offers) in nature.

5.1.3 Misdirection. The 'Misdirection' category of dark patterns uses visuals, language, and emotion to steer users toward or away from making a particular choice. Misdirection functions by exploiting different affective mechanisms and cognitive biases in users without actually restricting the set of choices available to users. Our version of the Misdirection dark pattern is inspired by Brignull's original Misdirection dark pattern [32]. However, while Brignull considered Misdirection to occur exclusively using stylistic and visual manipulation, we take a broader view of the term, also including Misdirection caused by language and emotional manipulation.

We observed four types of the Misdirection dark pattern: Confirmshaming [32], Trick Questions [32], Visual Interference [48], and Pressured Selling on 244 shopping websites. Figure 5 highlights instances of these four types.

Confirmshaming. Coined by Brignull [32], the 'Confirmshaming' dark pattern uses language and emotion to steer users away from making a certain choice. Confirmshaming appeared most often in popup dialogs that solicited users' email addresses in exchange for a discount, where the option to decline the offer—which the website did not want users to select—was framed as a shameful choice. Examples of such framing included 'No thanks, I like paying full price', 'No thanks, I hate saving money', and 'No thanks, I hate fun & games'. By framing the negative option as such, the Confirmshaming dark pattern exploits the framing effect cognitive bias in users and shame, a powerful behavior change agent [58]. Figure 5a shows one instance of the Confirmshaming dark pattern on radioshack.com. In our data set, we found a total of 169 such instances.

Using our taxonomy of dark pattern characteristics, we classify Confirmshaming as *asymmetric* (the opt-out choice shames users into avoiding it) in nature. However, Confirmshaming is not *covert*, since users can visibly see and realize that the design is attempting to influence their choice.

Visual Interference. The 'Visual Interference' dark pattern uses style and visual presentation to influence users into making certain choices over others (Brignull's original description of Misdirection [32]). Although we excluded style information in our clustering analysis, we extracted these patterns as a consequence of examining the text the patterns displayed. In some instances, websites used the Visual Interference dark pattern to make certain courses of action more prominent over others. For example, the subscription offering on `exposedskincare.com` is stylistically more prominent and emphasized than the non-subscription offering. In other instances, websites used visual effects on textual descriptions to inflate the discounts available for products. For example, websites such as `dyson.co.uk` and `justfab.com` offered free gifts to users, and then used these gifts to inflate the savings on users' purchases in the checkout page—even when the originally selected product was not on discount. In one instance on `greenfingers.com`, we discovered that the option to decline marketing communication is greyed out, creating an illusion that the option is unavailable or disabled even though it can be clicked, as shown in Figure 5b. In our data set, we found a total of 25 instances of the Visual Interference dark pattern.

Using our taxonomy of dark pattern characteristics, we classify Visual Interference as sometimes *asymmetric* (in some instances it creates unequal choices, steering users into one choice over the other), *covert* (users may not realize the effect the visual presentation has had on their choice), and sometimes *deceptive* (e.g., when a website presents users with a 'lucky draw' from a list of potential deals, but the draw process is deterministic unbeknownst to users) in nature.

Trick Questions. Also originating from Brignull's taxonomy [32], the 'Trick Questions' dark pattern uses confusing language to steer users into making certain choices. Like Confirmshaming, Trick Questions attempt to overcome users' propensity to opt out of marketing and promotional messages by subtly inverting the entire opt-out process. Most often, websites achieved this effect by introducing confusing double negatives (e.g., 'Uncheck the box if you prefer not to receive email updates'), or by using negatives to alter expected courses of action, such as checking a box to opt out (e.g., 'We would like to send you emails. If you do not wish to be contacted via email, please ensure that the box is not checked').

We note here that we only considered an opt-out choice as a Trick Question dark pattern when it was misleading, such as when the user has to check a box and the text began with an affirmative statement about the undesirable practice (e.g., 'We want to send you marketing email...') since these would more likely be missed by users as opposed to ones that began with the opt-out choice (e.g., 'Please tick here to opt-out of...').[9] Trick Questions exploits the default and framing effect cognitive biases in users, who become more susceptible to a choice they erroneously believe is aligned with their preferences. Figure 5c shows one instance of Trick Questions on `newbalance.co.uk`. In our data set, we found a total of 9 such instances, occurring most often during the checkout process when collecting user information to complete purchases.

Using our taxonomy of dark pattern characteristics, we classify Trick Questions as *asymmetric* (opting out is more burdensome than opting in) and *covert* (users fail to understand the effect of their choice as a consequence of the confusing language) in nature.

[9]We note that while Gray et al. [48] consider the latter as Trick Questions, we do not take that stance. However, we do consider all opt-out messages as concerning. We discovered 23 instances of opt-out choices that did not begin with an affirmative statement in total.

Pressured Selling. The 'Pressured Selling' dark pattern refers to defaults or often high-pressure tactics that steer users into purchasing a more expensive version of a product (*upselling*) or into purchasing related products (*cross-selling*). The Pressured Selling dark pattern exploits a variety of different cognitive biases, such as the default effect, the anchoring effect, and the scarcity bias to drive user purchasing behavior. Figure 5d shows one such instance on `1800flowers.com`, where the largest flower bouquet is selected by default. The dark pattern makes the most expensive option the point of comparison—an 'anchor'—and thus increases the probability of users overlooking the least expensive option [70]. In another instance, on `fashionworld.co.uk`, the website opened popup dialogs that the user had to explicitly decline immediately after adding a product to cart. These dialogs urged users to buy more 'Hot sellers', 'Deals', and 'Bundled' products. In our data set, we found a total of 67 instances of the Pressured Selling dark pattern.

Using our taxonomy of dark pattern characteristics, we classify Pressured Selling as sometimes *asymmetric* (it pushes users towards accepting more expensive product options) and at least partially *covert* (users fail to realize that they have purchased a more expensive product than they would have, had they been defaulted with the least expensive product to begin with) in nature.

5.1.4 Social Proof. According to the social proof principle, individuals determine the correct action and behavior for themselves in a given situation by examining the action and behavior of others [37, 69]. The 'Social Proof' dark pattern uses this influence to accelerate user decision-making and purchases, exploiting the bandwagon effect cognitive bias to its advantage. Studies have shown that individuals are more likely to impulse buy when shopping with their peers and families [61].

We observed two types of the Social Proof dark pattern: Activity Notifications and Testimonials of Uncertain Origin on 275 websites across their product and cart pages. In all these instances, the Social Proof messages indicated other users' activities and experiences shopping for products and items. Figure 6 highlights instances of these two types.

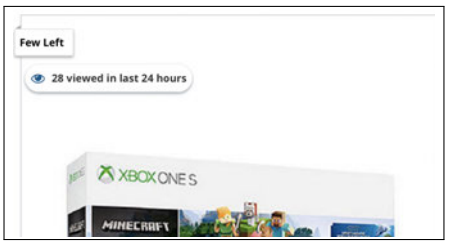
Activity Notifications. The 'Activity Notification' dark pattern is a transient, often recurring and attention grabbing message that appears on product pages indicating the activity of other users. These can be grouped into different categories: dynamic and periodic messages that indicated other users just bought a product (e.g., 'Abigail from Michigan just bought a new stereo system'); static or dynamic text to indicate how many users have a specific item in their cart (e.g., '35 people added this item to cart'); and similar text to indicate how many users have viewed a product (e.g., '90 people have viewed this product'). Figures 6a, 6b, and 6c highlight three instances of Activity Notification on `tkmaxx.com`, `thredup.com`, and `jcpenney.com`, respectively. In our data set, we found a total of 313 such instances.

Deceptive Activity Notifications. We examined the Activity Notification messages in our data set for deceptive practices. To facilitate our analysis, we manually inspected the page source of each shopping website that displayed these notifications to verify their integrity. We ignored all those notifications that were generated server-side since we had limited insight into how and whether they were truly deceptive. We considered an instance of Activity Notification to be deceptive if the content it displayed—including any names, locations statistics, counts—was falsely generated or made misleading statements.

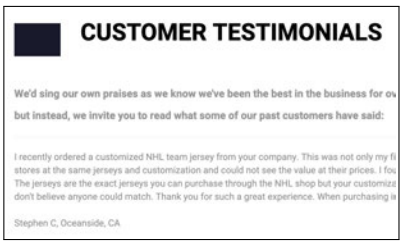
In our data set, we discovered a total of 29 instances of deceptive Activity Notifications on 20 shopping websites. The majority of these websites generated their deceptive notifications in a random fashion (e.g., using a random number generator to indicate the number of users who are 'currently viewing' a product) and others hard-coded previously generated notifications, meaning they never changed. One notable case was `thredup.com` as shown in Figure 6b, where the website

(a) Activity Notification on tkmaxx.com. The message indicates how many people added the product to the cart in the last 72 hours.

(b) Activity Notification on thredup.com. The message always signals products as if they were sold recently ('just saved'), even in the case of old purchases.



(c) Activity Notification on jcpenney.com. The message indicates the number of people who viewed the product in the 24 hours along with the quantity left in stock.



(d) Testimonials of Uncertain Origin on coolhockey.com. We found the same testimonials on ealerjerseys.com with different customer names.

Fig. 6. Two types of the Social Proof category of dark patterns.

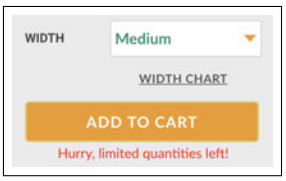
generated messages based on fictitious names and locations for an unvarying list of products that was always indicated to be 'just sold'.

Using our taxonomy of dark pattern characteristics, we classify Activity Notifications as partially *covert* (in instances where the notifications are site-wide for example, users may fail to understand their effect on their choices) and sometimes *deceptive* (the content of notifications can be deceptively generated or misleading) in nature.

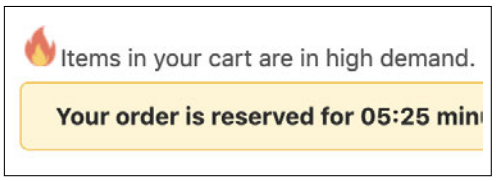
Testimonials of Uncertain Origin. The 'Testimonials of Uncertain Origin' dark pattern refers to the use of customer testimonials whose origin or how they were sourced and created is not clearly specified. For each instance of this dark pattern, we made two attempts to validate its origin. First, we inspected the website to check if it contained a form to submit testimonials. Second, we performed exact searches of the testimonials on a search engine (google.com) to check if they appeared on other websites. Figure 6d shows one instance on coolhockey.com, where we found the same set of testimonials on ealerjerseys.com with different customer names attached to them. In our data set, we found a total of 12 instances of this pattern.

5.1.5 Scarcity. 'Scarcity' refers to the category of dark patterns that signal the limited availability or high demand of a product, thus increasing its perceived value and desirability [37, 55, 62, 69]. We observed two types of the Scarcity dark pattern: 'Low-stock Messages' and 'High-demand Messages' on 609 shopping websites across their product and cart pages. In both pages, they indicated the limited availability of a product or that a product was in high demand and thus likely to become unavailable soon. Figure 7 highlights instances of these two types.

(a) Low-stock Message on 6pm.com. Left: Choosing product options shows *Only 3 left in stock*. Right: The out-of-stock product makes it seem that it just sold out.



(b) Low-stock on orthofeet .com. Appears for all products.



(c) High-demand Message on fashionnova.com. The message appears for all products in the cart.

Fig. 7. Two types of the Scarcity category of dark patterns.

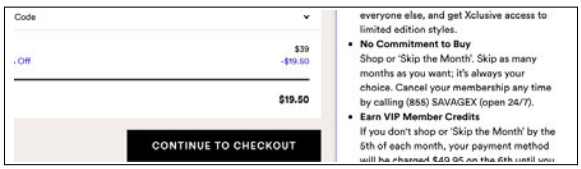
Low-stock Messages. The 'Low-stock Message' dark pattern signals to users about limited quantities of a product. Figure 7a shows an instance of this pattern on 6pm.com, displaying the precise quantity in stock. In our data set, we found a total of 632 instances of the Low-stock Message dark pattern. However, not all of these instances displayed stock quantities. 49 of these instances only indicated that stock was limited or low, without displaying the exact quantity, resulting in uncertainty, increased desirability of products, and impulse buying behavior in users. Figure 7b shows one such instance on orthofeet.com.

Deceptive Low-stock Messages. We examined all the Low-stock Message dark patterns for deceptive practices using the method described in Section 4.4. From the resulting data, we ignored those websites whose stock amounts remained the same between visits, reasoning that those are unlikely to be indicative of deceptive practices. We then manually examined the remaining sites and identified how the stock information was generated.

In our data set, we discovered a total of 17 instances of deceptive Low-stock Messages on 17 shopping websites. On further examination, we observed that 16 of these sites decremented stock amounts in a recurring, deterministic pattern according to a schedule, and the one remaining site (forwardrevive.com) randomly generated stock values on page load. Exactly 8 of these sites used third-party JavaScript libraries to generate the stock values, such as Hurrify [17] and Booster [11]. Both of these are popular plugins for Shopify—one of the largest e-Commerce companies—based websites. The remaining websites injected stock amounts through first-party JavaScript or HTML.

Besides the use—or non-use—of numeric data and deception, Low-stock Messages can be concerning in other ways. For example, we observed that several websites, such as 6pm.com and orthofeet.com, displayed Low-stock Messages for nearly all their products—stating 'Only X left' and 'Hurry, limited quantities left!' respectively. The former, in particular, showed a 'Sorry, this is out of stock. You just missed it' popup dialog for every product that was sold out, even if it had already been out of stock in the previous days.

(a) Hard to Cancel on sportsmanguide.com. The website only discloses in the terms PDF file that canceling the recurring service requires calling customer service.



(b) Hard to Cancel on savagex.com. The website discloses upfront that the recurring service can only be canceled through customer care.

Fig. 8. The Hard to Cancel type from the Obstruction category of dark patterns.

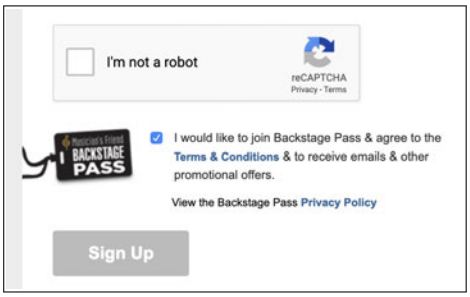
Using our taxonomy of dark pattern characteristics, we classify Low-stock Messages as partially *covert* (it creates a heightened sense of impulse buying, unbeknownst to users), sometimes *deceptive* (it can mislead users into believing a product is low on stock when in reality it is not, creating false scarcity), and sometimes *information hiding* (in some instances, it does not explicitly specify the stock quantities at hand) in nature.

High-demand Messages. The 'High-demand Message' dark pattern signals to users that a product is in high demand, implying that it is likely to sell out soon. Figure 7c shows one such instance on fashionnova.com on the cart page, indicating that the products in the cart are selling out quickly. In our data set, we found a total of 47 instances of the High-demand dark pattern; 38 of these instances appeared consistently, regardless of the product displayed on the website, or regardless of the items in cart. As with Low-stock Messages, we classify High-demand Messages as partially *covert*.

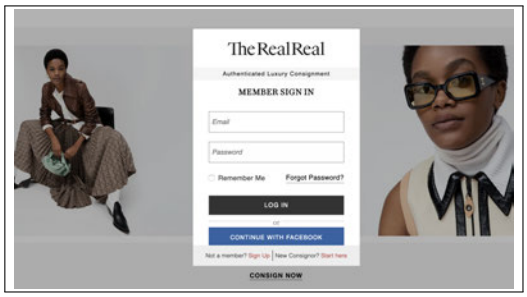
5.1.6 Obstruction. 'Obstruction', coined by Gray et al. [48], refers to the category of dark patterns that make a certain action harder than it should be in order to dissuade users from taking that action. We observed one type of the Obstruction dark pattern: 'Hard to Cancel'—a pattern similar to Brignull's *Roach Motel* dark pattern [32]—on 31 websites. Obstruction makes it easy for users to sign up for recurring subscriptions and memberships, but it makes it hard for them to subsequently cancel the subscriptions.

More often than not, shopping websites did not disclose upfront to users that canceling the subscription or membership could not be completed in the same manner they signed up for the memberships in the first place. For example, as shown in Figure 8a, sportsmansguide.com promotes a 'buyer's club' discount membership price and makes it easy for users to sign up for the annual recurring membership, as they are under the impression they can 'cancel anytime.' However, sportsmansguide.com's terms of service reveal that the membership can only be cancelled by calling their customer service. In rare instances, as shown in Figure 8b, websites such as savagex.com disclosed upfront that cancellation required calling customer service.

Using our taxonomy of dark pattern characteristics, we classify Hard to Cancel as *restrictive* (it limits the choices users can exercise to cancel their services) in nature. In cases where websites do



(a) Forced Enrollment on `musiciansfriend.com`. Agreeing to the terms of use also requires agreeing to receive emails and promotions.



(b) Forced Enrollment on `therealreal.com`. Browsing the website requires creating an account even without making a purchase.

Fig. 9. The Forced Enrollment type from the Forced Action category of dark patterns.

not disclose their cancellation policies upfront, Hard to Cancel also becomes *information hiding* (it fails to inform users about how cancellation is harder than signing up) in nature.

5.1.7 Forced Action. 'Forced Action' refers to the category of dark patterns—originally proposed by Gray et al. [48]—that require users to take certain additional and tangential actions to complete their tasks. We observed one type of the Forced Action dark pattern, 'Forced Enrollment', on 6 websites. This type of dark pattern explicitly coerces users into signing up for marketing communication, or creates accounts to surrender users' information. By using the Forced Enrollment dark pattern, online services and websites collected more information about their users than they might otherwise consent to—resulting from an all-or-nothing proposition.

On four out of six websites, the Forced Enrollment dark pattern manifested as a checkbox in the user interface, requiring users to simultaneously consent to the terms of service *and* to receiving marketing emails as part of the consent process. Figure 9a shows one such instance on `musiciansfriend.com`. In another instance of the Forced Enrollment on `therealreal.com`—as shown in Figure 9b—the website displayed a popup dialog that prevented users from viewing product offerings on the website without creating an account—even if users eventually decide against making a purchase.

Using our taxonomy of dark pattern characteristics, we classify Forced Enrollment as *asymmetric* (it requires competing the additional, tangential tasks, creating unequal choices) and *restrictive* (it mandates enrolling in marketing communication or creating accounts) in nature.

5.2 Dark Patterns as A Third-Party Service: A Case Study Of Social Proof Activity Notifications

In many instances, third-party entities—i.e., organizations and companies other than the shopping websites themselves—were responsible for creating and presenting dark patterns on behalf of the shopping websites. We observed this frequently to be the case for one dark pattern in particular: Social Proof Activity Notifications (Section 5.1.4). In this section, we shed light on the ecosystem of third parties that enable Social Proof Activity Notifications, using our starting point as the list of websites in our data set that displayed such Activity Notifications.

5.2.1 Detecting Third-party Entities. In order to detect third-party entities, it is sufficient to uncover scripts that are served from third-party domains and are responsible for creating Social Proof

Activity Notifications. However, automatically attributing certain interface elements and webpage modifications to third-party scripts constitutes a more challenging task because modern browsers do not expose any means to attribute DOM changes (e.g. displaying a popup dialog) to particular scripts. Further, web pages may be modified by several different first and third-party scripts in the same visit, making attribution trickier.

To overcome this challenge, we employed a combination of automated and manual analyses. We used the following observation: when a third-party entity displays an Activity Notification on a shopping website, its content should be included in the HTTP response received from this third party's servers on that website. For example, if the notification states 'Jane from Washington, DC just purchased this product', looking up the customer name and location—in this case 'Jane' and 'Washington, DC'—in the HAR file for that website should reveal the end point of the server that issued the notification. Thus, for all notifications of this kind, we extracted the name and location pairs from the content, searched the HAR files for these pairs; where successful, we recorded the HTTP endpoints corresponding to the third-parties. We then manually verified these endpoints and determined the responsible entities by using the WHOIS database, visiting the script domains and using search engines to uncover the company identities and websites.

Where this analysis failed to return an HTTP endpoint from the HAR files, and for all other kinds of Social Proof Activity Notification (e.g., 'This product was added to cart 10 times in the last day'), we manually visited the websites containing the message to determine the responsible third parties. We sped up this analysis using Google Chrome Developer Tool's 'DOM change breakpoints' feature [16], which helped us easily determine the responsible entities.

Having determined the third-party entities, we measured their prevalence across all the shopping websites in our data set. To do so, we searched the HTTP request data from checkout crawls for the third-party domains we identified. Finally, as a reference point, we also determined their prevalence on the web—beyond shopping websites—using the latest publicly available crawl data (November 2018) from the Princeton Web Census Project [7, 40]. This public project documents the prevalence of third-party scripts using periodic scans of home pages of Alexa top million sites and is available for external researchers to use.

5.2.2 The Ecosystem Of Third-party Entities. Table 2 summarizes our findings. We discovered a total of 22 third-party entities, embedded in 1,066 of the 11K shopping websites in our data set, and in 7,769 of the Alexa top million websites. We note that the prevalence figures from the Princeton Web Census Project data should be taken as a lower bound since their crawls are limited to home pages of websites. This difference in prevalence is particularly visible for certain third-party entities like Qubit and Taggstar, where their prevalence is higher in our data set compared to the Web Census data. By manually examining websites that contained these third parties, we discovered that many shopping websites only embedded them in their product—and not home—pages, presumably for functionality and performance reasons.

We learned that many third-party entities offered a variety of services for shopping websites, including plugins for popular e-commerce platforms such as Shopify[10] and Woocommerce[11]. To better understand the nature and capabilities of each third-party entity, we examined any publicly available marketing materials on their websites.

Broadly, we could classify the third-party entities into two groups. The first group exclusively provided Social Proof Activity Notifications integration as a service. The second group provided a wider array of marketing services that often enabled other types of dark patterns; most commonly

[10]https://shopify.com
[11]https://woocommerce.com

Table 2. List and prevalence of Social Proof Activity Notifications enabling third-party entities in our data set of 11K shopping websites and the home pages of Alexa top million websites [7]. Where available, we list additional dark patterns the third parties claim to offer. Nice/Bizzy, Woocommerce Notification, Boost, and Amasty are Shopify, Woocommerce, Wordpress and Magento plugins respectively.

Third-party Entity	Prevalence		Additional Dark Patterns
	# Shopping Websites	# Alexa Top Million	
Beeketing	406	4,151	Pressured Selling, Urgency, Scarcity
Dynamic Yield	114	416	Urgency
Yieldify	111	323	Urgency, Scarcity
Fomo	91	663	–
Fresh Relevance	86	208	Urgency
Insider	52	484	Scarcity, Urgency
Bizzy	33	213	–
ConvertCart	31	62	–
Taggstar	27	4	Scarcity, Urgency
Qubit	25	73	Pressured Selling, Scarcity, Urgency
Exponea	18	180	Urgency, Scarcity
Recently	14	66	–
Proof	11	508	–
Fera	11	132	Pressured Selling, Scarcity, Urgency
Nice	10	80	–
Woocommerce Notification	10	61	–
Bunting	5	17	Urgency, Scarcity
Credibly	4	67	–
Convertize	3	58	Scarcity, Urgency
LeanConvert	2	0	–
Boost	1	3	–
Amasty	1	0	Pressured Selling, Scarcity, Urgency

these were Scarcity and Urgency dark patterns. We list all these additional dark pattern capabilities in the rightmost column of Table 2.

Many of the third-parties advertised practices that appeared to be—and sometimes unambiguously were—manipulative: '[p]lay upon [customers'] fear of missing out by showing shoppers which products are creating a buzz on your website' (Fresh Relevance), '[c]reate a sense of urgency to boost conversions and speed up sales cycles with Price Alert Web Push' (Insider), '[t]ake advantage of impulse purchases or encourage visitors over shipping thresholds' (Qubit). Further, Qubit also advertised Social Proof Activity Notifications that could be tailored to users' preferences and backgrounds.

In some instances, we found that third parties openly advertised the deceptive capabilities of their products. For example, Boost dedicated a web page—titled 'Fake it till you make it'—to describing how it could help create fake orders [12]. Woocommerce Notification—a Woocommerce platform plugin—also advertised that it could create fake social proof messages: '[t]he plugin will create fake orders of the selected products' [24]. Interestingly, certain third parties (Fomo, Proof, and Boost) used Activity Notifications on their websites to promote their own products.

Finally, we also discovered that some of these deceptive practices resulted in e-commerce platforms taking action against third-party entities. For instance, Beeketing's—the most popular third

Fig. 10. Mockup of a possible browser extension that can be developed using our data set. The extension flags instances of dark patterns with a red warning icon. By hovering over the icon, the user can learn more about the specific pattern.

party provider in our data set—'Sales Pop' Shopify plugin was temporarily removed from Shopify in an effort to crack down on deceptive practices [67, 76]. The plugin had allowed websites to create fake Activity Notifications by entering fabricated sales data.

In summary, we discovered that third party entities widely enable dark patterns on shopping websites. Furthermore, some of these third-parties even advertised the deceptive use of their services.

6 DISCUSSION

6.1 Dark Patterns and Implications For Consumers

Many dark patterns constitute manipulative and deceptive practices that past work has shown users are increasingly becoming aware of [36]. Our current data set of dark patterns, comprising of screenshots and text segments, can be used to build countermeasures to help users make more informed decisions even in the presence of dark patterns. One such countermeasure could be a public-facing website that scores shopping websites based on their use of dark patterns. Our data set can also enable the development of browser extensions that automatically detect and flag dark patterns (e.g., shopping websites, as shown in Figure 10). Such a tool could be augmented to flag dark patterns on websites not in our data set through users' submissions, through community-generated and maintained lists (similar to how ad blockers work [26]), or through trained machine learning classifiers. Eventually, such tools could be integrated into browsers themselves. For example, in recent years, Firefox and Safari have shown interest in integrating tools that promote consumer privacy (e.g., features to block web tracking by default [66, 82]). However, finding the right incentives for browser vendors to implement these solutions might be challenging in the context of dark patterns, since they might be wary of policing content on the web. Finally, future studies could leverage our descriptive and comparative taxonomy of dark pattern characteristics to better understand their effects on users, as well as to ascertain which dark patterns are considered most egregious by users (e.g., by means of users studies).

6.2 Implications for Consumer Protection Policy and Retailers

Our results demonstrate that a number of shopping websites use deceptive dark patterns, involving affirmative and false representations to consumers. We also found 22 different third-party entities that enable the creation of Social Proof Activity Notification dark patterns. Some of these entities promote blatantly deceptive practices and provide the infrastructure for retailers to use these

practices to influence consumer behavior for profit. These practices are unambiguously unlawful in the United States (under Section 5 of the Federal Trade Commission Act and similar state laws [45]), and the European Union (under the Unfair Commercial Practices Directive and similar member state laws [42]).

We also find practices that are unlawful in a smaller set of jurisdictions. In the European Union, businesses are bound by an array of affirmative disclosure and independent consent requirements in the Consumer Rights Directive [43]. Websites that use the Sneaking dark patterns (Sneak into Basket, Hidden Subscription, and Hidden Costs) on European Union consumers are likely in violation of the Directive. Furthermore, user consent obtained through Trick Questions and Visual Interference dark patterns do not constitute freely given, informed and active consent as required by the General Data Protection Regulation (GDPR) [44]. In fact, the Norwegian Consumer Council filed a GDPR complaint against Google in 2018, arguing that Google used dark patterns to manipulate users into turning on the 'Location History' feature on Android, and thus enabling constant location tracking [47].

In addition to demonstrating specific instances of unlawful business practices, we contribute a new approach for regulatory agencies and other consumer protection stakeholders (e.g., journalists and civil society groups) to detect dark patterns. The crawling and clustering methodology that we developed is readily generalizable, and it radically reduces the difficulty of discovering and measuring dark patterns at web scale. Furthermore, our data set of third-party entities which provide the infrastructure to enable certain deceptive dark patterns can be used by regulators as a starting point to inform policy and regulation around what kinds of practices should be allowable in the context online shopping.

6.3 Dark Patterns and Future Studies At Scale

We created automated techniques that can be used to conduct measurements of dark patterns at web scale. Researchers can extend our tools and infrastructure to document the presence of dark patterns other types of websites (e.g., travel and ticket booking websites) by building a crawler that traverses users' primary interaction paths on those websites. Researchers can also extend our techniques to measure dark patterns that are not inherently *dark* because of the text they display but because they take advantage of visual elements. For example, urgency can be created by a blinking timer; similarly, Hidden Subscriptions can make the default option (e.g., subscribing to a paid service) visually more appealing and noticeable than its alternative (e.g., not subscribing). One starting point to detect such interfaces could be to incorporate style and color as features for clustering, or even use the design mining literature [39, 56, 59] to analyze specific types of interfaces (e.g., page headers) in isolation. Finally, researchers can leverage our descriptive taxonomy of dark pattern characteristics to study and analyze dark patterns in other domains, such as emails and mobile applications.

6.4 Limitations

Our research has several limitations. First, we only take into account text-based dark patterns and, therefore, leave out those that are inherently visual (e.g., using font size or color to emphasize one part of the text more than another). Second, many of the dark patterns we document are derived from the existing dark patterns literature. However, some of these are exist in a gray area, and in those cases determining whether a dark pattern is deliberately misleading or not can sometimes be hard to discern. Opinions of dark patterns may also vary between and among experts and users (e.g., countdown timers to indicate when to order to be eligible for free shipping). Clarifying this gray area and establishing the degree to which these patterns are perceived as manipulative by users can be further investigated by future user studies. Third, in Section 3 we drew connections between

each type of dark pattern and a set of cognitive biases it exploits. However, these connections may be more nuanced or complex. For example, not all individuals may be equally susceptible to these cognitive biases; some individuals may be more susceptible to one kind over another. Fourth, during our crawls we experienced a small number of Selenium crashes, which did not allow us to either retrieve product pages or complete data collection on certain websites. Fifth, while the crawler was mostly effective in simulating user actions, it failed to complete the product purchase flow on some websites (see Section 4). Sixth, and finally, we only crawled product pages and checkout pages, missing out on dark patterns commonly present in other pages, such as the home page, product search, and account creation pages. Many dark patterns also appear after purchase (e.g., upselling) which our crawler fails to capture because we do not make purchases. Future studies could consider collecting these kinds of dark patterns from users.

7 CONCLUSION

In this paper, we developed automated techniques to study dark patterns on the web at scale. By simulating user actions on the ~11K most popular shopping websites, we collected text and screenshots of these websites to identify their use of dark patterns. We defined and characterized these dark patterns, describing how they affect users' decisions by linking our definitions to the cognitive biases leveraged by dark patterns. We found at least one instance of dark pattern on approximately 11.1% of the examined websites. Notably, 183 of the websites displayed deceptive messages. Furthermore, we observed that dark patterns are more likely to appear on popular websites. Finally, we discovered that dark patterns are often enabled by third-party entities, of which we identify 22; two of these advertise practices that enable deceptive patterns. Based on these findings, we suggest that future work focuses on empirically evaluating the effects of dark patterns on user behavior, developing countermeasures against dark patterns so that users have a fair and transparent experience, and extending our work to discover dark patterns in other domains.

ACKNOWLEDGMENTS

We are grateful to Mihir Kshirsagar, Finn Myrstad, Vincent Toubiana, and Joe Calandrino for feedback on this paper.

REFERENCES

[1] 2013. Marketing Firm Agrees To $30 Million Settlement. https://www.wsj.com/articles/marketing-firm-agrees-to-30-million-settlement-1381441148. Accessed March 12, 2019.
[2] 2014. Affinion Group faces class action after paying out claims to AGs. https://www.washingtonexaminer.com/affinion-group-faces-class-action-after-paying-out-claims-to-ags. Accessed March 12, 2019.
[3] 2015. rafaelw/mutation-summary: A JavaScript library that makes observing changes to the DOM easy. https://github.com/rafaelw/mutation-summary Accessed March 17, 2019.
[4] 2018. aboSamoor/polyglot: Multilingual text (NLP) processing toolkit. https://github.com/aboSamoor/polyglot Accessed March 12, 2019.
[5] 2018. Facebook has been collecting call history and SMS data from Android devices. https://www.theverge.com/2018/3/25/17160944/facebook-call-history-sms-data-collection-android. Accessed April 2, 2019.
[6] 2018. MDN. https://developer.mozilla.org/en-US/docs/Web/HTML/Block-level_elements Accessed March 12, 2019.
[7] 2018. Princeton Web Census Data Release. https://webtransparency.cs.princeton.edu/webcensus/data-release/. Accessed April 2, 2019.
[8] 2018. Selenium. https://selenium-python.readthedocs.io Accessed March 12, 2019.
[9] 2019. Alexa Top Sites - API Reference. https://docs.aws.amazon.com/AlexaTopSites/latest/ApiReferenceArticle.html Accessed March 12, 2019.
[10] 2019. Alexa Web Information Service. https://docs.aws.amazon.com/AlexaWebInfoService/latest/index.html Accessed March 12, 2019.
[11] 2019. Booster. https://boostertheme.com Accessed March 12, 2019.
[12] 2019. Fake it till you make it - Social Proof. https://www.boostplugin.com/fake-boosts. Accessed April 4, 2019.

[13] 2019. .har - Wikipedia. https://en.wikipedia.org/wiki/.har Accessed March 12, 2019.
[14] 2019. The hdbscan Clustering Library. https://hdbscan.readthedocs.io/en/latest/index.html Accessed March 15, 2019.
[15] 2019. Hotel booking sites forced to end misleading sales tactics. https://www.theguardian.com/business/2019/feb/06/hotel-booking-sites-forced-to-end-misleading-sales-tactics Accessed March 12, 2019.
[16] 2019. How To Pause Your Code With Breakpoints In Chrome DevTools | Tools for Web Developers | Google Developers. https://developers.google.com/web/tools/chrome-devtools/javascript/breakpoints#dom. Accessed April 2, 2019.
[17] 2019. Hurrify - Countdown Timer. https://apps.shopify.com/hurrify-countdown-timer Accessed March 12, 2019.
[18] 2019. MDN. https://developer.mozilla.org/en-US/docs/Web/API/MutationObserver Accessed March 12, 2019.
[19] 2019. Node.nodeType - Web APIs | MDN. https //developer.mozilla.org/en-US/docs/Web/API/Node/nodeType Accessed March 12, 2019.
[20] 2019. Promotional marketing: Closing dates. https://www.asa.org.uk/advice-online/promotional-marketing-closing-dates.html Accessed August 12, 2019.
[21] 2019. Senators Introduce Bipartisan Legislation to Ban Manipulative "Dark Patterns". https://www.fischer.senate.gov/public/index.cfm/2019/4/senators-introduce-bipartisan-legislation-to-ban-manipulative-dark-patterns. Accessed April 4, 2019.
[22] 2019. The top 500 sites on the web. https://www.alexa.com/topsites/category/Top/Shopping Accessed March 12, 2019.
[23] 2019. Webshrinker. https://www.webshrinker.com Accessed March 12, 2019.
[24] 2019. WooCommerce Notification | Boost Your Sales - Recent Sales Popup - Live Feed Sales - Upsells - WordPress plugin| WordPress.org. https://wordpress.org/plugins/woo-notification/. Accessed April 4, 2019.
[25] Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, and Claudia Diaz. 2014. The Web Never Forgets: Persistent Tracking Mechanisms in the Wild. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14)*. ACM, New York, NY, USA, 674–689. https://doi.org/10.1145/2660267.2660347
[26] AdBlock. 2019. AdBlock. https://adblockplus.org. Accessed April 4, 2019.
[27] Praveen Aggarwal and Rajiv Vaidyanathan. 2015. Use It Or Lose It: Time-Limited Promotions And Purchase Behavior. In *Proceedings of the 2002 Academy of Marketing Science (AMS) Annual Conference*, Harlan E. Spotts (Ed.). Springer International Publishing, Cham, 2–2.
[28] George Ainslie. 1975. Specious Reward: A Behavioral Theory of Impulsiveness and Impulse Control, Vol. 82. American Psychological Association, 463–496. https://doi.org/10.1037/h0076860
[29] Hal R Arkes and Peter Ayton. 1999. The sunk cost and Concorde effects: Are humans less rational than lower animals? *Psychological bulletin* 125, 5 (1999), 591.
[30] Steven Bird, Ewan Klein, and Edward Loper. 2009. *Natural Language Processing with Python* (1st ed.). O'Reilly Media, Inc.
[31] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies* 2016, 4 (2016), 237–254.
[32] Harry Brignull. 2018. Dark Patterns. https://darkpatterns.org/. Accessed March 12, 2019.
[33] Will Browne and Mike Swarbrick Jones. 2017. What works in e-commerce - a meta-analysis of 6700 online experiments. *Qubit Digital Ltd* (2017).
[34] Ryan Calo. 2013. Digital market manipulation. *Geo. Wash. L. Rev.* 82 (2013), 995.
[35] Ricardo J. G. B. Campello, Davoud Moulavi, and Joerg Sander. 2013. Density-Based Clustering Based on Hierarchical Density Estimates. In *Advances in Knowledge Discovery and Data Mining*, Jian Pei, Vincent S. Tseng, Longbing Cao, Hiroshi Motoda, and Guandong Xu (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 160–172.
[36] Shruthi Sai Chivukula, Chris Watkins, Lucca McKay, and Colin M. Gray. 2019. "Nothing Comes Before Profit": Asshole Design In the Wild. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (CHI EA '19)*. ACM, New York, NY, USA, Article LBW1314, 6 pages. https://doi.org/10.1145/3290607.3312863
[37] Robert B Cialdini. 2009. *Influence: Science and practice*. Vol. 4. Pearson education Boston.
[38] Gregory Conti and Edward Sobiesk. 2010. Malicious interface design: exploiting the user. In *Proceedings of the 19th international conference on World wide web*. ACM, 271–280.
[39] Biplab Deka, Zifeng Huang, Chad Franzen, Joshua Hibschman, Daniel Afergan, Yang Li, Jeffrey Nichols, and Ranjitha Kumar. 2017. Rico: A Mobile App Dataset for Building Data-Driven Design Applications. In *Proceedings of the 30th Annual ACM Symposium on User Interface Software and Technology (UIST '17)*. ACM, New York, NY, USA, 845–854. https://doi.org/10.1145/3126594.3126651
[40] Steven Englehardt and Arvind Narayanan. 2016. Online Tracking: A 1-million-site Measurement and Analysis. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. ACM, New York, NY, USA, 1388–1401. https://doi.org/10.1145/2976749.2978313

[41] Worldwide Retail Ecommerce Sales: Emarketer's Updated Estimates and Forecast Through 2019. 2019. Online Shopping and E-Commerce. https://www.emarketer.com/public_media/docs/eMarketer_eTailWest2016_Worldwide_ECommerce_Report.pdf Accessed March 12, 2019.
[42] European Parliament and Council of European Union. 2011. Directive 2011/83/EU. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0083. Accessed March 12, 2019.
[43] European Parliament and Council of European Union. 2011. Directive 2011/83/EU of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0083. Accessed March 12, 2019.
[44] European Parliament and Council of European Union. 2018. Consent under the GDPR: valid, freely given, specific, informed and active consent. https://www.i-scoop.eu/gdpr/consent-gdpr/. Accessed March 12, 2019.
[45] Federal Trade Commission. 1914. 15 U.S. Code §45. Unfair methods of competition unlawful; prevention by Commission. https://www.law.cornell.edu/uscode/text/15/45. Accessed March 12, 2019.
[46] Frobrukerrådet. 2018. Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy. (2018).
[47] Frobrukerrådet. 2018. New study: Google manipulates users into constant tracking. https://www.forbrukerradet.no/side/google-manipulates-users-into-constant-tracking. Accessed March 12, 2019.
[48] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 534, 14 pages. https://doi.org/10.1145/3173574.3174108
[49] Saul Greenberg, Sebastian Boring, Jo Vermeulen, and Jakub Dostal. 2014. Dark Patterns in Proxemic Interactions: A Critical Perspective. In *Proceedings of the 2014 Conference on Designing Interactive Systems (DIS '14)*. ACM, New York, NY, USA, 523–532. https://doi.org/10.1145/2598510.2598541
[50] Jon D Hanson and Douglas A Kysar. 1999. Taking behavioralism seriously: The problem of market manipulation. *NYUL Rev.* 74 (1999), 630.
[51] Martie G Haselton, Daniel Nettle, and Damian R Murray. 2015. The evolution of cognitive bias. *The handbook of evolutionary psychology* (2015), 1–20.
[52] Joel Huber, John W. Payne, and Christopher Puto. 1982. Adding Asymmetrically Dominated Alternatives: Violations of Regularity and the Similarity Hypothesis. *Journal of Consumer Research* 9, 1 (1982), 90–98. http://www.jstor.org/stable/2488940
[53] J. Jeffrey Inman and Leigh McAlister. 1994. Do Coupon Expiration Dates Affect Consumer Behavior? *Journal of Marketing Research* 31, 3 (1994), 423–428. http://www.jstor.org/stable/3152229
[54] Eric J. Johnson, Steven Bellman, and Gerald L. Lohse. 2002. Defaults, Framing and Privacy: Why Opting In-Opting Out1. *Marketing Letters* 13, 1 (01 Feb 2002), 5–15. https://doi.org/10.1023/A:1015044207315
[55] Jae Min Jung and James Kellaris. 2004. Cross-national differences in proneness to scarcity effects: The moderating roles of familiarity, uncertainty avoidance, and need for cognitive closure. *Psychology and Marketing* 21 (09 2004), 739 – 753. https://doi.org/10.1002/mar.20027
[56] Ranjitha Kumar, Arvind Satyanarayan, Cesar Torres, Maxine Lim, Salman Ahmad, Scott R. Klemmer, and Jerry O. Talton. 2013. Webzeitgeist: Design Mining the Web. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, New York, NY, USA, 3083–3092. https://doi.org/10.1145/2470654.2466420
[57] Chris Lewis. 2014. *Irresistible Apps: Motivational Design Patterns for Apps, Games, and Web-based Communities* (1st ed.). Apress, Berkely, CA, USA.
[58] Brian Lickel, Kostadin Kushlev, Victoria Savalei, Shashi Matta, and Toni Schmader. 2014. Shame and the motivation to change the self. *Emotion* 14, 6 (2014), 1049.
[59] Thomas F. Liu, Mark Craft, Jason Situ, Ersin Yumer, Radomir Mech, and Ranjitha Kumar. 2018. Learning Design Semantics for Mobile Apps. In *Proceedings of the 31st Annual ACM Symposium on User Interface Software and Technology (UIST '18)*. ACM, New York, NY, USA, 569–579. https://doi.org/10.1145/3242587.3242650
[60] Sheng Luo, Bin Gu, Xingbiao Wang, and Zhaoquan Zhou. 2018. Online Compulsive Buying Behavior: The Mediating Role of Self-control and Negative Emotions. In *Proceedings of the 2018 International Conference on Internet and e-Business*. ACM, 65–69.
[61] Xueming Luo. 2005. How Does Shopping With Others Influence Impulsive Purchasing? *Journal of Consumer Psychology* 15 (12 2005), 288–294. https://doi.org/10.1207/s15327663jcp1504_3
[62] Michael Lynn. 1991. Scarcity effects on value: A quantitative review of the commodity theory literature. *Psychology & Marketing* 8, 1 (1991), 43–57.
[63] Arunesh Mathur, Arvind Narayanan, and Marshini Chetty. 2018. Endorsements on Social Media: An Empirical Study of Affiliate Marketing Disclosures on YouTube and Pinterest. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 119 (Nov. 2018), 26 pages. https://doi.org/10.1145/3274388
[64] Luigi Mittone and Lucia Savadori. 2009. The scarcity bias. *Applied Psychology* 58, 3 (2009), 453–468.

[65] Carol Moser, Sarita Y. Schoenebeck, and Paul Resnick. 2019. Impulse Buying: Design Practices and Consumer Needs. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA, Article 242, 15 pages. https://doi.org/10.1145/3290605.3300472

[66] Mozilla. 2019. What Happened To Tracking Protection? https://support.mozilla.org/en-US/kb/tracking-protection-pbm. Accessed April 4, 2019.

[67] Dang Van Nhan. 2018. Beeketing eCommerce Success Community Public Group | Facebook. https://www.facebook.com/groups/beeketing.ecommerce.community/permalink/1691157507670306/. Accessed April 2, 2019.

[68] Nick Nikiforakis, Luca Invernizzi, Alexandros Kapravelos, Steven Van Acker, Wouter Joosen, Christopher Kruegel, Frank Piessens, and Giovanni Vigna. 2012. You Are What You Include: Large-scale Evaluation of Remote Javascript Inclusions. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS '12)*. ACM, New York, NY, USA, 736–747. https://doi.org/10.1145/2382196.2382274

[69] Chris Nodder. 2013. *Evil by design: Interaction design to lead us into temptation*. John Wiley & Sons.

[70] C. Whan Park, Sung Youl Jun, and Deborah J. MacInnis. 2000. Choosing What I Want versus Rejecting What I Do Not Want: An Application of Decision Framing to Product Option Choice Decisions. *Journal of Marketing Research* 37, 2 (2000), 187–202. http://www.jstor.org/stable/1558499

[71] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay. 2011. Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research* 12 (2011), 2825–2830.

[72] Steven Reiss. 2004. Multifaceted Nature of Intrinsic Motivation: The Theory of 16 Basic Desires. *Review of General Psychology* 8, 3 (2004), 179–193. https://doi.org/10.1037/1089-2680.8.3.179 arXiv:https://doi.org/10.1037/1089-2680.8.3.179

[73] Quirin Scheitle, Oliver Hohlfeld, Julien Gamba, Jonas Jelten, Torsten Zimmermann, Stephen D. Strowes, and Narseo Vallina-Rodriguez. 2018. A Long Way to the Top: Significance, Structure, and Stability of Internet Top Lists. In *Proceedings of the Internet Measurement Conference 2018 (IMC '18)*. ACM, New York, NY, USA, 478–493. https://doi.org/10.1145/3278532.3278574

[74] Natasha Dow Schüll. 2014. *Addiction by design: Machine gambling in Las Vegas*. Princeton University Press.

[75] Muzafer Sherif. 1936. The psychology of social norms. (1936).

[76] Ben Shuffer. 2018. Shopify Cracking Down On Fake Scarcity? https://medium.com/@benshaffer_83355/shopify-cracking-down-on-fake-scarcity-e1509b11cb75/. Accessed April 2, 2019.

[77] Daniel Susser, Beate Roessler, and Helen Nissenbaum. 2018. Online Manipulation: Hidden Influences in a Digital World. *Available at SSRN 3306006* (2018).

[78] Richard H. Thaler and Cass R. Sunstein. 2003. Libertarian Paternalism. *American Economic Review* 93, 2 (May 2003), 175–179. https://doi.org/10.1257/000282803321947001

[79] Amos Tversky and Daniel Kahneman. 1974. Judgment under uncertainty: Heuristics and biases. *Science* 185, 4157 (1974), 1124–1131.

[80] Amos Tversky and Daniel Kahneman. 1981. The framing of decisions and the psychology of choice. *Science* 211, 4481 (1981), 453–458. arXiv:http://science.sciencemag.org/content/211/4481/453.full.pdf http://science.sciencemag.org/content/211/4481/453

[81] Amos Tversky and Daniel Kahneman. 1989. Rational Choice and the Framing of Decisions. In *Multiple Criteria Decision Making and Risk Analysis Using Microcomputers*, Birsen Karpak and Stanley Zionts (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 81–126.

[82] WebKit. 2019. Intelligent Tracking Protection. https://webkit.org/blog/7675/intelligent-tracking-prevention. Accessed April 4, 2019.

[83] T. Martin Wilkinson. 2013. Nudging and manipulation. *Political Studies* 61, 2 (2013), 341–355.

[84] Bo Xiao and Izak Benbasat. 2011. Product-Related Deception in E-Commerce: A Theoretical Perspective. *MIS Quarterly* 35, 1 (2011), 169–195. http://www.jstor.org/stable/23043494

[85] José P Zagal, Staffan Björk, and Chris Lewis. 2013. Dark patterns in the design of games. In *Foundations of Digital Games 2013*.

[86] Fuzheng Zhang, Nicholas Jing Yuan, Kai Zheng, Defu Lian, Xing Xie, and Yong Rui. 2015. Mining consumer impulsivity from offline and online behavior. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 1281–1292.

A APPENDIX

Table 3. Confusion Matrices From Our Evaluation of Alexa's and Webshrinker's Website Classifiers.

		Alexa Prediction		Webshrinker Prediction	
		Not Shopping	Shopping	Not Shopping	Shopping
Truth	Not Shopping	442	1	423	20
	Shopping	53	4	10	47

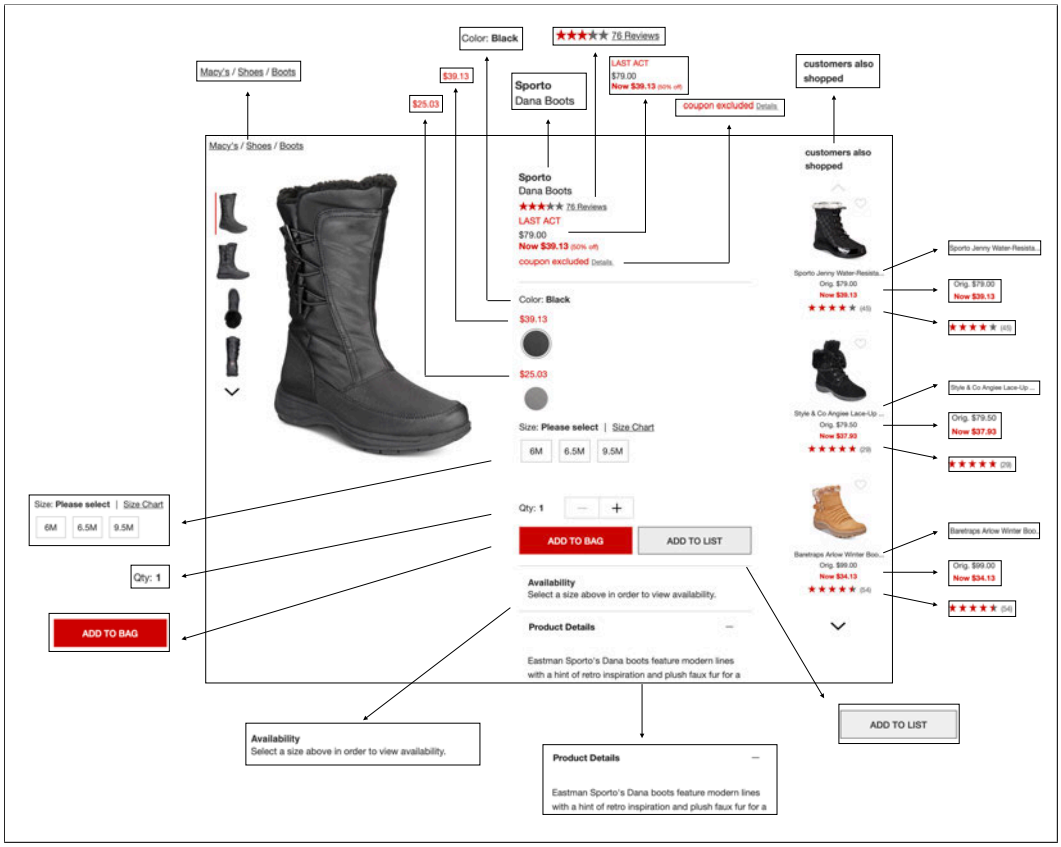


Fig. 11. An illustration of the page segmentation algorithm. The page is segmented into smaller meaningful "building blocks" or segments. Only segments containing text are recorded.

Algorithm 1 Page Segmentation

```
ignoredElements ← ['script', 'style', 'noscript', 'br', 'hr']
blockElements ← ['div', 'section', 'article', 'aside', 'nav', 'header', 'footer', 'main', 'form', 'fieldset', 'table']

function SEGMENTS(element)                                  ▷ Returns a list of segments
    if not element then
        return empty list
    end if
    tag ← element.tagName
    if tag in ignoredElements or element not visible or element not bigger than 1 pixel then
        return empty list
    end if
    if tag in blockElements then
        if element does not contain visible blockElements then
            if all of element's children in ignoredElements then
                return empty list
            else
                if element occupies more than 30% of the page then
                    return list of segments(child) for each child in element's children
                else
                    return [element]
                end if
            end if
        else if element contains text nodes then
            return [element]
        else
            return list of segments(child) for each child in element's children
        end if
    else
        if element has at least one child with tag in blockElements then
            return list of segments(child) for each child in element's children
        else
            if element occupies more than 30% of the page then
                return list of segments(child) for each child in element's children
            else
                return [element]
            end if
        end if
    end if
end function
```

Received April 2019; revised June 2019; accepted August 2019

From: Jen King
To: Privacy Regulations
Subject: CCPA Comments
Date: Tuesday, February 25, 2020 3:31:08 PM
Attachments: King_Li_CCPA_Feb_2020_Comments.pdf

Dear Ms. Kim,

please accept these comments for the CCPA Feb. 2020 comment period prepared by myself (Jennifer King, Stanford Law School) and Tianshi Li (Carnegie Mellon University). A PDF of the comments is attached.

Thanks,
Jen King

Jennifer King, Ph.D
Director of Consumer Privacy
Center for Internet and Society
Stanford Law School
[redacted]
https://cyberlaw.stanford.edu/about/people/jen-king

www.jenking.net/publications
Google Scholar profile: https://scholar.google.com/citations?user=O5jENBMAAAAJ&hl=en

Stanford Law School

Center for Internet and Society

Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610
Tel 650 723-5205
Fax 650 725-4086
cyberlaw.stanford.edu

February 25, 2020

To Whom It May Concern:

We are pleased to submit comments to the California Attorney General's office regarding the February 10th revision of the regulations for the California Consumer Privacy Act (CCPA). We make these comments on behalf of ourselves individually and provide our institutional affiliation for identification purposes only.

As researchers with expertise in information privacy and human-computer interaction, we share our concerns with aspects of the regulations as currently drafted, and offer suggestions we hope the AG's office will consider as you continue with this process.

Issue 1: The AG Should Not Adopt the Proposed Opt-Out Logo in the 2/10/20 Draft Regulations

In §999.306 (f)(1-3), the 2/10/20 version of the regulations include a proposal for the Opt-Out logo as required by the CCPA statute. Based on our expertise in human-computer interaction and design, we recommend the AG not adopt this design for the reasons we explicate below. Instead, the AG's office should either adopt the version recommended by the Carnegie Mellon (CMU) report[1], or alternatively, decline to adopt any logo for the final regulations at this time.

W243-1

1. Background

Per the statute, §1798.185(4)(C) calls "[f]or the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information." We presume the authors of the original ballot initiative (later statute) reasoned that the opt-out of sale provision was significant enough that they desired to elevate and call attention to this option as compared to the other rights conferred by the statute. While this goal is laudable, it unfortunately opens a Pandora's Box of complex and competing issues with respect to visual signifiers and information privacy.

As the CMU report references, there have been multiple attempts over the years to signal privacy risks and options to consumers through the development and use of icons, including a set developed at Dr. King's institution, the Center for Internet and Society at Stanford Law School[2]. Unfortunately, none of these efforts have gained traction, in part due to a lack of incentives and regulation, but also because of the difficulty with

[1] Cranor, et al., *Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA* (February 4, 2020). Posted to the CCPA website.
[2] Cranor *et al,* Appendix A (p. 40).

representing the often complex concepts the icons attempt to capture. For example, explaining the practice of third party ad targeting through an icon to those who are unfamiliar with the concept is extremely difficult at best. As the CMU report details, there are many opportunities for misunderstanding on the part of consumers who know little to nothing about these practices. Add to the challenge an existing universe of competing icons and other signifiers (*e.g.*, browser lock icons, e-commerce verified merchant badges, etc.), and the Do Not Sell logo becomes yet another new element in an already crowded universe competing for consumer attention. Thus, one must raise the question of whether any logo for Do Not Sell will effectively inform consumers of this new right, especially if there remains no budget or plan for public education about the CCPA informing them of its existence.

W243-1 (cont.)

2. The CMU Report Provides a Specific Recommendation Based on Credible Research

The CMU report provides a set of specific recommendations for the Do Not Sell logo based on a well-executed research study. The report calls for a "toggle" icon paired with a specific tagline ("Do Not Sell My Personal Information") to communicate the Do Not Sell right. Further, the report suggests a slightly different option to communicate the broader concept of privacy controls beyond Do Not Sell: the toggle icon paired with a "Privacy Options" tagline. We will not review this report in depth here, but we found the methods and analysis sound and the recommendations well-informed and appropriate. We do wish to highlight several findings from this report that are relevant to this discussion.

- *Privacy Options vs. Do Not Sell*: The report raises an issue which we think points to the need to consider a different option than what the statute requires: to not adopt any logo. While the report presents a clear path to follow to inform consumers about the Do Not Sell right, the report's discussion of a broader possibility, that of giving consumers a standardized method for locating privacy choices (beyond, but including, Do Not Sell), highlights an important need within the national (and even international) consumer privacy policy sphere to move beyond the "Privacy Policy" link (as mandated today by Cal-OPPA) and provide U.S. consumers with a discoverable and consistent means to inform them of where to find privacy-related information on any website or mobile app. The existing notice and consent framework, including privacy policies, privacy controls, and the methods in which we inform consumers of their existence, is in dire need of reform. This is a bigger problem than CCPA and Do Not Sell, and one that should be approached methodically, rather than piecemeal. To that end, we would suggest not adopting a Do Not Sell logo at this juncture in favor of pursuing the opportunity for comprehensive reform at either the state or federal level. That said, if the requirement to adopt a logo is read as absolute, then we suggest the toggle icon + Do Not Sell My Personal Information version as recommended by the CMU report.

- *Public Education:* As the CMU report argues, and as did Dr. King in her 2019 comments regarding the CCPA, we cannot expect consumers to broadly learn about and exercise these rights without a well-funded plan for public education. The development of a logo is no substitute for this problem. This lack of public education will particularly affect Californians living at the economic and social margins in our state. Absent a concerted public education effort, the Californians who do learn about the CCPA and their new rights will predominantly be those with access to media resources and education. Undoubtedly this will mean that the law will have a disparate impact, favoring those with higher incomes, education levels, technical literacy, and English proficiency.

- *Standardizing Do Not Sell/Deletion/Access Requests:* The CMU report, on page 34, suggests a standardized format for Do Not Sell requests that ensures they are simple, straightforward, and consistent. We endorse this approach and would suggest it also be considered for deletion and access

requests as appropriate. Since January 1st, Dr. King has been informally tracking CCPA notices and have observed a considerable diversity in terms of format, language, and even location on webpages. Some notices are even argumentative in their language, disputing the meaning of "sale" and suggesting the company is grudgingly complying with the law. Notices should not be a platform for arguing about the law. In order to provide consistency for consumers, the AG should require, or strongly suggest, the adoption of standardized notices for these new rights.

3. The AG Should **Not** Adopt the Logo In the 2/10/2020 Version of the Regulations

The logo included in the 2/10/2020 version of the regulations is problematic and should not be adopted. It is deficient in the following ways:

- *Confusing Design*: While the CMU toggle uses visual elements that are similar to an interactive button but do not replicate an existing design, the 2/10 logo appears to be based closely on the design of an Apple iOS toggle user interface element[3]. Thus, it raises the possibility for confusion among the public that the logo is an actual, interactive switch (rather than a logo or icon) that denotes a current system state. The CMU report raised the possibility of risk with their own toggle icon on page 31 of their report, though they found actual confusion to be very low[4]. The 2/10 logo inherently has this problem: in a very informal survey Dr. King conducted[5], when she showed individuals the 2/10 logo, all assumed it was an actual functioning button that indicated the current system state (set to Do Not Sell == yes). All assumed they did not have to take any action at all because the system default was set to Do Not Sell. In addition, according to general UI design guidelines[6], toggle switches should have an immediate effect and not require further "save" or "submit" action. Users may be confused if they try to click on the icon but do not see any change in the user interface. This may reduce the discoverability of the actual controls. W243-1 (cont.)

- *Color*: The 2/10 logo is red, which contributes to the confusion over its function. The individuals Dr. King asked about the logo assumed it was red because the button state was "on" (and that if Do Not Sell were inactivated, the button would be green or grey). Red is also a color generally reserved for critical errors in user interfaces; even using a red version of the proposed CMU logo would be problematic.

- *Dependency on a specific platform:* The toggle icon is a popular way to express the meaning of "control" due to its compatibility with mobile applications, wherein the primary interaction media is tactile. Therefore, the preferences of the toggle icon over other options may be a result of today's proliferation of mobile devices. However, the emergence of new consumer computing devices like virtual reality, augmented reality, and Internet of Things, may call for different interaction paradigms in the future, and affect the familiarity and interpretation of icons of the general public. The recommendation of an icon design tailored to a specific platform concerns us that future legislative updates may not be frequent enough to adapt to changes of perception. And even if the icons are updated in a timely manner, it can take a considerable amount of effort to make sure all websites and apps are also subsequently updated.

[3] https://developer.apple.com/design/human-interface-guidelines/ios/controls/switches/
[4] "[T]he *toggle* icon has a slight possibility of being viewed as an actual control (rather than a static icon) to give websites permission to sell data, which could deter users from interacting with it."
[5] Consisting of asking fewer than 10 people I personally know to look at the proposed logo and tell me what they thought its purpose was and how it functioned. This is not a scientific survey; however, within usability testing circles small-scale tests are a valid way of identifying critical user interface problems.
[6] https://www.nngroup.com/articles/toggle-switch-guidelines/

- *Source?*: Should the AG's office persist in recommending this logo, the source of the design, and any information related to its development and testing should be released in order to give researchers the opportunity to audit the development process. If the AG is in possession of evidence suggesting that this option is a better choice than what was suggested by CMU, then we should be able to review that evidence. In sum, no logo design should be adopted without user testing and research, and the results of those tests should be made public.

W243-1 (cont.)

In sum, we strongly recommend that the AG adopt the toggle design with tagline that was recommended by CMU and do not adopt the version in the 2/10 regulations. However, we also suggest that there is a strong rationale for not adopting a logo at this juncture.

Issue 2: Mobile Notices

We are pleased to see the addition of §999.304(d)(4) to the CCPA draft regulations. Given the challenges of presenting notices on mobile devices, more clarity is welcome in this area. We would like to offer the following suggestions to further clarify this section.

1. Developer Engagement and Platform Involvement

W243-2

The CCPA is targeted at companies that meet a threshold based on annual gross revenues or the centrality of information sales to the business based on either quantity or percentage of revenue. While these requirements likely exclude many small-scale mobile application developers, some will undoubtedly be subject to the law. The proposed mobile notice requirements appear to directly target large mobile developers as a major audience, as they propose specific language, icon, notice format (e.g. just-in-time notice) recommendations. These proposals have two requirements to make the law effective. First, developers should have sufficient knowledge and incentives to comply with the law. Next, an organization should be responsible to educate developers and audit their practices. A recent research study of privacy-related questions on software development question & answer sites showed that platform requirements are a more frequently mentioned driver (46% of sampled posts on the website Stack Overflow) than laws and regulations (only 2% of sampled posts)[7]. Platforms serve as an important force to drive developers to comply with legal requirements, and the CCPA can take advantage of their capabilities by making the role of platforms more explicit in the law. For example, platform app stores (e.g., mobile app stores, browser plugin stores, etc.) could take proactive steps towards detecting apps that lack a privacy policy on their app store pages and remind developers that these notices are required for California consumers of their apps, or even remove non-compliant apps from their app stores.

2. Specifying The Criteria For "Just-In-Time" Notices

W243-3

The current regulation needs more specificity regarding the triggers for the just-in-time notice described … §999.304(d)(4). In part, this could be determined by more clearly explicating the purpose and limitations of the just-in-time notice: is it only for "personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect[8]," meaning any form of data collected from the consumer that is not demonstrably linked to the core purpose of the app? Would this notice apply only to the app developer, or to any

[7] Tahaei, Mohammad, et al. "Understanding Privacy-Related Questions on Stack Overflow." Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 2020.

[8] While there is certainly extant research that maps the contours of what users expect from mobile experiences in order to define more precisely what consumers would not reasonably expect in a particular context, it is worth raising the question as to whether it makes sense to also define this requirement similarly to the GDPR's legitimate interest requirement. See: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504.

third-party library the app developer incorporates into the app that collects user information for ad targeting or other purposes outside the core functionality of the app? If it applied to both, who would ultimately be responsible for the notice? Further, would this notice appear every time a user opens an app, or just the first time?

The AG should be cautious in moving forward with this requirement to ensure that it does not inadvertently create a CCPA-version of the EU e-Privacy cookie notice, which has been the target of substantial criticism for subjecting EU internet users with routine cookie notices that are largely ineffective at offering users with any substantive choices, habituating the public to simply clicking "I Accept.[9]" However, the fact that it will not be present on every app may ensure enough novelty to avoid this issue, at least in part. That said, the inclusion of this new requirement raises the issue as to why only apps that are subject to the CCPA are targeted for this requirement, given that informing consumers of any app collection of personal information that is outside an app's core functionality is important for all app users to know.

W243-3 (cont.)

In order to create a consistent user experience, platform providers (e.g., Apple for iOS, Google for Android) could implement the design and presentation (based on public input/feedback) of just-in-time privacy notices and their subsequent choices (e.g., selecting Do Not Sell) by providing a centralized interface, also known as a "native" user interface, that developers cannot change. Further, platform providers could provide developers with methods to specify the moments their app collects information from its users in a machine-readable format. Information provided in this way should be treated equally to information in privacy policies, for which developers should be held accountable for its accuracy.

In sum, this new provision could be an effective tool in raising consumer awareness about information collection in excess of what apps require for functionality. However, the existing language needs more specificity regarding the purpose of the notice and aspects of its functionality.

Issue 3: General Issues with CCPA Notices

The 2/10 version of the regulations raise several issues around notices that we think may require some additional clarification. We present them here in no specific order.

1. Providing New Notices

W243-4

Section 999.304(d)(6) states that: "A business shall not collect categories of personal information other tha those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection." In response, we ask whether businesses will be required to inform consumers who have already viewed or consented to a previous notice. Will consumers be required to re-consent or acknowledge the new terms of collection?

2. CCPA and Cal-OPPA

W243-5

Sections 999.305(a)(2)(a-d) lay out several rules regarding how companies must provide CCPA notices, wh §999.308(a) provides guidelines for privacy policies. We ask whether these requirements will govern all privacy policies for California consumers, or only those companies subject to the CCPA? This regulation appears to

[9] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (*CCS '19*). Association for Computing Machinery, New York, NY, USA, 973–990. DOI:https://doi.org/10.1145/3319535.3354212

require that businesses with existing privacy policies that are now subject to the CCPA will also have to updat their privacy policies to meet these requirements. Given that Cal-OPPA provides no requirements to businesses about the clarity of the language in a privacy policy, this appears to be a new requirement that may benefit consumers. Furthermore, §999.308(b) appears to conflict with Cal-OPPA regarding the proscription of the precise wording of the "privacy policy" link itself ("The privacy policy shall be posted online through a conspicuous link using the word 'privacy,' on the business's website homepage or on the download or landing page of a mobile application.") Will the CCPA requirements preempt those of Cal-OPPA? If yes, this opens the possibility to companies exploring other options for privacy policy links beyond "privacy policy," such as the "Privacy Options" language recommended by the CMU report. If this is the case, we would caution the AG to be specific in explicating exactly what terms can be used to avoid companies entitling the links with terms such as "Privacy Benefits" or "Privacy Choices" when the "benefits" and "options" available to them are fictional or lack substantive choice.

W243-6

3. Notices to Minors

Sections 999.331 and 999.332 include directives regarding notices to minors. As currently written, these sections do not include any language that requires companies to produce notices for minors that are written at a comprehension level using language that children can understand. Without such a requirement, we are likely to see notices written for well-educated adults that are beyond the grasp of children to understand. To that end, we recommend the AG's office review the Age Appropriate Design Code recently drafted by the U.K. Information Commissioner's Office. In particular, we recommend standard #4:

W243-7

- **"**Transparency**:** The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated."[10]

Our concern is that without such a requirement, notices to minors will be ineffective. Requiring companies to both write notices at a level of understanding for minors, as well as potentially including links to content educating minors about data privacy and related issues, both creates an ineffective regulation as well as a missed opportunity to educate children about data privacy and data protection.

Thank you for the opportunity to submit these comments.

Sincerely,

Dr. Jennifer King (via email)
Director of Consumer Privacy
Center for Internet and Society, Stanford Law School

Tianshi Li (via email)
Ph.D. Student
Human-Computer Interaction Institute, Carnegie Mellon University

[10] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/

Privacy Regulations

From: Robert Rutkowski [redacted]
Sent: Tuesday, February 25, 2020 3:27 PM
To: Xavier Becerra; Privacy Regulations
Subject: Proposed CCPA Regulations

Xavier Becerra, Attorney General
Attorney General's Office
California Department of Justice
Attn: Public Inquiry Unit
P.O. Box 944255
1300 I Street, Suite 1740
Sacramento, CA 94244-2550
xavier.becerra@doj.ca.gov, PrivacyRegulations@doj.ca.gov
Phone: 916-445-9555
Fax: 916-323-5341

Re: Proposed CCPA Regulations

Dear Attorney General:

Today, a coalition of privacy advocates filed comments regarding its ongoing rulemaking process for the California Consumer Privacy Act (CCPA). The CCPA was passed in 2018, and took effect on January 1, 2020.
Later this year, regulations will be finalize that dictate how exactly the law will be enforced.

Last time they weighed in, they called the initial proposed regulations a "good step forward" but encouraged them to go further. Now, they are disappointed that the latest proposed regulations are, compared to the AG's initial proposal, largely a step backwards for privacy.

To start, the modified regulations improperly reduce the scope of the CCPA by trying to carve out certain identifiers (such as IP addresses) from the definition of "personal information." This classifies potentially sensitive information as outside the law's reach—and denies Californians the right to access, delete, or opt out of the sale of that information. W244-1

Furthermore, the new regulations make it harder for consumers to exercise their right to opt out of the sale of their personal information. The proposed opt-out icon, which businesses will be required to display on their websites, is confusing; independent research has shown that many users don't understand what it means. W244-2
Worse, the new regulations provide that user-friendly, automatic controls like Do Not Track (DNT) cannot be used to opt out of data sale.
Today, millions of users around the world use DNT to signal their clear intent to opt out of the collection, misuse, sharing, and sale of their data. Until now, few companies have chosen to honor that intent, but the CCPA gives user requests to opt-out of data sale the force of law. The AG should make sure that businesses treat well-established signals like DNT as an opt-out from sale of their data. W244-3

The coalition letter details a number of other changes to the original draft regulations that reduce consumer protections. Please reconsider these changes and make sure CCPA does what it's supposed to protect Californians' privacy.

Yours sincerely,
Robert E. Rutkowski

cc:
Representative Steny Hoyer
House Majority Leader
Legislative Correspondence Team
1705 Longworth House Office Building
Washington DC 20515
Office: (202) 225-4131
Fax: (202) 225-4300
https://urldefense.proofpoint.com/v2/url?u=https-3A__www.majorityleader.gov_content_email-2Dwhip&d=DwIDaQ&c=uASjV29gZuJt5_5J5CPRuQ&r=kXcUIWCJFJC3Y7A6WPl5oNx0wEUzL_7MxjOspe9bxxI&m=WDlQHhhXXKsmNm8iJzsnNxuoG1_ns4k8ILd31t9LMMM&s=5sC975R9RfNo-i_pqbo3rIqFiB-dr9RQdH4e3poZpMQ&e=

[redacted]
P/F [redacted]
E-mail [redacted]

Re: Privacy advocate coalition letter:
https://urldefense.proofpoint.com/v2/url?u=https-3A__www.eff.org_document_ccpa-2Dcomments-2Dattorney-2Dgenerals-2Doffice-2Dcalifornia-2D2252020&d=DwIDaQ&c=uASjV29gZuJt5_5J5CPRuQ&r=kXcUIWCJFJC3Y7A6WPl5oNx0wEUzL_7MxjOspe9bxxI&m=WDlQHhhXXKsmNm8iJzsnNxuoG1_ns4k8ILd31t9LMMM&s=_of_fCTUtNcIO7M3ANOsdK8WpqTESUfmP2dzt-fqC3Y&e=

From: [redacted]
To: Privacy Regulations
Subject: Comments on Modified Regulations - CCPA
Date: Tuesday, February 25, 2020 3:26:12 PM
Attachments: myLetter.pdf

February 25, 2020

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

RE: Comments on Modified Regulations - CCPA

Dear Ms. Kim,

I am writing on behalf of the California and Nevada Credit Union Leagues (Leagues), one of the largest state trade associations for credit unions in the United States, representing the interests of approximately 250 credit unions and their more than 11 million members/consumers.

On June 28, 2018, then Governor Jerry Brown signed into law Assembly Bill 375 which enacted the California Consumer Privacy Act of 2018 (CCPA). As a sweeping data privacy law, CCPA gives California consumers significant expanded rights as to the collection and use of their personal information. California Attorney General Xavier Becerra released proposed regulations governing compliance with the CCPA on October 11, 2019. The Attorney General has now issued modified regulations in response to comments received and/or to clarify and conform the proposed regulations to existing law. The Leagues support several of the modifications, but we still have significant concerns on several issues. We respectfully offer the following comments.

The Credit Union Difference

The Leagues support the spirit of the law; however, it is important the Attorney General understand the credit union difference. Credit unions exist for the financial benefit of their member-owners, but they are driven by the philosophy of people-helping-people.

Credit unions are member-owned, democratically governed, not-for-profit cooperatives whose purpose is to promote thrift and improve access to credit for their member-owners, particularly those of modest means. As not-for-profit entities, credit union earnings are passed on to their member-owners in the forms of reduced fees, higher savings rates, and lower loan rates.

The credit union structure is vastly different than for-profit entities. Consumer personal information collected by credit unions is the personal information of their member-owner consumers in order to provide them with the products and services they desire. In the case of credit unions, "owners" are not proprietors or shareholders in a business whose only goal is that the business maximize profits. Instead, they are a member of a not-for-profit cooperative.

Credit unions are the original consumer financial protection advocates. In addition, as insured depository institutions, credit unions already comply with a plethora of data privacy and security requirements, including the federal Gramm-Leach-Bliley Act (Public Law 106-102) and its implementing regulations, the California Financial Information Privacy Act (Cal. Fin. Code §4050, et seq.), and the National Credit Union Administration's (NCUA's) data security regulations (12 CFR

Part 748 and its Appendixes).

Definition of a Business

We continue to call on the Attorney General to clarify the definition of a business. The modified regulations do not define or further clarify the statute's definition of a business. We strongly recommend the final regulations clarify both the threshold criteria and the phrase "doing business in California."

Thresholds

Part of the definition of a business is that it satisfies one or more of the following thresholds:

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

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

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

The meaning of "receives for the business's commercial purposes" under threshold (B) is confusing and should be clarified.

The application of threshold (B) to the personal information of 50,000 or more "consumers, households, or devices" is also confusing. A consumer, as defined in the CCPA is a natural person California resident. Is the rest of the threshold then related to households and devices of natural person California residents?

W245-1

Doing Business in CA

Another part of the definition of a business is that the entity "does business in the State of California." There is no clear definition under the CCPA or the proposed or modified regulations on what it means to "do business" in the State of California. Clarification is needed.

"Doing business" in a state should mean something more than isolated or incidental transactions. There should be a defined standard that contemplates repeated and successive transactions that clearly indicates a pattern or practice of doing business with California consumers, and not one-time or occasional transactions.

W245-2

Effective and Enforcement Dates

The CCPA became effective January 1, 2020. However, the proposed implementing regulations were not issued until October 11, 2019, and these modified proposed regulations have a comment deadline of February 25, 2020. Given how general the statute is and how detailed the modified proposed regulations are, the CCPA effective date should be extended.

Covered businesses should have adequate time to understand the requirements of the statute as well as the final regulations prior to designing and implementing comprehensive compliance solutions. The Leagues recommend the Attorney General and Governor delay the statute's effective date by two years, until Jan. 1, 2022. Accordingly, the enforcement date should also be delayed until July 1, 2022.

Barring a delay in the effective date of the statute, then we recommend the Attorney General delay enforcement until at least six months after publication of final regulations.

W245-3

GLBA and CFIPA Exemptions

There is significant confusion regarding the exemption for personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (GLBA) or the California Financial Information Privacy Act (CFIPA). We are disappointed neither the proposed nor modified regulations clarify this exemption.

The confusion arises because the CCPA uses terms that are inconsistent with the GLBA and CFIPA. The GLBA and CFIPA both use the terms "nonpublic personal information" and define that term to mean "personally identifiable financial information." W245-4

The CCPA uses the term "personal information," which is defined in Calif. Civil Code 1798.145(o) and is much broader than the GLBA/CFIPA's definition of "nonpublic personal information."

In addition, 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.

Because of the inconsistent terminology, the exemption provided in Calif. Civil Code 1798.145(e) is unclear and can be interpreted several ways. It is essential that the Attorney General provide clarification in the final regulations.

Model Notices Needed

The CCPA and proposed regulations create several notice requirements, including: Notice at or Before Collection, Right to Opt-Out, Notice of Financial Incentives, and updated Privacy Notices. In addition, the proposed regulations require specific responses to Requests to Know and Requests to Delete.

For all required notices, the proposed and modified regulations require the notices be easy to read and understandable by the average consumer and provide some standards to achieve that. This direction is subjective and does not contemplate a method or metric to assess the readability. W245-5

Since all businesses need to provide the required notices, uniform, model notices would help ensure consumer's understanding of the notices, simplify the requirements for businesses, and create an objective review on whether a business' notices meet the required standards.

We are disappointed neither the proposed nor modified regulations provide model notices. The Leagues strongly recommend the Attorney General draft proposed model notices for public comment and then include a safe harbor in the final regulations for the use of notices substantially similar to the model notices.

Other Observations

Many areas in the proposed and modified regulations exceed the requirements in the statute—requiring more detailed levels of explanation to the consumer, written confirmations beyond what the statute indicated, and additional steps.

While the Attorney General was given broad statutory authority to establish rules and procedures to implement and further the purposes of the CCPA, some of these additional proposed requirements create unnecessary burden on businesses and should be reconsidered.

§ 999.305. Notice at Collection

- The modified regulations provide that if a business intends to use a consumer's personal information for a purpose materially different than what was previously disclosed in the Notice W245-6

at Collection, the business must directly notify the consumer of the new use and obtain "explicit consent" from the consumer to use their personal information for this new purpose. [999.305(a)(5)]

This is an improvement over the proposed regulations which required this process if the business intended to use the personal information for any other purpose. However, this still exceeds the statutory requirement and creates a new opt-in requirement. The Leagues recommend replacing this requirement with a new notice to the consumer along with a 30-day opportunity to opt-out. Under this revised process, personal information of the consumer may not be disclosed for the new purpose unless the updated notice is provided, the consumer is given 30 days to opt-out, and the consumer does not opt out.

W245-6 (cont.)

§ 999.306. Notice of Right to Opt-Out

- The modified regulations amend the purpose statement of the Notice of Right to Opt-Out, removing the reference to the future sell of information [§999.306(a)]. Also, there is a related modification providing that the Notice of Right to Opt-Out is not required if the business does not sell personal information [999.306(d)]. The Leagues support these amendments in that the notice should only reflect current practices.

W245-7

- The modified regulations provide that a business shall not sell the personal information it collected during the time the business did not have a Notice of Right to Opt-Out posted unless it obtains the affirmative authorization of the consumer. [§999.306(e)]

  This modifies the proposed regulations that previously stated in this scenario the consumer is deemed to have opted-out. However, it is unclear as to the start date for the information collected prior to the Notice of Right to Opt-Out being posted. For example, is this for information collected Jan. 1, 2020 or later (the statute's effective date) and before the notice is posted, or some other start date? The Leagues recommend the final regulations clarify this section.

W245-8

Financial Incentives - §999.301, § 999.307, §999.337

- Clarity is needed regarding "financial incentive." There are inconsistencies between the statute and the proposed and modified regulations. The CCPA allows businesses to offer financial incentives for the collection, sale, or deletion of personal information, CA Civil Code 1798.125(b).

  However, the definition of "financial incentive" in the proposed and modified regulations, §999.301(j), is related to the disclosure, deletion, or sale of personal information — "collection" is not included and "disclosure" is added. "Disclosure' is too broad of a term as financial incentives are specific to the collection, sale or deletion of personal information. Further, in determining the value of consumer data, the proposed and modified regulations, §999.337(a), provide a list of considerations from which businesses are required to consider one or more of the items. These items include the sale, collection, deletion and retention of personal information — "retention" is not part of the statute.

  For clarity purposes, the Leagues recommend the final regulations be consistent throughout and with the statute.

W245-9

W245-10

- The modified regulations, 999.307(b)(5), require the notice of financial incentive include an explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including: (a) a good-faith estimate of the value of the consumer's data; and (b) a description of the method the business used to calculate the value.

  This requires disclosure of additional information not required in the CCPA and creates additional burden. The statute requires the incentive be directly related to the value provided to the business and that the business notify the consumer of the material terms of the incentive

W245-11

program. The statute does not require businesses to disclose how they calculate the value. We recommend removing the requirement to disclose a description of the value calculation method. W245-11 (cont.)

- In addition, clarity is needed regarding the definition of "value." The modified regulations provide that the "Value of the consumer's data" means the value provided to the business by the consumer's data as calculated under section 999.337 (discussed above). W245-12

  The Leagues request the final regulations clarify whether or not the definition of "value" includes non-financial or intangible values, and we strongly recommend that it does not.

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

- The CCPA requires businesses make available to consumers two or more designated methods for submitting Requests to Know. Except, if a business operates exclusively online and has a direct relationship with a consumer from whom it collects PI, then it is only required to provide an email address for submitting Requests to Know. All other businesses must provide two or more methods for submitting Requests to Know, including, at a minimum, a toll-free telephone number. W245-13

  The modified regulations remove the requirement that if a business operates a website, they must also provide an interactive web form as one of two the designated methods. [§999.312(a)]

  There is some confusion regarding this modification and how it conforms to the statute. The CCPA (CA Civil Code 1798.130(a)(1)(B)) requires businesses that maintain an internet website make the internet website available to consumers to submit Requests to Know. The Leagues ask for clarity regarding this modification.

- The proposed regulations required businesses to use a two-step process for online Requests to Delete where the consumer must first, clearly submit the Request to Delete and then second, separately confirm that they want their personal information deleted. The Leagues opposed this as this requirement is not in the statute and may not be practicable in execution. We support the modified regulations that now make the two-step process optional. [999.312(d)] W245-14

§ 999.313 Responding to Requests to Know and Requests to Delete

- The proposed regulations required businesses to describe the process they will use to verify a consumer's Request to Know/Delete, including any information the consumer must provide. W245-15

  The League opposed this requirement as describing the process the business will use to verify the consumer's request adds an additional burden, possibly discloses proprietary information, and adds little value to the consumer. We support the modified regulations that now only require a general description. [§999.313(a), §999.308(c)(1),(2)]

- The modified regulations require businesses to respond to Requests to Know and Requests to Delete within 45 calendar days. The 45-day period begins on the day the business receives the request, regardless of time required to verify the request. The modified regulations permit an additional 45 calendar days to respond, for a maximum total of 90 calendar days. [999.313(b)] W245-16

  However, the CCPA, Calif. Civil Code 1798.145(g)(1), allows up to 90 additional days where necessary, taking into account the complexity and number of the requests.

  Given that the statute contemplates complex and/or high volume of requests, and the 45-day period begins before the requests are verified, we are concerned the regulations allow less time than permitted by the statute. We recommend the regulations allow the 90-day extension permitted by statute.

- The proposed regulations stated a business *shall not* provide a consumer with specific pieces W245-17

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. While this exception was welcome, the Leagues were concerned that it was subjective and created liability risk if a consumer claims a business "should have known" of the disclosure risks. We support the modified regulations that provide a business is not required to search for personal information if certain conditions are met. [§999.313(c)(3)]

W245-17 (cont.)

- Previously, the proposed regulations required, *for each category* of personal information collected, the business 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 Leagues opposed this as it significantly expands the policy beyond what is contemplated in the statute by requiring the information "for each category" of personal information. This would have required more complex, detailed disclosures that would likely not be clear or helpful to consumers.

  We support the modified regulations that no longer require businesses to link categories of personal information to sources and business purpose(s). [§999.313(c)(10); deleted 999.308(c)(1)(d)(1)]

W245-18

- For a Request to Delete, the proposed regulations required that if a business cannot verify the identity of the requestor, the business may deny the Request to Delete, inform the requestor that their identity cannot be verified, and treat the request as a Request to Opt-Out of Sale.

  The modified regulations change the automatic opt-out to instead require the business to ask the consumer if they would like to opt-out and provide them with the contents of, or a link to, the Notice of Right to Opt-Out. [999.313(d)(1)]

  We question this requirement to provide an unverified requestor an opportunity to opt-out. We recognize that generally a request to opt-out need not be a verifiable consumer request. However, §999.315(h) permits a business to deny an opt-out request if it has a good-faith, reasonable, and documented belief that an opt-out request is fraudulent. We believe that when a business has attempted to, and could not, verify the identity of a requestor then the business has a reasonable belief of fraud. We recommend this section be amended to simply require the business to inform the consumer that their Request to Delete is denied because their identity cannot be verified.

W245-19

- In cases where a business denies a consumer's Request to Delete, the modified regulations require the business do all the following:

  a. Inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including *any* conflict with federal or state law, or exception to the CCPA, unless prohibited from doing so by law;

  b. Delete the consumer's personal information that is not subject to the exception; and

  c. Not use the consumer's personal information retained for any other purpose than provided for by *that* exception. [999.313(d)(6)]

  Subparagraph (a) was slightly amended in the modified regulations; however, our concerns remain. It adds a specific response requirement not included in the statute. Further, there may be multiple statutory and regulatory exceptions that apply (e.g., GLBA, Bank Secrecy Act, USA Patriot Act, Home Mortgage Disclosure Act, etc.). One might interpret this section to prohibit further use of the information except for the stated exception provided to the consumer. This subparagraph should be amended to permit an example of one or more statutory or regulatory exceptions.

W245-20

Subparagraph (c) was not amended in the modified regulations, and our concerns remain. If a business lawfully has the consumer's personal information under one or more statutory or regulatory exceptions, then the business should be able to use the personal information. This subparagraph should be deleted or amended to not permit the sale of the personal information except as provided for under any exceptions.

W245-20 (cont.)

§ 999.315 Requests to Opt-Out

- The proposed regulations provided that if a business collects personal information from consumers online, the business shall treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted for that browser or device, or, if known, for the consumer.

  The modified regulations mitigated concerns with this requirement to a degree. The modified regulations provide that any privacy control developed in accordance with these regulations clearly communicate the consumer's intent to opt-out and require the consumer affirmatively select their choice to opt-out. Further, if a global privacy control conflicts with the business's specific privacy settings, the business must respect the global privacy control but may notify the consumer of the conflict and confirm their choice. [999.315(d)]

  These requirements exceed the original statute and may still create significant compliance and technological challenges. Since businesses will be required to provide two or more designated methods for submitting requests to opt-out, this additional, onerous method should be deleted. Further, it is unclear whether this imposes obligations for businesses to adopt new technology developed in accordance with these regulations.

W245-21

- The modified regulations require a business to act upon a request to opt-out as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. [§999.315(e)]

  This adds a response timing obligation that is not specified in the original statute and is more prescriptive than the federal GLBA requirements. The Leagues recommend, for consistency purposes, that the regulations follow the GLBA regulations at 12 CFR 1016.7(g)which states, "You must comply with a consumer's opt out direction as soon as reasonably practicable after you receive it."

W245-22

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

- The proposed and modified regulations require that an opt-in to the sale of personal information use a two-step opt-in process whereby the consumer must first, clearly submit the request to delete and then second, separately confirm that they want their personal information deleted.

  This requirement is not in the statute, may not be practicable in execution, and the modified regulations lack compliance guidance. The Leagues recommend removing the two-step process requirement.

W245-23

§999.323. General Rule Regarding Verification

- Clarity is needed regarding verification of persons making a Request to Know or a Request to Delete when the requestor's identity may be verifiable in one system maintained by the business, but not verifiable in another. For example, a credit union may have different operating systems or platforms for various product types, and it will be necessary to search multiple systems. One system may have the data that allows verification (e.g., name, address, phone), while a second system may not (e.g., phone number is different). The Leagues recommend the final regulations provide clarity regarding a business's response requirements when multiple systems are maintained by the business.

W245-24

Conclusion

The Leagues support the spirit of the law, but we have significant concerns with the practicality and implementation of the proposed and modified regulations.

We thank you for the opportunity to comment. We trust you will carefully consider our views and recommendations. If you have any questions regarding our comments, please contact me.

Sincerely,

Diana R. Dykstra
President and CEO
California and Nevada Credit Union Leagues

cc: CCUL

From: Cynthia Pantazis
To: Privacy Regulations
Subject: Google comments to the modifications of the proposed CCPA regulations
Date: Tuesday, February 25, 2020 3:24:52 PM
Attachments: Google Comments on CA AG"s Updated Proposed CCPA Regulations.pdf

Dear Ms. Kim: Attached Please find Google's comments in response to the modifications of the proposed CCPA regulations.

Sincerely,

Cynthia Pantazis

Cynthia Pantazis
Director, State Policy
Google LLC
25 Massachusetts Avenue, NW
Washington, DC 20001
[redacted] (O)
(C)

By Email

February 25, 2020

Ms. Lisa B. Kim
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, California 90013

Dear Ms. Kim:

Please find below Google's comments on the Attorney General's proposed modifications to the draft California Consumer Privacy Act ("CCPA") regulations. We thank the Attorney General and staff for the time and effort to consider public comments and provide clarity to the proposed regulations.

1. **Sec. 999.305(a)(4): Modified Regulation Addressing Mobile Device Notices**

The modified draft regulations would provide additional clarity regarding the notices required under the regulations and the methods available to provide consumers with a meaningful understanding of this information. The revised draft would also require that consumers are provided notice where data collection from a mobile device may be unexpected. Google has long supported these transparency principles and builds notices into its own products to inform consumers about its data practices, as well as requires developers publishing applications on the Google Play Store to provide such notices.

W246-1

However, we recommend refinement of the proposed requirement in section 999.305(a)(4) that businesses "provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection," and that such notice be provided "through a pop-up window when the consumer opens the application." This requirement would single out a specific technology and impose extremely detailed and prescriptive notice obligations concerning the business's full data collection practices any time it collects one form of personal information that may not be expected. Such a rigid requirement would potentially require lengthy disclosures on mobile devices that are likely to confuse rather than help consumers.

Rather than prescribe detailed and specific notice obligations, we recommend adopting a more flexible standard, to encourage businesses to provide notice where they collect personal information that might not be reasonably expected, in a manner that provides consumers with a meaningful understanding of the information being collected. Such a standard would ensure that consumers are provided information they need to make informed decisions without overwhelming them with less relevant information. It would also align this requirement more closely to the GDPR, which requires that information be provided to consumers in "a concise, transparent, intelligible and easily accessible form, using clear and plain language." GDPR, Art. 12(1). Finally, it would accord with other provisions of the draft regulations, requiring that privacy policies "be designed and presented in a way that is easy to read and understandable to consumers" and "[u]se plain, straightforward language and avoid technical or legal jargon." Sec. 999.308(a)(2). W246-1 (cont.)

Proposed Amendment: "When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall ~~provide a~~ take reasonable steps to ensure that the consumer reasonably understands such information will be collected, such as through just-in-time notice of the information collected ~~containing a summary of the categories of personal information being collected and a link to the full notice at collection~~. For example, if a business offers a flashlight application and the application collects geolocation information, the business could ~~shall~~ provide a just-in-time notice, such as through a pop-up window when the consumer first opens the application, which explains that the application collects geolocation information ~~contains the information required by this subsection~~."

2. Sec. 999.313(c)(3) and (c)(4): Provisions Addressing Risks to Businesses and Consumers in Responding to Requests to Know

The original draft regulations would have prohibited businesses from providing a consumer with specific pieces of personal information where the disclosure would create "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." Sec. 999.313(c)(3). That requirement has been removed in the current draft in its entirety. While we agree that the regulations should not impose these new obligations on businesses, we also believe it is important that the regulations recognize that businesses should be *permitted* to consider the risks to consumer of providing personal information, and that they not be required to provide information where doing so would pose a security risk to either the consumer or the business. Similarly, the current draft would also revise the provision that purports to prohibit a business from disclosing, "in response to a request to know 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, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics." Sec. 999.313(c)(4). Again, we suggest that the regulations not impose new obligations by flatly prohibiting the provision of such information, but that they permit businesses to decline to provide such information. Accordingly, we recommend reinserting and modifying language to this effect. W246-2 W246-3

Proposed Amendment: "A business shall not be required to provide a consumer with specific W246-2 (cont.)

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."

W246-2 (cont.)

Proposed Amendment: "A business ~~shall~~need not disclose in response to a request to know 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, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics."

W246-3 (cont.)

3. Sec. 999.313(c)(10): Modified Regulation Addressing Responding to Requests to Know

As noted above, the modified draft regulations provide additional clarity to businesses on the notices required under the CCPA. We encourage further refinement of these obligations. For example, provisions such as section 999.313(c)(10)(f) would appear to require that a business disclose to individual consumers a detailed accounting of "[t]he categories of personal information that the business disclosed for a business purpose in the preceding 12 months, and for each category identified, the categories of third parties to whom it disclosed that particular category of personal information." This could include, for example, auditing and compiling a detailed list of every category of personal information shared with a "service provider" under strict contractual guarantees.

W246-4

The draft regulations similarly provide that businesses must provide "individualized" responses, and may not refer the consumer to the businesses' general practices outlined in its privacy policy "unless its response would be the same for all consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories." Sec. 999.313(c)(9). Requiring such individualized accountings would impose substantial burdens on businesses where a privacy policy already provides consumers with meaningful information about its data practices, and the consumer can request the specific pieces of information a business has collected about them. We recommend instead allowing businesses to provide consumers with meaningful disclosures about the relevant data practices, and to clarify with the consumer what information they are seeking. As we noted in prior comments, such a standard would align with the GDPR, which permits businesses to engage with consumers to specify the information or processing activity to which their request relates. *See* GDPR, Recital 63. It would also help ensure that businesses can provide consumers with the information most relevant to them, rather than blanket disclosures.

W246-5

Proposed Amendment: "In responding to a verified request to know categories of personal information, the business shall provide the consumer with meaningful disclosures about the following information, and may request that the consumer specify the information being requested before providing such an individualized response:"

* * * * *

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

Sincerely,

Cynthia Pantazis
Director, State Policy

From:	Ken Dreifach
To:	Privacy Regulations
Subject:	Comments to Modified Proposed CCPA Regulations
Date:	Tuesday, February 25, 2020 3:22:42 PM
Attachments:	ZwillGen Comment Letter - CCPA Modified Proposed Regulations.pdf

On behalf of the law firm ZwillGen, PLLC, I am respectfully submitting (attached hereto) our comments in response to the modified proposed CCPA regulations.

We are very pleased to have this the opportunity to submit our views on this important matter.

Sincerely,

Ken Dreifach

Ken Dreifach
Shareholder | ZwillGen PLLC
183 Madison Avenue, Suite 1504, New York, NY 10016
Office: 646 362 5590 **Direct:** [redacted]
Website | Twitter | LinkedIn

ZwillGen

183 Madison Avenue, Suite 1504
New York, NY 10016

Phone: +1 646 362 5590
Website: www.zwillgen.com
[redacted]
646-362-5590

February 25, 2020

By email to privacyregulations@doj.ca.gov

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

These comments are submitted on behalf of ZwillGen,[1] a law firm that advises hundreds of clients on privacy and security generally and on compliance with the CCPA specifically. We thank you for considering these comments.

We appreciate the Attorney General's extremely thoughtful consideration of the first set of public comments to the regulations, which we know were voluminous. The revised draft regulations have added clarity and provided important guidance to lawyers and businesses, while continuing to protect consumers' vital privacy interests. While we are generally aware of several issues as to which other groups intend to seek clarification, we are writing to shine a light on one particular instance in which we believe the revised regulations inadvertently do a substantial disservice to consumers and businesses alike, while also creating needless taxpayer waste.

1. Background: The Pro-Consumer and Pro-Taxpayer Benefits of Data Hygiene Providers

The current draft regulations would significantly hinder "data hygiene" providers, who perform important public services by preventing misdelivered mail. These companies typically "clean" – i.e., correct – personal information that was incorrectly input or transcribed. To spot these errors, they must (to be effective) draw on similar information across many of their customers.

W247-1

For instance, a data hygiene provider might see the following name and address in a business customer's database: **"Jane Q. Advocate | 3# Justice Drive | Anywhere CA 9420."**

The provider might in turn "clean" this information by comparing it to its other business customers' databases, and then conclude that "3# Justice Drive" is a typo that should read "3**3** Justice Drive," with a corrected zip code of 9420**7**. The provider might also "augment" the information" by adding the consumer's apartment number. The provider's business customer

[1] ZwillGen consists of two entities, ZwillGen PLLC, and ZwillGen Law LLP.

may then either (a) simply send the package to the now-correct address, or (b) if unsure, alert the consumer or double-check its own records.

This "cleaning and augmenting" process occurs millions of times each year, and likely prevents millions of packages and commercial mailings from being misdelivered. Indeed, according to the USPS, about 1.4 *billion* pieces of First-Class and standard mail were marked "returned to sender" in 2015, many due simply to missing address elements or apartment numbers.[2]

2. The Obstacles To Data Hygiene Posed by the Draft Regulations

The draft regulations make this vital data hygiene service much more difficult to offer in California. This is because section 999.314 provides that,

> "A service provider **shall not retain, use, or disclose** personal information obtained in the course of providing services except . . .
>
> (3) For internal use by the service provider to build or improve the quality of its services, **provided that the use does not include** building or modifying household or consumer profiles, **or cleaning or augmenting data acquired from another source[.]"**

W247-1 (cont.)

By excluding "cleaning or augmenting" from the list of permitted service provider uses, the regulations strongly discourage such data hygiene, thus restricting Californians from receiving the same benefits the rest of the nation will continue to receive.

Under the draft regulations, the data hygiene service provider would not be allowed to correct the mailing address unless its customers have all undertaken to describe this corrective use case as a "sale" – a highly non-intuitive step. The consumer's mail (in the above example) in turn would not have been delivered to her – or perhaps would have been delivered to the homeowner at "3 Justice Drive" instead. This would be to the detriment of:

- The consumer, who would not have received her package;
- The business, who would have a dissatisfied customer;
- The US Postal Service, which would have to return the package, incurring double costs;
- The US taxpayer, which would have to pay those additional costs.

[2] See US Postal Service Website: https://about.usps.com/publications/sar2015/sar2015/sar2016_doc_028.htm; Gary Seitz, *Undeliverable As Addressed Mail: Where Does It Come From, and How Do You Fix It?*, Mailing Systems Technology, Sept. 28, 2016 (available online at https://mailingsystemstechnology.com/article-4043-Undeliverable-As-Addressed-Mail-Where-Does-It-Come-From-and-How-Do-You-Fix-It.html.

3. The Real Dollar Impact of Misaddressed Mail

According to the US Postal Service, misaddressed mail "is costly to both the Postal Service and its customers – about $1.5 billion a year for the Postal Service and $20 billion for the mailing industry."[3] The proposed regulations doubtless would cause these numbers to increase, by labeling this important public service as a "sale" rather than a customary (and important) service provider function. We respectfully submit that it is in the interest of consumers, businesses, and taxpayers alike to retain and encourage these protections.

W247-1 (cont.)

4. Our Proposed Revision

We therefore respectfully propose the following revision to *Section 314(c)(3)*:

> A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except . . . **[f]or cleaning or augmenting data acquired from another source,** or internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles~~, or cleaning or augmenting data acquired from another source~~.

Thank you for considering these comments. If we can be of further assistance to you during the rulemaking process now or in the future, please do not hesitate to contact us.

Respectfully Submitted

ZwillGen

By: Kenneth M. Dreifach
Shareholder

[3] See "Undeliverable as Addressed Costs More Than You Think" United States Postal Service Office of Inspector General blog, available at https://www.uspsoig.gov/blog/undeliverable-addressed-costs-more-you-think.

From:	Mohammed, Shoeb
To:	Privacy Regulations
Cc:	Leder, Leslie; Barrera, Jennifer
Subject:	CalChamber Comments to Modified CCPA Regulations
Date:	Tuesday, February 25, 2020 3:21:01 PM
Attachments:	CalChamber Comments to AG Modified CCPA Regs.pdf

Privacy Regulations Coordinator,

Attached please find the California Chamber of Commerce's written comments on the Attorney General's Modified CCPA Regulations.

Respectfully,

Shoeb Mohammed
Policy Advocate

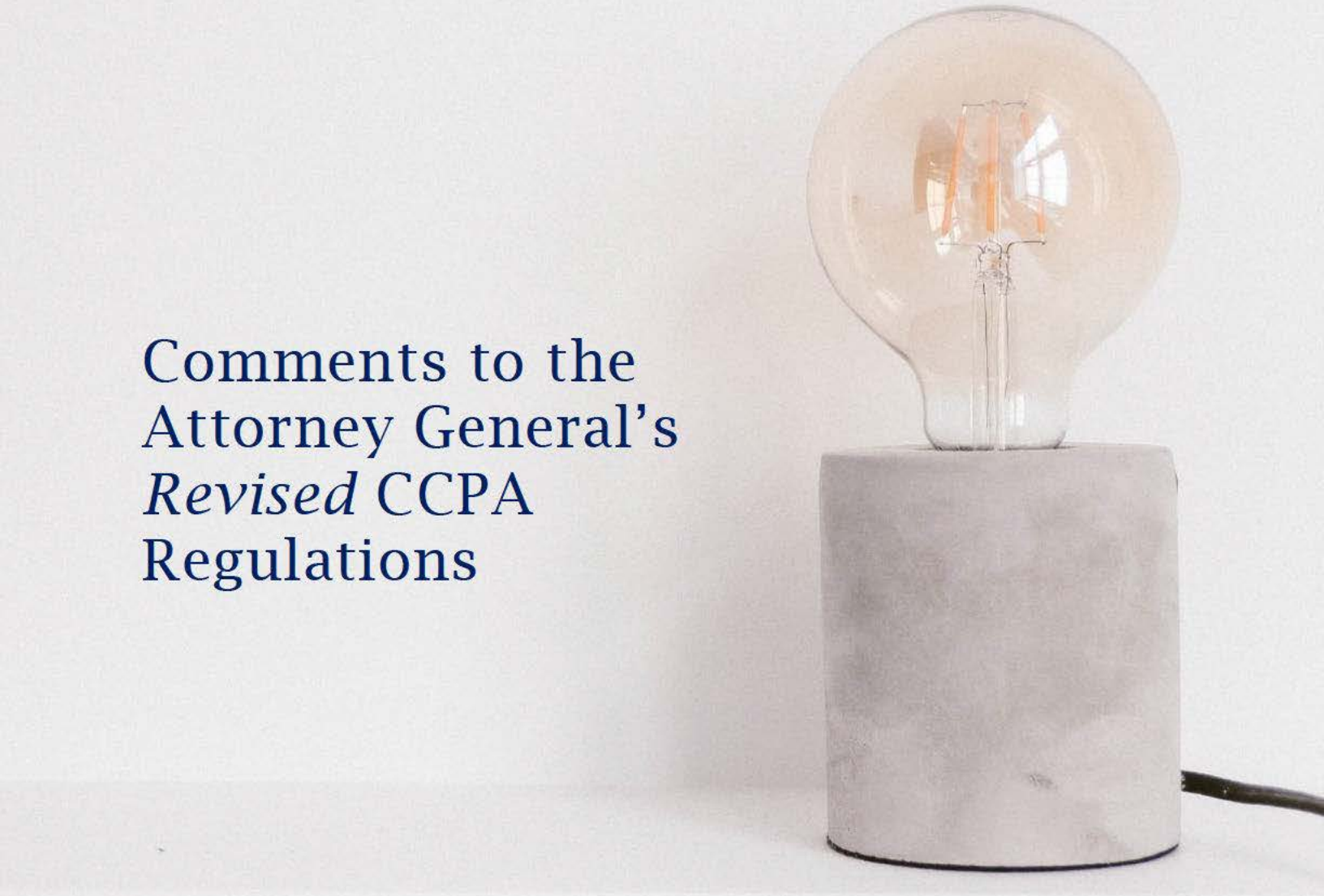
CalChamber.
HR Expert & Business Advocate™

California Chamber of Commerce
1215 K Street, 14th Floor
Sacramento, CA 95814

T [redacted]
F 916 325 1272

CalChamber
CALIFORNIA CHAMBER OF COMMERCE

California Chamber of Commerce



Comments to the Attorney General's *Revised* CCPA Regulations

SHOEB MOHAMMED
Policy Advocate
[redacted]

Executive Summary

The California Chamber of Commerce ("CalChamber") respectfully submits the following comments to the California Attorney General's ("AG") office regarding the AG's Revised Proposed Regulations for the California Consumer Privacy Act (CCPA), last modified on February 10, 2020. CalChamber appreciates the significant effort put forward by the AG and requests that the AG consider the following additional comments.

For convenience, each comment is presented separately in three parts: (a) the header which identifies the proposed regulation; (b) issue headers that synthesize the individual issues or concerns with the proposed regulation; and (c) subparts that identify the problem with proposed regulation, and recommended change(s) to resolve or mitigate CalChamber's related concern(s).

We additionally request that the enforcement date of the regulations be delayed until January 1, 2021 so that business owners have time to change their processes to make compliance more efficient, more effective, and more accountable. California's business owners are demonstrating their commitment to privacy rights by spending millions of dollars on employee training and updates to business practices for compliance with CCPA. It would be burdensome, costly, and in some instances, impossible to change administrative and technical processes for regulations that are not yet final. W248-1

Finally, although groups are raising a variety of discrete issues with the proposed regulations, this is not a collectively exhaustive list; rather, this report is intended to reflect key issues for the CalChamber at large.

I. SECTION 999.315 - REQUESTS TO OPT-OUT

A. Issue: Businesses should not be denied the option to provide an opt-out button.

1. **Proposed Reg:** §§999.315(d); 999.315(g)

a. **Opt-out signals are not standardized.** Websites, devices, browsers, applications, and plug-ins are created independently by developers and software companies around the world who use differing and constantly evolving programming languages to construct their products. Because there is no standardized opt-out signal, no standardized language by which devices and software communicate such signals, and because so many programs, languages, and devices are incompatible with one another, businesses operating online are ill-equipped to receive, interpret, and respond to the wide variety of signals from all the devices and browser plug-ins that developers continue to invent. This regulation cannot be operationalized until opt-out signals are standardized across all platforms and operating systems. Instead, Businesses must have the option to provide consumers with a standardized opt-out button on their individual websites, as the text of CCPA states.

W248-2

b. **Postponing This Issue Can Reduce Government Waste and Lower Costs on Business Owners**. Because the California Privacy Rights Act of 2020 (CPRA) provides for its own rule making at Section 1798.185, it would reduce government waste and lower costs on business owners if regulators and industry did not have to repeat this process again in two years. Accordingly, CalChamber respectfully reiterates its request that the AG's Office defer the provision on user-enabled global privacy controls until after CPRA is voted on in November, 2020 (if it qualifies) or until the industry has agreed upon a standardized procedure for communicating user preference. Because discussions aimed at developing such a procedure is underway, it appears likely that a standardized procedure will exist within the next two to three years.

2. **Recommended Change:**

Strike §999.315(a) in its entirety.

Alternatively, revise § 999.315(a): "If a business collects personal information from consumers online, the business ~~shall~~ may treat user-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism, that clearly and reliably 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."

B. Issue: Proposed regulations allow browsers to use opt-out signals for their own benefit.

1. **Proposed Reg:** §§999.315(a); 999.315(d)

W248-3

a. **Consumers Should Choose How to Exercise Their Rights, Not Developers.** The regulations give browser plugins and privacy settings the power to exercise consumer rights by communicating consumer opt-out requests on behalf of consumers. But putting

the exercise of consumer rights in the hands of software companies that develop browsers and plugins will increase the likelihood that those companies will create self-serving exceptions that use consumer rights as a means to advantage themselves or disadvantage their competition.

b. **Consumers Should Be in Control, Not Developers.** The CCPA empowers consumer choice, and businesses support this consumer-focused approach. The CCPA does not intend for developers and device manufacturers to substitute their own presets for consumer choices. Instead, it empowers consumers by creating mechanisms like the "Do Not Sell" button, which is a standardized icon that can be recognized in any language and signals to consumers that clicking on the symbol allows them to exercise their rights. It runs contrary to the statute to mandate adherence to a non-standardized opt-out signal mechanism, and harms competition by favoring the few advertisers who have direct relationships with customers.

W248-3 (cont.)

c. **Consumers should be empowered to make their own decisions.** This requirement harms competition by favoring the few advertisers who have direct relationships with consumers and can therefore ask consumers to override browser or device settings based opt-out requests. If consumers make a general decision to opt out via a single setting, it will restrict the capacity of online advertisers without a direct consumer relationship to compete in the online advertising market. The dominance of a few advertisers can easily lead to lower revenues for online journalism and higher prices for businesses who seek to reach new consumers. The result is the availability of less free content online. Consumers will not be aware of these trade-offs when they click on a global device setting.

2. **Recommended Change:**

Revise §999.315(d)(1): Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a customer intends to opt-out of the sale of personal information. The privacy control shall require that the consumer affirmatively select their choice to opt-out and shall not be designed <u>in a manner that would prevent the sale of personal information unless the customer affirmatively selects their choice to opt-out</u> ~~with any pre-selected settings~~.

C. Issue: Businesses should not be denied the ability to verify or authenticate opt-out requests.

1. **Proposed Reg:** §§999.315(h)

a. **Opt-out requests can threaten the security of consumer information.** Opt-out requests can block consumers from participation in services that utilize the sale of data to prevent fraud and authenticate consumer identities, effectively removing security measures designed to protect consumers. Without authentication on the front-end, businesses will have no way of knowing if an opt-out request is fraudulent. If a consumer is opted-out of such fraud protection services by a criminal, or even unknowingly, businesses utilizing those services to prevent identity theft or other crimes would then need to try improvised ways to confirm identity; or choose simply to forego identity authentication. Either result puts consumers at greater risk.

W248-4

2. **Recommended Change:**

Revise section 999.315(h): "A request to opt-out need not be a verifiable consumer request. If a business, however, cannot verify the identity of a person making a request concerning personal information sold for purposes other than advertising or marketing, or has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request either because it could not verify identity or ~~and shall provide an explanation why~~ that it believes the request is fraudulent.

W248-4 (cont.)

II. SECTION 999.307 – NOTICE OF FINANCIAL INCENTIVE

A. Issue: Data does not have independent value.

1. **Proposed Regulation:** §§999.307; 999.337

a. **Estimates of the value of consumer data are ineffective because data does not have independent value.** The reason certain businesses can offer their services for free is not because they are being compensated for peoples' data, it is because they make money by selling ads. Ads are valued using objective metrics such as the number of clicks or the number of views. The implication that data can be valued with a dollar amount demonstrates a fundamental misunderstanding of how businesses use data in the marketplace. Further, it is misleading to communicate to consumers that their personal data is valued at a certain dollar amount.

W248-5

2. **Recommended Change:**

Revise §999.307(b)(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 ~~and the value of the consumer's data~~.

B. Issue: Notice of Financial Incentive requirements do not address businesses that do not sell first party data but use it for sales and advertising.

1. **Proposed Regulation:** §§999.307

a. The Notice of Financial Incentive requirements as written do not adequately address the situations where a business does not sell its first party data and therefore does not assign a value to that data. Using first party data to communicate discounts or special offers is a means for a business to increase brand awareness, build brand loyalty and meet consumer needs, all of which is hard to objectively value.

W248-6

2. **Recommended Change:**

We suggest that the regulations be amended to specify that providing a price or service difference, by simply using its first party data, is not within scope of requiring a notice of

financial incentive as long as the business does not sell the consumer's personal information. W248-6 (cont.)

III. SECTION 999.313 – RESPONDING TO REQUESTS TO KNOW AND REQUESTS TO DELETE

A. Issue: Consumers should be allowed to request specific elements of data.

1. **Proposed Reg:** §§ 999.313(c)(10)

a. **Requiring businesses to conflate consumer rights eliminates consumer choice.** CCPA allows consumers to assert each of the enumerated rights separately under §1798.100(b), §1798.110, and §1798.115.

b. **Businesses should not be required to overproduce.** Businesses should not be required to provide all six elements of personal information when responding to a request to know categories of information because some consumers may request narrower portions of information. As written, even if a consumer wants specific information, businesses are required to disclose all six categories of data enumerated in this section. Flooding consumers with more information then they requested could overwhelm them and unnecessarily adds more administrative burden to businesses seeking to comply. W248-7

2. **Recommended Change:**

Revise §999.313(c)(10) to allow businesses the option to provide consumers with the information than what they requested, or to provide all six elements of personal information when responding to a consumer's more narrow request.

B. Issue: Unverifiable Requests to delete should not be converted into opt-out requests.

1. **Proposed Reg:** §§ 999.313(d)(1)

a. **It is unreasonable to require businesses to offer opt-out rights to individuals whose identity could not be verified.** This rule requires businesses to offer unverifiable persons the right to exercise additional rights on behalf of the person whose identity could not be verified to begin with. Businesses should only act upon requests when consumers express a clear preference. These regulations presuppose consumers' wishes by treating an unverified delete request as a Do Not Sell preference. Requiring businesses to conflate consumer rights requests eliminates consumer choice, may be confusing for consumers, and is not supported by the CCPA. W248-8

2. **Recommended Change:**

a. Align language with statute.

b. A revision to Section 999.313(c)(9) expanding the circumstances in which a company could rely on a generic articulation of categories in the Privacy Notice, as opposed to a customer-specific feed. For example, the regulation could be broadened to clarify that we W248-9

may refer to our privacy policy when our response would be the same for "substantially all" or "most" consumers. W248-9 (cont.)

c. A revision to Section 999.313(c) to add new Section 999.312(c)(12) that would clarify that a company need not *additionally* fulfill a request to provide *categories* of information collected if it is *also* providing specific pieces of information. (Perhaps this could be time-bound to make it more palatable?). W248-10

d. A revision to Section 999.313(c) to add new Section 999.312(c)(13) that would clarify a business shall identify the personal information responsive to a request to know by conducting a commercially reasonable search of its records. W248-11

C. Issue: Unverifiable Requests to delete should not be converted into opt-out requests.

1. **Proposed Reg:** §§ 999.313(c)(3)

a. **The modified regulations removed an important security exception.** The exception stated that, "A business shall not withhold specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of the personal information, the customer's account with the business, or the security of the business's systems or networks." This additional qualification is helpful in affirming that businesses are not required to provide access to information that could place consumers, or their systems, at risk. W248-12

2. **Recommended Change:**

Include the language from the initial draft regulations in this section.

D. Issue: Regulation should be specified to focus on making sure information is not linked to an individual because all information is searchable or to some extent accessible.

1. **Proposed Regulation:** §999.313(c)(3)

a. "Searchable or reasonably accessible format" is a technologically concerning standard as part of the basis for searching or accessing data is the computational cost of accessing it, which, generally goes down over time. This means that from an implementation standpoint parties will have to consistently re-review exemptions. In contrast, "where the information is not directly or indirectly linked to such data in a searchable or reasonably accessible format" means that the focus is on whether or not the information is linked to an individual, which is the underlying issue and something that is binary and not going to evolve over time. W248-13

2. **Recommended Change:**

Revise Section 999.313(c)(3)(a): "The ~~business does not maintain the personal~~ information is not directly or indirectly linked to such data in a searchable or reasonably accessible format."

E. Issue: Disclosure of consumer personal information is necessary to support portability.

1. **Proposed Reg:** §§ 999.313(c)(4)

a. **Certain information enumerated in this section is necessary to support portability.** The language does not address requests seeking portability of information where such identifiers enumerated in Section 999.313(c)(4) are necessary to support portability. W248-14

b. **The prohibition on biometric data should be narrowed to include data containing identifying information.** Because CCPA defines biometric data to include health or exercise data, this prohibition should only apply to biometric data that could itself identify the individual. As written, it could potentially prevent consumers from transferring exercise metrics and other non-identifiable health information that falls under the CCPA definition of "biometric data." W248-15

2. **Recommended Change:**

Revise Section 999.313(c)(4): "A business shall not disclose in response to a request to know 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, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics and can be used to identify any particular individual. A business, however, may do so in response to requests seeking portability of information where such identifiers enumerated in Section 999.313(c)(4) are necessary to support portability except where the disclosure creates a substantial, articulable, and unreasonable risk to the security of the personal information, the consumers account with the business, or the security of the business systems or networks. W248-15 (cont.) W248-14 (cont.)

F. Issue: Regulation creates risk of inappropriate disclosure of information about a consumer in response to an unverified request.

1. **Proposed Reg:** §§ 999.313(c)(1)

a. **Creating obligations in response to unverified requests is contrary to, and inconsistent with, the statute.** The CCPA contemplates that unverified requests should be discarded precisely because they are unverified: "A business is not obligated to provide information to the consumer pursuant to Sections … 1798.105 … if the business cannot verify … that the consumer making the request is the consumer about whom the business has collected information …" Practically, the very reason a business should discard an unverified request is to protect the consumer—the business is unable to verify the individual's identity and therefore should not act on requests related to that consumer's personal information. And the statute creates a specific mechanism for opting-out of the sale of information. Collapsing verification and opt-out procedures is contrary to the statute and creates vectors for abuse. W248-16

2. **Recommended Change:**

Strike language in §999.313(c)(1) mandating that a request that fails verification be considered for disclosure of categories of personal information, as follows:

"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).~~"

W248-16 (cont.)

IV. SECTION 999.301 – DEFINITIONS

A. Issue: Definition of "affirmative authorization" requirement for two-step process to opt-in is overly burdensome for consumers and business.

1. **Proposed Regulation:** §999.301(a)

a. For consumers 13 years and older, Section 999.301(a) mandates a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in. Mandating a two-step process can be cumbersome and disruptive for consumers and overly prescriptive for businesses. It can prevent businesses from developing innovative consent flows based on extensive UX/UI research.

W248-17

2. **Recommended Change:**

Strike the language in section 999.301(a) mandating a two-step process, and instead indicate that a two-step process is permissible.

B. Issue: Proposed regulations need to provide clarification regarding definition of "direct notice" to consumers.

1. **Proposed Regulation:** §999.301; *see also* §§999.305(a)(3); 999.305(d)(1); 999.306(d)(2)

a. There is a lack of clarity as to direct notification under the regulations. Providing a definition of "directly notify" would provide certainty as well as coordination across all the rules that require some sort of direct notice to consumers.

W248-18

2. **Recommended Change:**

Add a new subsection 999.301(g): "Directly Notify" means contacting the consumer directly with the required information, provided, however, that a business will have been deemed to directly notify a consumer of changes to its policies and practices if the notification is published and made available on its website for a sufficient period of time or other standard method of providing privacy policies and notices to consumers."

C. Issue: Definition of right to know still conflicts with requirements for how to respond to right to know.

1. **Proposed Regulation: §§999.301(q);**

   a. The definition of right to know under Section 999.301(q) says a consumer has a right to "any or all" of the following categories of personal information. However, Section 999.313(c)(10), instructing businesses how to respond to requests to know, uses the conjunctive "and"—not "and/or"—for the categories of information a business must disclose in response to a consumer request. Thus, under Section 999.313, a business is required to disclose all enumerated categories, even if consumer only makes a limited request.

2. **Recommended Change:**

   Correct the wording in Section 999.313(c)(10) to allow consumers to make more specific requests, and permit businesses to respond by producing information responsive to those specific requests only.

W248-19

D. Issue: The definition of right to know still creates infeasible requirements for responding to individual consumer requests.

1. **Proposed Regulation:** §999.301(q).

   a. This definition lumps one request into different categories, sources, and a variety of different requests. It would be preferred if each subsection (1) through (6) were separately defined. Subsections (2) through (6) should be addressed through a notice so it is standardized across the board for all consumers. It is not feasible or scalable to provide the customized set of categories to each individual consumer.

1. **Recommended Change:**

   The "Request to know" should be linked only to subsection (1).

W248-20

E. Issue: Modified regulations add a new and undefined term, "materially different," further complicating the explicit consent requirement.

1. **Proposed Regulation:** § 999.305(a)(5)

   a. Section 999.305(a)(5) requires businesses to obtain explicit consent from consumers to use personal information for a purpose that is materially different than those purposes disclosed at the time of collection. The term "materially different" should be defined to clarify this regulation.

2. **Recommended Change:**

W248-21

Add a definition for the term "materially different." We propose the following: "a purpose is materially different if a reasonable person would not reasonably expect that purpose to be consistent with the scope based on the nature and extent of the business' usual activities."

W248-21 (cont.)

V. SECTION 999.305 – NOTICE AT COLLECTION

A. Issue: Regulations do not address when and how non-data broker third parties must provide notice to consumers in situations when they collect information at the direction of the consumer, and then generate their own relationship with that consumer.

1. **Proposed Regulation:** § 999.305(c)-(d)

a. Section 999.305(c) addresses notice owed by a business to a consumer if a business collects PI from a consumer. Section 999.305(d) addresses notice owed to a consumer from a data broker who does not collect PI directly from consumers. The regulations do not provide clarity as to when and how a non-data broker third party that collects information about a consumer, at the direction of the consumer, and then generates its own relationship with that consumer, is to provide notice. These types of transactions do not practically lend themselves to providing notice to the consumer "at or before" the point of collection. The most efficient and transparent way to provide notice and to meet consumers' expectations is to provide notice at the time when the first direct interaction with the consumer occurs.

W248-22

2. **Recommended Change:**

The regulations be amended to specify that, in that circumstance, notice be provided when the business first contacts or is contacted by the consumer to create that relationship.

B. Issue: Providing oral notice to customers seeking support or otherwise calling-in does not align with consumer expectations because it would further increase wait times at support centers that handle large volumes of calls.

1. **Proposed Regulation:** § 999.305(a)(3)(d)

a. Section § 999.305. (a)(3)(d) sets forth that notice at collection shall be made readily available where consumers will see encounter it at or before the point of collection of any personal information is collected and that when a business collects personal information over the telephone or in person, it may provide the notice orally. Providing notice orally at or before the point of collection to consumers that initiate calls to a business does not align with consumers' expectations and would cause increased wait times, especially at customer contact centers that handle large volumes of calls. Additionally, this requirement would be burdensome and expensive for businesses to implement.

W248-23

2. **Recommended Change:**

The regulations be amended to specify that if a consumer initiates a phone call with a business and intentionally provides personal information, for the provision of a good or service, that the notice can be provided by email immediately following the transaction. This method would allow for transparency and would meet consumers' service expectations. W248-23 (cont.)

C. Issue: A Previous Exception Has Been Inadvertently Deleted.

1. **Proposed Regulation:** § 999.305(d)

a. This exception, as it appeared in the unmodified proposed regulation, would have eliminated the requirement for notice at collection in instances of indirect collection of publicly available data that will be used for purposes reasonably expected by the customer. As currently drafted, only registered data brokers are permitted to forego notice at time of indirect collection of personal information. We believe this deletion was unintended and ask that it be reinstated. W248-24

2. **Recommended Change:**

Reinstate the exception for notice at collection in instances of indirect collection of publicly available data that is used for purposes reasonably expected by the consumer. An alternative approach would be to excuse notice at indirect collection in instances of indirect collection of publicly available data for purposes reasonably expected by the customer (e.g., obtaining job title and contact information from a company website for recruitment, collecting author names from published studies to identify thought leaders in a field).

VI. SECTION 999.317 – TRAINING; RECORD KEEPING

A. Issue: Record-Keeping Requirement Is Not Supported By CCPA.

1. **Proposed Regulation:** § 999.317(g)

a. The reporting requirement in §999.317(g) does not exist in the statute itself and has no support in the law. W248-25

2. **Recommended Changes:**

Recommend striking §999.317(g).

Alternatively, we recommend that §999.317(g) be clarified to better explain what actions do or do not trigger the record keeping requirement.

VII. SECTION 999.316 – REQUESTS TO OPT-IN AFTER OPTING OUT OF THE SALE OF PERSONAL INFORMATION

A. Issue: These regulations should not dissuade consumers from expressing their preferences.

1. **Proposed Regulation:** § 999.316(a)

a. **Consumers should not be dissuaded from opting in after they have opted out.** This requirement creates unpleasant hurdles for consumers who wish to express a preference to opt-in following an opt-out request. These hurdles are inconsistent with consumer expectations and would require businesses to build new systems that force users to experience hostile user interfaces in order to express their preference. It attempts to nudge consumers toward a course of action, rather than empowering them to make their own decisions in a straightforward and unbiased manner. W248-26

2. **Recommended Changes:**

Recommend striking the reference to a "two-step" process in Section 999.316(a).

VIII. SECTION 999.325 VERIFICATION FOR NON-ACCOUNTHOLDERS

A. Issue: Requiring business to provide two tiers of authentication for right to know requests is extremely burdensome where a consumer already has an authenticated, and secure online account with a business.

1. **Proposed Regulation:** §999.325(c)

a. Requiring businesses to provide two tiers of authentication for right to know requests, depending on whether the request is for categories of specific pieces of personal information, imposes additional implementation requirements that go beyond the text of CCPA. This is not common practice for third party verification service providers and should not be made part of a business's practice. W248-27

b. The language requires "a signed declaration under penalty of perjury" but there are alternative methods of verifying identity that are more reliable than a signed declaration in a business's environment (e.g., blockchain or otherwise).

2. **Recommended Change:**

We recommend deleting Section 999.325(c).

In the alternative, revise 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 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 and/or any other information or practices that the business reasonably determines is necessary to confirm that the requestor is the consumer whose personal information is the subject of the request. If a business uses this method for verification, the business shall maintain all signed declarations as part of their record-keeping obligations."

W248-27 (cont.)

IX. SECTION 999.323 – GENERAL RULES REGARDING VERIFICATION

A. Issue: Requirement to generally avoid requesting additional consumer information for verification is counterintuitive to need to ensure verification and protect consumer security.

1. **Proposed Regulation: §999.323(c)**

a. The requirement that businesses shall "generally avoid" requesting additional information from a consumer for the purposes of verification is at odds with the need to ensure verification. Verification should allow asking what's necessary for positive identification to protect consumers.

W248-28

2. **Recommended Change:**

Revise section 999.323(c) to strike "A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify . . ."

X. SECTION 999.302, 999.313(c)(3), 999.313(d)(3)) – GENERAL RULES REGARDING VERIFICATION

A. Issue: The guidance in §999.302 regarding the definition of "personal information" fails to appreciate that most pseudonyms or de-identified information could be linked to an individual but is not in practice.

W248-29

1. **Proposed Regulation: §999.302(a)**

a. A business often maintains such information in de-identified fashion as a privacy safeguard, using technical and administrative controls such as hashing, encryption, and contractual safeguards to prevent its linkage to an individual. The European Union's General Data Protection Regulation recognizes this as a good practice.

b. Similarly, the clarifications in § 999.313(c)(3) are helpful in exempting from right to know requests personal information that a business maintains in backup or archive systems, but this exemption could also apply to personal information that is not routinely linked to an individual consumer. These considerations should also apply to deletion requests in § 999.313(d)(3).

W248-30

W248-38

c. The elimination of the previous text in § 999.313(c)(3) is not helpful. The previous text allowed a business to forgo disclosure if it "creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account

W248-31

with the business, or the security of the business's systems or networks". We request the reinstatement of this deleted text.

W248-31 (cont.)

2. **Recommended Change:**

a. Revise §999.302(a): "Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "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." For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be "personal information."

W248-29 (cont.)

XI. SECTION 999.308 – PRIVACY POLICY

A. Issue: Requiring businesses to describe the process used for verifying consumer requests in their privacy policy does not account for the fact that the verification process and information required may change or upgrade quicker than privacy policies can be updated.

1. **Proposed Regulation: §999.308(c)(1)(c)**

a. As part of the privacy policy disclosure, the regulations would require the business to describe the process it will use to verify the consumer request, which even generally would include laying out what information the consumer must provide. The problem with this is that the process and the information required to verify the consumer's identity may need to be changed or upgraded quickly to address emerging security concerns – but privacy policies cannot be changed or upgraded nearly so fast.

W248-32

2. **Recommended Change:**

We recommend that the business only be required to disclose a link to the company's current process, instead of the entire process verbatim, so that the process can be updated much more quickly and easily in response to changing security concerns.

B. Issue: Regulation is unclear whether a business that sells personal information would be required to make disclosures regarding minors in its privacy policy.

1. **Proposed Regulation: §999.308(c)(1)(e)(3)**

a. The addition of the "actual knowledge" standard is well received, but we would suggest further refining this section to make clear that only a business that engages in "sales" of personal information would be required to make such a statement in its privacy policy that has actual knowledge of the sale of personal information of minors under the age of 16. In the absence of such clarity, this could result in businesses having to include in their privacy policy a statement that they do not have actual knowledge that they are selling the personal information of minors, even if they already state that they do not sell the personal information of users generally.

W248-33

2. **Recommended Change:**

Suggest revising §999.308(c)(1)(e)(3) to include language that would achieve the same goal but with more clarity: "State whether a ~~the~~ business that sells personal information has actual knowledge that it sells the personal information of minors under 16 years of age." W248-33 (cont.)

XII. SECTION 999.314 – SERVICE PROVIDERS

A. Issue: Requirements relating to service providers go beyond the text of CCPA.

1. **Proposed Regulation: §314(d)**

a. The CCPA does not impose requirements relating to consumer rights on service providers, as opposed to businesses. These service providers do not obtain personal information for commercial gain from the data, and they are not in the best position to provide any information on consumers or verify the identity of consumers, since service providers are unlikely to have direct relationships with consumers. Finally, service providers may not be permitted to disclose the identity of their clients. W248-34

2. **Recommended Change:**

Strike the requirement that service providers must respond to consumer requests.

B. Issue: The word "cleaning" is not defined in the regulations.

1. **Proposed Regulation: §999.314(c)(3)**

a. The word "cleaning" is not defined in the regulations. Without a definition, it could be interpreted as meaning that service providers can't anonymize their users' personal information. This not only could disrupt analytics functions that involve de-identifying data but seems to go against the overall purpose of promoting privacy. W248-35

2. **Recommended Change:**

Suggested revision: We recommend the deletion of the word "cleaning" or the inclusion of a definition that allows service providers to de-identify data in efforts to build or improve the quality of services.

XIII. SECTION 999.306 – NOTICE OF RIGHT TO OPT OUT OF SALE OF PERSONAL INFORMATION

A. Issue: Opt-Out Button Graphic Is Misleading.

1. **Proposed Regulation: §999.306(f)**

a. Under commonly accepted graphic design principles, the "opt-out button" misrepresents its actual function because it is designed as a slider-toggle, suggesting that the button itself is a control when it is not. In fact, the purpose of the button is to provide consumers W248-36

with the option to opt-out and simultaneously provide consumers with disclosures and education regarding their privacy rights.

2. **Recommended Change:**

Suggested revision: Recommend this button be eliminated or more appropriately designed to make clear that it is a link and not an actual control.

W248-36 (cont.)

B. Issue: Clarification Requested on Date of Applicability

1. **Proposed Regulation: §999.306(e)**

a. This provision could be interpreted as prohibiting businesses from selling consumer data that was collected prior to the opt-out link being posted (12/31/2019), unless it goes back to those consumers and obtains their affirmative authorization. CCPA does not authorize retroactive enforcement.

W248-37

2. **Recommended Change:**

Clarification is needed regarding whether this provision applies from the time that CCPA went into effect.

From: Angelena Bradfield
To: Privacy Regulations
Subject: BPI Comment Letter on Revised Proposed CCPA Regulations
Date: Tuesday, February 25, 2020 3:13:51 PM
Attachments: BPI Comment Letter on Revised Proposed CCPA Regulations.pdf

---

Hello Ms. Kim:

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

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

Sincerely,
Angelena

Angelena Bradfield
Senior Vice President, AML/BSA, Sanctions & Privacy
[redacted]
Phone: [redacted]

BANK POLICY INSTITUTE

February 25, 2020

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

Re: Revised Proposed Regulations Under the California Consumer Privacy Act

Dear Ms. Kim:

The Bank Policy Institute (BPI)[1] appreciates the opportunity to submit comments on the Attorney General's Revised Proposed Regulations, as modified on February 7 and 10, 2020, under the California Consumer Privacy Act (CCPA) (Revised Proposed Regulations).[2] BPI supports numerous revisions in the Revised Proposed Regulations. For example, BPI applauds the guidance in § 999.302 regarding the interpretation of "personal information." The new language helps clarify the meaning of that important term and appears to be consistent with the intent of the CCPA. BPI also supports the revision in § 999.305(b)(2) to permit businesses to provide the business or commercial purposes for which "the categories of personal information" will be used rather than listing the business or commercial purposes for each individual category of personal information. This change will aid businesses in providing consumers with privacy policies "designed and presented in a way that is easy to read and understandable to consumers," as prescribed in § 999.308(a)(2).

I. Executive Summary

As explained in BPI's prior comment letter, the Attorney General plays a critical role in ensuring that any new requirements under the Revised Proposed Regulations are consistent with the CCPA's terms and are consistent with the intent of the CCPA. The harmonization is critical to allow businesses adequate time to test and implement strong compliance policies and processes to help consumers understand their rights and responsibilities.

Financial institutions, in particular, have been required to invest significant time and resources to build compliance programs that align with both the policies set forth in the CCPA and existing federal and state financial laws. The regulations should take these programs into account and ensure that consumer protections are not unintentionally weakened by companies' CCPA compliance efforts. In Part II, we propose several amendments to the Revised Proposed Regulations in order to address these concerns.

---

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

2 Cal. Civ. Code § 1798.100 *et seq.*

II. Proposed Amendments

A. The regulations' effective date should be at least six months after the final regulations are published in order to account for the imposition of requirements that go beyond the statute, and the Attorney General should not bring enforcement actions for conduct that occurs before January 1, 2021.

As explained in BPI's prior comment letter, the CCPA is a highly complex statute that requires businesses to invest significant time and resources in compliance. The Revised Proposed Regulations would add additional requirements and so will increase still further the time and resources needed for businesses to design, test, and implement compliant systems and processes. Many of these burdens are not contemplated by the CCPA itself. Thus, businesses have had less than two months to evaluate the implementation requirements of the original proposed regulations, and considerably less time to respond to Revised Proposed Regulations, much less to invest substantial resources into compliance, given the uncertain content of any final and binding rules. Requiring businesses to compress this timeline unreasonably will neither benefit consumers nor advance the goals of the CCPA. W249-1

Financial institutions face additional compliance costs given their obligations under state, federal, and international laws. For example, the CCPA does not apply to certain personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (GLBA) and the California Financial Information Privacy Act (Cal FIPA).[3] Banks have been required to invest significant time and resources to build compliance programs that properly determine whether certain personal information falls under the scope of the CCPA and to balance the requirements of the CCPA with the GLBA and Cal FIPA.

The Revised Proposed Regulations would add further complexity to financial institutions' compliance programs. Additional time is required to meet these compliance obligations. The regulations' effective date should thus be at least six months after the final regulations are published, and the Attorney General should not bring enforcement actions for conduct that occurs before January 1, 2021.

B. The requirement in § 999.317(g)(2) to publish metrics regarding responses to consumer requests in a business's privacy policy will not help consumers and may increase the risk of identity fraud. These metrics should instead be provided to the Attorney General upon request.

Subsection 999.317(g)(2) of the Revised Proposed Regulations would require covered businesses to disclose by July 1 of every calendar year "within their privacy policy or posted on their website and accessible from a link included in their privacy policy" several metrics about consumer requests they received under the CCPA and their responses to those requests. At the same time, subsection 999.308(a)(2) would require businesses to make available to consumers a privacy policy "designed and presented in a way that is easy to read and understandable to consumers." Subsection 999.317(g)(2)'s requirement to publish metrics regarding consumer requests may make privacy policies complex and less readable, cutting against the core goals of subsection 999.308(a)(2). Publication of metrics in businesses' privacy policies would lengthen and complicate these notices, without providing useful information about how personal information is collected and used. W249-2

Moreover, the metrics publication requirement may have the unintended consequence of creating an unfair perception of avoidance by businesses. The Revised Proposed Regulations contemplate legitimate grounds for denial of consumer requests, for example, if a business cannot verify the identity of the requestor. Financial institutions, in particular, must balance the CCPA's consumer request requirements with existing financial laws. Requiring publication of metrics, without context, may lead consumers to think businesses are avoiding compliance with consumer access rights and deter the sharing of personal information, even when denials are based on

[3] *Id.* at § 1798.145(e).

legitimate and lawful grounds. This is especially true for financial institutions collecting personal information regulated under GLBA and Cal FIPA, which may unfairly be viewed as avoiding compliance with the CCPA.

The Attorney General, instead, should require covered businesses to provide such metrics only to the Attorney General, and only upon request. Since the CCPA is enforced by the Attorney General and not by the consumers for whom a privacy policy is drafted, it would be more appropriate for businesses to be required to provide these metrics to the Attorney General upon request. Such an approach would also respect the principle embodied in subsection 11346.3(a) of the California Administrative Procedure Act, which states that an agency must consider the impact on California businesses and avoid imposing "unnecessary or unreasonable regulations or reporting, recordkeeping, or compliance requirements." W249-2 (cont.)

C. Subsection 999.313(c)(10) should be revised to permit businesses not to provide each category of third parties to whom they disclosed a particular category of personal information when doing so would create a substantial, articulable risk of fraud or hinder the ability of a business to comply with legal obligations.

Subsection 999.313(c)(10)'s requirement that covered businesses provide individual consumers with categories of third parties to whom they disclosed particular personal information may subject businesses to additional security risks and run afoul of existing laws. This is especially relevant for banks and other financial institutions that have reporting obligations under federal financial laws. For example, the Bank Secrecy Act requires banks and other financial institutions to submit Suspicious Activity Reports (SARs) in certain circumstances. The Act contains confidentiality requirements for SARs, including prohibitions on revealing the existence of a SAR.[4] If an individual requesting information is the subject of a SAR, banks risk being trapped in a "catch-22," required on one hand to comply with the CCPA's regulations and potentially reveal the existence of a SAR; and on the other hand, obligated to comply with a federal law prohibiting the provision of that exact information. W249-3

BPI recommends that the Revised Proposed Regulations be further revised to permit businesses not to provide each category of third parties to whom they disclosed that particular category of personal information when doing so would create a substantial, articulable risk of fraud or hinder the business's ability to comply with legal obligations. Such an exemption would be consistent with federal laws. For example, § 1033(b)(2) of the Dodd Frank Act exempts financial institutions from providing consumers with information collected for "the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct."[5] Furthermore, such a statement would support the provisions set forth in Section 1798.145(a)(1-3) of the CCPA that the law shall not restrict a business's ability to comply with relevant federal, state, or local laws and cooperate with law enforcement. In the absence of a general exemption in § 999.313(c)(10), BPI requests a specific exemption for banks and other financial institutions subject to federal financial laws.

D. Language added in § 999.314(e) about service providers responding to consumer data requests on behalf of businesses may (incorrectly) be read to permit service providers to respond without notice to or consent of the involved business, thereby possibly opening businesses up to unauthorized exposure of data, encouraging fraud, or facilitating violations of federal financial laws.

The CCPA contemplates that businesses that collect personal information from consumers act as the controller of that information.[6] Enabling service providers to make decisions unilaterally as to how to respond to consumer data requests jeopardizes businesses' ability to sufficiently control that information and comply with the W249-4

---

4 *See, e.g.*,31 U.S.C. §§ 5318(g)(2), 5321, and 5322.

5 12 U.S. Code § 5533(b)(2).

6 *See, e.g., id.* at § 1798.140(c)(defining "business" as an organization meeting certain criteria "that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information.") (emphasis added).

CCPA's requirements. This is an issue that, under the CCPA's terms, should be handled in contract negotiations between the covered entity and its service providers rather than being mandated by regulation.

Financial institutions may face additional compliance problems due to subsection 999.314(e)'s apparent blessing of service providers unilaterally responding to consumer data requests. As outlined previously, financial institutions are required to have protocols to protect consumer financial data under federal and state financial laws. Specifically, financial institutions must have vendor management protocols that outline a vendor's ability to use, disclose and process consumer financial data.[7] Enabling vendors to directly respond to consumer data requests, without input from financial institutions, may run afoul of such financial laws. Likewise, service providers may lack the tools and capabilities to properly verify consumer data requests, which may lead to exposure of data or fraudulent activity.

W249-4 (cont.)

For these reasons, subsection 999.314(e) should be omitted from the final regulations. At a minimum, if it is retained, it should be revised to make clear that covered businesses may prohibit service providers by contract from responding to consumer data requests on their behalf.

E. The Attorney General should add back in subsection 999.313(c)(3) the requirement 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."

The Revised Proposed Regulations would ease the burden on businesses in responding to consumer requests when a business does not maintain personal information in a searchable or reasonable format and certain other conditions are met. At the same time, however, the Revised Proposed Regulations omit a critical protection for both businesses and consumers by eliminating the ability of a business not to provide specific pieces of information when doing so would pose a risk to the security of personal information, consumer accounts, or businesses' systems or networks. No alternative protections appear in the Revised Proposed Regulations so the reason for removing this provision is unclear. For the protection of consumers, a business should be afforded the flexibility to only provide categories of information when it determines that disclosure of personal information in a given circumstance would pose a substantial, articulable security risk. Adding this exception back into the Revised Proposed Regulations would maintain a critical security measure to protect consumers and businesses. Moreover, adding flexibility for businesses to protect their records and systems would not harm consumers because they still would be able to understand the data maintained and exercise their rights in accordance with relevant laws.

W249-5

F. Language added in § 999.317(e) prohibiting sharing information obtained for record keeping purposes with third parties should be revised to clarify that businesses should be able to share such information as required by applicable law and for security and anti-fraud purposes.

Subsection 999.317(e)'s prohibition on sharing information maintained for record keeping purposes with third parties may subject businesses to additional security risks and run afoul of existing laws. For example, 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.

W249-6

As noted above, financial institutions are required to maintain and submit certain records to applicable federal and state regulators as part of its compliance program. The language in § 999.317(e), as written, may put financial institutions in a position to have to decide whether to comply with federal and state financial laws or the CCPA. BPI asks that § 999.317(e) be revised to enable businesses to share information maintained for record

[7] *See, e.g.*, 15 U.S.C. § 6802(b)(2); 16 C.F.R. 313.3; Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 66 Fed. Reg. 8,616 (2001).

keeping purposes where required by applicable law and where shared for security and anti-fraud purposes. Such a statement would also support statutory language in Section 1798.145(a)(1-3) of the CCPA that states that the law shall not restrict a business's ability to comply with relevant federal, state, or local laws and cooperate with law enforcement.

W249-6 (cont.)

*****

The Bank Policy Institute appreciates the opportunity to submit comments on the Attorney General's Revised Proposed CCPA Regulations. If you have any questions, please contact the undersigned by phone at [redacted] or by email at [redacted].

Respectfully submitted,

Angelena Bradfield

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

From: Tobin, Timothy P.
To: Privacy Regulations
Subject: Auto Innovators Comments on the Proposed California Consumer Privacy Act Regulations
Date: Tuesday, February 25, 2020 3:10:46 PM
Attachments: 2020-2-25 - Auto Innovators - NPRM Comments_final.pdf

To Whom it May Concern:

Please find attached comments on the CCPA by the Alliance for Automotive Innovation (the "Auto Innovators").

Regards,

Timothy Tobin
Partner

Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004

Tel: +1 202 637 5600
Direct: [redacted]
Fax: +1 202 637 5910
Email: [redacted]
Blog: www.hldataprotection.com
www.hoganlovells.com

Please consider the environment before printing this e-mail.

ALLIANCE FOR AUTOMOTIVE INNOVATION

February 25, 2020

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

RE: Comments of the Alliance for Automotive Innovation on the California Attorney General's Proposed California Consumer Privacy Act Regulations

To Whom It May Concern:

The Alliance for Automotive Innovation ("Auto Innovators") welcomes the opportunity to provide these comments ("Comments") to the Attorney General's Office regarding the Revised Proposed California Consumer Privacy Act Regulations ("Revised Regulations").

Auto Innovators is the leading advocacy group for the auto industry, representing 35 innovative manufacturers and value chain partners who together produce nearly 99 percent of all light-duty vehicles sold in the United States. The members of Auto Innovators include (alphabetically) Aptiv PLC, Aston Martin, Robert Bosch LLC, BMW Group, Byton, Cruise LLC, DENSO, Fiat Chrysler Automobiles, Ferrari S.p.A., Ford Motor Company, General Motors Company, Honda Motor Company, Hyundai Motor America, Isuzu Motors Ltd., Jaguar Land Rover, Karma Automotive, Kia Motors, Local Motors, Maserati, Mazda Motor Corporation, McLaren Automotive, Mercedes-Benz USA, Mitsubishi Motors, Nissan Motor Company, NXP Semiconductors, Panasonic Corporation, Porsche, PSA North America, SiriusXM, Subaru, Suzuki, Texas Instruments, Toyota Motor Company, Volkswagen Group of America, and Volvo Car USA.

Automakers and value chain partners have long recognized the privacy considerations raised by collecting data in association with connected vehicle technologies and services. As a result, Auto Innovators' members have taken proactive steps to protect consumer privacy. In 2014, the Alliance for Automobile Manufacturers, the Association of Global Automakers, and their respective members (which joined together to form Auto Innovators in early 2020) issued the Privacy Principles for Vehicle Technologies and Services ("Principles").[1] The Principles were groundbreaking. The signatories have all committed to meet or exceed the commitments contained in the Principles when offering innovative vehicle technologies and services.

[1] Consumer Privacy Protection Principles (2014) [hereinafter "Principles"], *available at* https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf.

1050 K Street, NW
Suite 650
Washington, DC 20001

AutosInnovate.org

The Alliance for Automotive Innovation and its members appreciate the careful work that the Office of the Attorney General has undertaken in drafting the proposed regulations. In particular, Auto Innovators welcomes the following aspects of the Revised Regulations with just a couple of caveats:

W250-1
- Service providers would be permitted to use personal information received in the course of providing services to develop new and improve current offerings, provided that the use does not include profiling, cleaning data from other sources, or data supplementation. This revision will help participants in the automotive ecosystem develop and improve technologies to support efficiency, security, safety, and other mobility goals.[2]

W250-2
- Businesses that do not collect personal information directly from consumers and can register as data brokers with the Attorney General can rely on their registrations to address notice at collection requirements. This will reduce administrative burdens on all types of businesses.[3] However, we believe this provision can be clarified and improved. Please see the discussion below regarding complications for businesses that do not collect personal information directly from consumers but are unable to register as data brokers as they do not resell the information.

W250-3
- Addressing the challenges of providing privacy disclosures in mobile applications by clarifying that businesses may provide links to privacy notices and Do Not Sell mechanisms within application settings menus.[4]

W250-4
- Permitting businesses to not search for personal information in response to access requests if the information is not maintained in a readily searchable format, is maintained solely for legal or compliance purposes, and is not sold, so long as the business informs the requestor regarding the reasons for not searching for the information.[5] This provision is both helpful and under-inclusive. This will be beneficial to businesses that maintain audio, video, vehicle, or other records that likely contain personal information in formats that are not readily searchable, and where businesses are keeping the information for legal and compliance reasons. However, this provision can be improved to reflect commercial realities that are not privacy intrusive. As reflected in the comments below, Auto Innovators requests that the Attorney General revise the relevant provision so that the exception also applies to businesses where they are not retaining information for legal and compliance purposes, but for future reasonable and internal business purposes.

The remainder of this submission contains requests for modifications to the Revised Regulations, including those noted above. As summarized directly below and discussed more fully in Section I, we present those requests that are of particular relevance to Auto Innovators. Also summarized directly below and addressed further in Section II are issues of general relevance:

Requests and Comments of Particular Relevance to Auto Innovators

W250-5
- In the interest of public safety, reinstating the provision that permits businesses to not disclose personal information in response to an access request if the disclosure creates a substantial, articulable, and unreasonable risk to the security of a consumer's personal information, a consumer's account with a business, or the security of a business's systems or networks, except that the unreasonable risk should also include risks to consumers themselves (such as physical safety);

---

[2] Revised Regulations § 999.314.
[3] Revised Regulations § 999.305(d).
[4] Revised Regulations §§ 999.305(a)(3)(b), .306(b)(1), .308(b).
[5] Revised Regulations § 999.313(c)(3).

W250-6
- Clarifying that if information cannot reasonably be linked with a particular consumer or household due to administrative, technical, or other controls, the information does not constitute personal information;

W250-4 (cont.)
- Not requiring business to search for information in response to requests to know when the information requested is stored in an unsearchable format for future use in support of reasonable, internal business purposes;

W250-2 (cont.)
- Extending § 999.305(d) to apply to businesses that do not collect personal information directly from a consumer;

W250-7
- Permitting businesses to satisfy notice at collection requirements through the use of publicly accessible and readily available website notices where direct, consumer interactions are not technologically feasible as is frequently the case with connected vehicles;

W250-8
- Clarifying whether or, alternatively, how and when user-enabled global privacy controls must be treated as opt-out requests; and

W250-9
- Clarifying that data transfers to affiliates do not constitute "sales."

Requests and Comments of General Relevance

W250-10
- Clarifying that in response to deletion requests, businesses must only delete personal information held by a business at the time of the request;

W250-11
- Modifying the standards for notice of financial incentives to allow businesses to provide flexibility in communicating the terms of such incentives to consumers;

W250-12
- Revising the definition of "signed" to reflect that electronic records must be executed electronically, not merely submitted in electronic form, to constitute a signed writing;

W250-13
- Clarifying the standards for website accessibility; and

W250-14
- Removing the requirement to publicly release statistics to avoid the potential of exposing information to competitors.

In Section III, Auto Innovators reiterates certain comments that its members have issued in prior submissions that do not appear to have been addressed in the Revised Regulations.

Auto Innovators appreciates the Attorney General's consideration of these requests and comments, and respects the efforts the Attorney General is undertaking to develop the regulations. Please contact us if you have any questions or would like to discuss any aspect of these comments.

I. REQUESTS AND COMMENTS OF PARTICULAR RELEVANCE TO THE ALLIANCE FOR AUTOMOTIVE INNOVATION AND ITS MEMBERS

ISSUE 1: Reinstate the provision that permits businesses to not disclose personal information in response to an access request if the disclosure creates a substantial, articulable, and unreasonable risk to the security of a consumer's personal information, a consumer's account with a business, or the security of a business's systems or networks, but expand it to include risks to consumers themselves.

W250-5 (cont.)

The first round of proposed regulations (the "October 2019 Proposed Regulations") contained a provision requiring that businesses not disclose specific pieces of personal information if the disclosure would create 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.[6] The Revised Regulations

[6] October 2019 Proposed Regulations § 999.313(c)(3).

removed this requirement and instead state that businesses are not required to search for information in response to a request to know if certain conditions are met.[7]

By removing the prohibition on disclosing information that creates an unreasonable and articulable risk, the Revised Regulations could be interpreted as requiring businesses to disclose information in response to an access request in situations that may lead to consumer harm, including physical harm. For example, many vehicles are driven by more than one individual, including family members or friends. The disclosure of the precise location history of a vehicle can create stalking or harassment risks, endangering individual or public safety. Accordingly, not only should the Office of the Attorney General reinstate the prior language that included threats to a consumer's personal information, it should extend the provision to cover threats to consumers themselves. Auto Innovators and its members view this as a public safety issue.

W250-5 (cont.)

Businesses in the mobility sector might, in certain specific circumstances, be able to rely on other provisions to protect consumers, such as the proposed household verification requirements under which all current household members jointly request access.[8] However, the risk of releasing precise location data to a fraudster or imposter is greater even with such robust verification procedures. And it is not clear that the provisions will always support reasonable withholding of personal information. For example, an estranged spouse may seek vehicle-related data regarding the other spouse who no longer lives in the same household, so the requirement to obtain consent from all current household members before collecting household data would not address the situation.

Reinstating the provision prohibiting disclosure of information where there is an articulable risk of harm would be consistent with Cal. Civil Code § 1798.145(m), which states that "[t]he rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers."

Auto Innovators therefore requests that the Attorney General reinstate and extend the exceptions to the right to know to include exceptions for individuals' safety or security.

PROPOSAL

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

(c)(3) 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, the security of the business's systems or networks, or the safety or security of the requesting consumer or other individuals.

ISSUE 2: Clarify that if information cannot reasonably be linked with a particular consumer or household due to administrative, technical, or other controls, the information does not constitute personal information.

W250-6 (cont.)

Auto Innovators appreciates the Attorney General's clarification that determining whether information constitutes personal information, "depends on whether the business maintains the information in a manner 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."[9] It is not clear from the language in Section 999.302, though, that the reasonableness of identification may depend on internal controls prohibiting and/or preventing information from being linked to consumers or households.

Automakers, for example, may need vehicle-specific data to effectively assess motor vehicle safety and performance, including to engage in longitudinal research. To mitigate privacy risk, automakers may choose

[7] Revised Regulations § 999.313(c)(3).
[8] Revised Regulations § 999.318.
[9] Revised Regulations § 999.302 (citing the CCPA definition of "personal information").

to maintain such data without including any information that could, on its own, directly identify specific vehicles or their owners. In addition, automakers may implement administrative and technical controls including maintaining data in segregated databases, designed to prevent those with access to the vehicle data from being able to identify specific vehicles or their owners. In such circumstances, the manner in which the data is maintained in combination with the safeguards preventing identification of vehicles or individuals can render the data not reasonably linkable to consumers or households.

Auto Innovators therefore requests that the Attorney General clarify that the reasonableness of linking data to particular consumers or households should take into account both the manner and format in which data is stored and the controls in place to prevent identification.

W250-6 (cont.)

PROPOSAL

§ 999.302. Guidance Regarding the Interpretation of CCPA Definitions

(a) Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "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." For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household due to administrative, technical, or other controls, then the IP address would not be "personal information."

ISSUE 3: Permit businesses to not search for personal information in response to a request to know if the information is not searchable or not readily accessible and if the personal information is maintained only for potential future, internal business purposes.

Section 999.313(c) of the Revised Regulations states that a business is not required to search for personal information in response to a request to know if each of four conditions are all met:

a. The business does not maintain the personal information in a searchable or reasonably accessible format;
b. The business maintains the personal information solely for legal or compliance purposes;
c. The business does not sell the personal information and does not use it for any commercial purpose; and
d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.

W250-4 (cont.)

While the addition of the provision generally is a welcome change, it is unduly restrictive. The change is positive in that it allows businesses to process rights requests more efficiently while focusing on the personal information that may be used in ways that may have an effect on consumers. However, the current language is too restrictive because it undercuts incentives to maintain personal information in systems in privacy-protective ways. For example, businesses in the mobility space may maintain vehicle-related data in non-searchable formats that are not readily accessible in anticipation of potential future research.

Maintaining information for potential future research where not searchable or reasonably accessible by individuals mitigates privacy risk in that it helps ensure that the data will be available to researchers only subject to clear authorization for specific, internal research purposes. Under the Revised Regulations, however, businesses would be required to search the information in response to a request to know unless the information were maintained solely for legal or compliance purposes. Counterintuitively then, if businesses wished to maintain information for internal research or product development, they would have strong incentives to maintain the information in searchable, readily accessible formats to support responding to requests to know.

Auto Innovators therefore requests that the Attorney General revise the provision to allow businesses to not search for personal information maintained in unsearchable or inaccessible formats if the information is maintained for reasonable, internal business purposes.

PROPOSAL

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

(c)(3) In responding to a request to know, a business is not required to search for personal information if all the following conditions are met:

a. The business does not maintain the personal information in a searchable or reasonably accessible format;

b. The business maintains the personal information ~~solely~~ only for one or more of the following purposes:

W250-4 (cont.)

1. Legal or compliance purposes;

2. To detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity;

3. To debug in order to identify and repair errors that impair existing intended functionality;

4. To undertake internal research for technological development and demonstration; or

5. To undertake 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;

c. The business does not sell the personal information and does not use it for any commercial purpose; and

d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.

ISSUE 4: Clarify that businesses that do not collect personal information directly from consumers can address notice at collection requirements by posting publicly and readily available privacy notices.

W250-2 (cont.)

The Revised Regulations delete the previous provision that stated that, "[a] business that does not collect information *directly from consumers* does not need to provide a notice at collection to the consumer."[10] In its place, the Revised Regulations exempt data brokers from having to provide a notice at collection if they register with the Attorney General and meet certain other requirements.[11]

The Revised Regulations do not directly address whether businesses that are not data brokers must comply with notice at collection requirements if they do not collect personal information directly from consumers. In

[10] October 2019 Proposed Regulations § 999.305(d) (emphasis added).
[11] Revised Regulations § 999.305(d).

referring to Section 999.305 (which applies to personal information collected "from a consumer"), businesses could interpret Revised Regulation Section 999.304(b) that way. However, it is not clear what the Office of the Attorney General intended. Some businesses (e.g., automakers and vehicle parts manufacturers) may obtain personal information from sources other than directly from consumers, including from independent dealers or repair facilities, for purposes that do not involve selling the information (e.g., for safety or product improvement) or where there may still be a direct relationship with the consumer and a future sale. Many such businesses may not receive information that enables them to contact consumers for purposes of providing a notice at collection. It would be impossible for such businesses to provide a notice at collection.

W250-2 (cont.)

In situations where businesses do not collect information directly from consumers, they will face substantial challenges in complying with the notice at collection requirements set forth in Section 999.305 of the Revised Regulations. For example, an automotive part manufacturer may receive from dealers or automakers vehicle-related data that contains device identifiers for purposes of assessing safety or performance issues. If the part manufacturers have no direct relationship with consumers, they will find it practically impossible to provide a notice at collection that "consumers will encounter [] at or before the point of collection."[12] Although Section 999.305 provides data brokers (i.e., those that sell personal information obtained from others) with a practical method of addressing notice at collection, no such method is available for businesses that do not resell the information. Moreover, consider that automakers sometimes receive personal information from independent dealers rather than collecting the information directly from consumers. As automakers often have direct relationships with the consumers who buy their vehicles, they would not be eligible to register as data brokers. Moreover, the information collected by dealers and provided to the automakers may not always be sufficient to support automakers in providing a notice at collection.

In light of the fact that data brokers are not the only businesses that may not collect information directly from consumers, Auto Innovators therefore requests that the Attorney General amend Section 999.305 to provide reasonable compliance options for businesses to address notice at collection requirements.

PROPOSAL

§ 999.305. Notice at Collection of Personal Information

(d) If a business ~~that~~ does not collect information directly from consumers ~~is registered with the Attorney General as a data broker pursuant to Civil Code section 1798.99.80, *et seq.*~~ it does not need to provide a notice at collection to the consumer. ~~if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt out.~~ If such a business does not have a direct relationship with consumers, and wishes to sell the personal information, it must register with the Attorney General as a data broker pursuant to Civil Code section 1798.99.80, *et seq.* and include in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt out.

Alternatively, if the Attorney General is not willing to adopt the proposed language above, Auto Innovators requests that the Attorney General revert to the prior proposed language for Section 999.305(d).

[12] Revised Regulations § 999.305(a)(3).

ISSUE 5: Allow for notice at collection requirements to support use of publicly accessible and readily available website notices where direct channels are not technologically feasible.

Section 999.305 of the proposed regulations requires businesses to "provide consumers with timely notice, at or before the point of collection."[13] Such notice must be "readily available where consumers will encounter it at or before the point of collection."[14] And just-in-time notices must be provided when mobile devices collect personal information for purposes that consumers would not reasonably expect.[15]

W250-7 (cont.)

While these provisions may be reasonable in the context of websites or applications running on mobile devices, complying with these requirements is challenging, if not technologically infeasible, for some participants in the connected vehicle or mobility ecosystems. Many legacy vehicle systems and technologies are not capable of displaying notices at collection. Even if vehicles are equipped with displays, the systems may not be capable of receiving updates to display new notices. Moreover, vehicles may change owners without notice to businesses in the automotive ecosystem. Businesses providing connected vehicle services may therefore have limited or no capabilities to directly provide new owners of used vehicles with notice at or before the point of collection.

In light of this challenge, Auto Innovators requests that the Attorney General clarify that the "notice at collection" and "just-in-time" notice requirements are satisfied by a privacy policy posted on the business's website, if the business maintains one and other direct channels for notice are not technologically feasible. And for sales of new devices, Auto Innovators asks that the "notice at collection" and "just-in-time" requirements be satisfied by providing notice when devices are activated and by taking reasonable steps to provide notice when businesses have actual knowledge that a device has changed owners.

PROPOSAL

§ 999.305. Notice at Collection of Personal Information

A business that collects personal information via a device should take reasonable steps to provide notice at collection and any required just-in-time notices to initial or subsequent owners of that device. The business will be deemed to have taken reasonable steps if:

(1) Notice is provided to the new owner via email, device updates, or upon device reset or reactivation; or

(2) The business posts a privacy policy on its website, if reasonable notice is not technologically feasible or cannot be provided by the methods above.

Notice to the owner of a device or account-holder of a service at collection constitutes notice at collection and just-in-time notice as to other users of the device or service.

ISSUE 6: Clarify how user-enabled global privacy controls must be treated as opt-out requests.

W250-8 (cont.)

The Revised Regulations require businesses that collect personal information from consumers online to treat "user-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism," as a request to opt-out if the controls communicate or signal a choice to opt-out.[16] However, the Revised Regulations do not clarify how businesses will be notified regarding the existence of such signals and how businesses can determine whether a signal reflects a "user-enabled global privacy control," which is not defined in the Revised Regulations.

---

[13] Revised Regulations § 999.305(a)(1).
[14] Revised Regulations § 999.305(a)(3).
[15] Revised Regulations § 999.305(a)(4).
[16] Revised Regulations § 999.315(a).

There are many privacy controls provided to users by browsers and operating systems at different levels of the user experience that mean different things in different contexts (e.g., just-in-time alerts on a mobile platform may stop targeted advertisements from being served but not stop data from being collected). Given the lack of consistency, a legal requirement to treat any privacy setting as an opt-out for sale creates an unworkable situation for businesses. In the absence of a multi-stakeholder process for creating or recognizing signals, businesses that collect information online through websites, mobile applications, connected vehicles, or other connected devices will not know what signals to recognize and honor.

Auto Innovators therefore requests that the Attorney General remove the requirement relating to opt-out signals. Alternatively, Auto Innovators requests that the Attorney General clarify which signals should be treated as opt-out requests or call upon industry to develop signals that will be clearly recognizable and interoperable. Otherwise, the Office of the Attorney General will be inviting widespread confusion, uncertainty and technological challenges over how to treat signals.

W250-8 (cont.)

PROPOSAL 1

§ 999.315. Requests to Opt-Out

(a) A business shall provide two or more designated methods for submitting requests to opt-out, including an interactive form 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, or a form submitted through the mail. ~~, and user-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information.~~

PROPOSAL 2

§ 999.315. Requests to Opt-Out

(a) A business shall provide two or more designated methods for submitting requests to opt-out, including an interactive form 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 global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information. The Office of the Attorney General shall publish a list by [month] of each year that specifies the signals that businesses must treat as valid opt-out requests and the sources of such signals. No other signals will be treated as valid opt-out requests unless businesses disclose that they will recognize specific, alternative signals.

ISSUE 7: Clarify that data transfers to affiliate businesses do not constitute "sales."

The CCPA sales opt-out does not impact data sharing between entities that are under common control and share common branding.[17] However, not all organizations that are closely affiliated (such as parent organizations and their subsidiaries) would be considered the same business under the CCPA as they may not share common branding. As a result, some subsidiary-to-parent data sharing arrangements may be disrupted by CCPA sales opt-outs.

W250-9 (cont.)

[17] *See* Cal. Civ. Code § 1798.140(c)(2).

W250-9 (cont.)

This is particularly problematic for certain global companies (including some automakers) that conduct operations in the United States via a subsidiary that is controlled by a parent company that does not share common branding with the U.S. entity, or for companies with numerous separate legal entities each with a different function. Sharing information with the parent company may be vital, particularly where the U.S. entity is primarily a distributor and the parent company manufactures the vehicles. The U.S. distributor may maintain direct relationships with consumers and transfer information to the parent company for product development and research. Other sharing arrangements among affiliates that in some cases may not be same-branded may also be vital to operations. Such transfers typically do not involve the exchange of money but further the common interests of the enterprise. But where the entities do not share common branding, there is a risk that the sales opt-out could disrupt the data sharing for important product development, safety, and performance purposes.

Auto Innovators therefore requests that the Attorney General permit businesses to continue sharing information with affiliates after receiving sales opt-out requests.

PROPOSAL

§ 999.315. Requests to Opt-Out

(e) In responding to a request to opt-out, ... A business may continue sharing personal information with its affiliates after receiving a request to opt-out.

II. REQUESTS AND COMMENTS OF GENERAL RELEVANCE

ISSUE 8: Clarify that deletion requests should apply only to personal information held by a business at the time of the request.

W250-10 (cont.)

Section 999.313(d)(5) contains a provision that could be interpreted as requiring businesses to honor deletion requests by deleting personal information collected after the request is completed, even if the consumer elects to engage further with the business or if the business otherwise obtains personal information about the consumer from a third party. Specifically, Revised Regulation § 999.313(d)(5) states in part: "A business may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from the business's records."

Auto Innovators does not believe the Office of the Attorney General's intent was to create an obligation to delete information once a consumer has made a deletion request if there is a new interaction with the consumer or new collection of personal information about the consumer. However, this provision could be interpreted as requiring businesses to delete personal information related to a consumer that is collected after the deletion request is honored. This goes beyond the statutory requirement for deletion, which applies only to information that "the business *has* collected from the consumer."[18] Moreover, a prospective interpretation of the deletion right would be counterintuitive in circumstances where consumers elect to reengage with a business after requesting the deletion of personal information. Auto Innovators therefore requests that the Attorney General clarify that consumers' right to deletion only applies to information a business has collected about a consumer at the time the request is submitted.

PROPOSAL

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

(d)(5) A business may retain a record of the request for the purpose of legal compliance ~~ensuring that the consumer's personal information remains deleted from the business's records~~.

[18] Cal. Civ. Code § 1798.105(a) (emphasis added).

ISSUE 9: Allow for flexibility in addressing notices of financial incentives.

Under the Revised Regulations, a notice of financial incentive must describe, "the value of the consumer's data" and "[a]n explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data."[19] Furthermore, Section 999.336 restricts businesses' opportunities to provide financial incentives to consumers by stating that, "[i]f a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference."

W250-11 (cont.)

This requirement may prove impossible to meet for commonplace and reasonable practices that may be considered financial incentives, almost all of which are consumer friendly practices. For example, many businesses may offer a coupon for consumers who sign up to receive email newsletters or other promotional communications. The precise value of a coupon that offers a percentage off of an initial purchase cannot be calculated in advance. The coupon will be worth more to consumers that spend a substantial amount on their initial purchases. Businesses may determine that a discount offer is worthwhile based on the value of attracting and engaging new customers, rather than on the value to the business of the consumer's email address or other contact information that is used to provide the consumer with the discount.

Auto Innovators therefore requests that the Attorney General allow businesses greater flexibility in providing notices of financial incentives.

PROPOSAL

§ 999.307. Notice of Financial Incentive

(b)(5) An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, to the extent that the business bases the financial incentive on the value of consumers' data, 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.

ISSUE 10: Revise the definition of "signed" in § 999.301(u) to clarify that electronic records must be executed electronically, not merely submitted in electronic form, in order to qualify as being signed.

W250-12 (cont.)

Section 999.301(u) of the regulations defines "signed" as a document that, "has either been physically signed or provided electronically per the Uniform Electronic Transaction Act." The proposed definition could be interpreted to mean that a record that is "provided electronically" counts as a signed record even if the record has not been executed with an electronic signature. However, this does not reflect current law regarding electronic signatures. The Uniform Electronic Transaction Act defines an electronic signature as, "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."[20] Auto Innovators requests that the Attorney General revise the definition of "signed" to reflect that the document must be physically signed or executed with an electronic signature per the Uniform Electronic Transaction Act.

[19] Revised Regulations § 999.307(b).
[20] Cal. Civ. Code 1633.2(h).

PROPOSAL

W250-12 (cont.)

§ 999.301. Definitions

(u) "Signed" means that the written attestation, declaration, or permission has either been physically signed or executed with an electronic signature and provided electronically per the Uniform Electronic Transactions Act, Civil Code section 1633.7 et seq.

ISSUE 11: Provide for flexibility in determining appropriate standards for website accessibility.

Auto Innovators supports the Attorney General's goal of ensuring that notices will be reasonably accessible to all consumers, including those who are differently abled and may not be able to consume information through traditional formats. However, the Attorney General's requirement that businesses meet industry accessibility standards[21] is unclear. At this time, many industries lack clear standards for accessibility. Some companies may have adopted version 2.1 of the Web Content Accessibility Guidelines cited in the Revised Regulations. Others may have adopted version 2.0 or some other standard. Even for companies that have adopted version 2.1, the Web Content Accessibility Guidelines establish different levels of accessibility. Some businesses may choose to adhere to Level A, others may adhere to Level AA, and still others may adhere to Level AAA. There is no single standard of compliance under the Guidelines.

W250-13 (cont.)

Auto Innovators therefore requests that the Attorney General clarify that there is no specific standard for accessibility requirements and instead require businesses to take reasonable steps to address accessibility in a manner that reflects changing technologies and shifting industry best practices.

PROPOSAL

§ 999.305. Notice at Collection of Personal Information

(a)(2)(d) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards~~, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Consortium, incorporated herein by reference~~ or undertake reasonable efforts to address accessibility in light of available technologies and resources. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.

ISSUE 12: Remove the requirement to publicly release statistics to avoid the potential of exposing information to competitors.

The Revised Regulations require that some businesses must compile metrics regarding rights requests that they have received and how they have handled those requests, including the number of requests to know, delete, and opt-out of sales that a business has received and the time a business took to respond to such requests.[22] Sharing these statistics publicly may lead to businesses being forced to expose information about their processes to competitors. A statement of the mean or median number of days a business takes to process a request could be used, for example, to embarrass a company in an attack ad by a competitor.

W250-14 (cont.)

[21] § 999.305(a)(2) proposes the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Consortium as the standard against which businesses will be held. These standards are also proposed in §§ 999.306(a)(2)(d), .307(a)(2)(d), and .308(a)(2)(d).

[22] Revised Regulations § 999.317(g).

Auto Innovators does not object to a requirement to track this information and share it with the Attorney General annually or upon request, as we recognize the importance of keeping accurate records for compliance and enforcement purposes. However, this requirement exceeds the scope of the California Consumer Privacy Act, which requires only that businesses process rights requests in accordance with the statute[23] and not that they publish the results of these efforts.

Auto Innovators therefore requests that the Attorney General remove the requirement publish metrics regarding compliance with rights requests publicly from the regulations.

W250-14 (cont.)

PROPOSAL

§ 999.317. Training; Record-Keeping

~~(2) Disclose, by July 1 of every calendar year, 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) In its disclosure pursuant to subsection (g)(1), a business may choose to identify the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.~~

~~(4) A business may choose to compile and disclose the information required by subsection (g)(1) for requests received from all individuals, rather than requests received from consumers. The business shall state whether it has done so in its disclosure and shall, upon request, compile and provide to the Attorney General the information required by subsection (g)(1) for requests received from consumers.~~

III. IMPORTANT ISSUES RAISED IN PRIOR SUBMISSIONS AND SEEMINGLY NOT ADDRESSED IN THE REVISED REGULATIONS

Auto Innovators wishes to reiterate and support previous comments filed by the Alliance of Automobile Manufacturers and the Association of Global Automakers, who are now members of Auto Innovators. In particular, we urge the Attorney General to consider the following:

ISSUE 13: Recognize that trade secrets do not need to be disclosed in response to requests to know.

W250-15

Section 1798.185(a)(3) of the CCPA requires that the Attorney General, "[e]stablish[] any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights…."

Today's vehicles deploy a variety of sensors and other technologies that collect information relating to vehicle safety, performance, efficiency, and security. Automakers devote substantial resources to determine what combination of sensors, what frequency of data collection, and what combination of information will best address those issues. Under the CCPA, consumers have the right to request that businesses disclose the specific pieces of personal information that businesses have collected.[24] For automakers, and other

[23] Cal. Civ. Code §§ 1798.100, .106, .120.
[24] Cal. Civ. Code § 1798.110.

businesses, disclosing all of the specific pieces of personal information, particularly if linkages between or uses of sensor data are revealed, would expose proprietary or trade secret information. Auto Innovators therefore requests that the Attorney General prevent businesses from being forced to disclose their proprietary or trade-secret information.

W250-15 (cont.)

PROPOSAL

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

(c)(12) A business shall not be required to disclose information that would reveal proprietary Information or trade secrets In response to a request to know.

ISSUE 14: Allow businesses to respond to requests to know specific pieces of personal information in a format that is useful and actionable for consumers.

As a practical matter, much of the data collected by sophisticated devices, such as vehicles, is not in a format that is easily understandable for consumers. For example, average consumers are unlikely to be able to meaningfully engage with detailed sensor data in the format that it is collected by a vehicle, especially given the volume of the information. Auto Innovators therefore requests that the Attorney General permit businesses to deliver personal information in response to requests to know specific pieces of personal information in a format that is useful and actionable for average consumers.

W250-16

PROPOSAL

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

(c)(13) In responding to a request to know specific pieces of personal information, a business may deliver the information to the requestor in a format that is useful and actionable for average consumers.

ISSUE 15: The regulations should include an exception to sharing for emergency purposes.

Under the broad definition of "sale" in the CCPA,[25] the sharing of consumer personal information between an automobile manufacturer and a provider of emergency or roadside assistance services could be considered a sale. As such, if a consumer registered an opt-out with a manufacturer, that could limit the manufacturer's ability to share information with vendors as necessary to provide emergency services.

W250-17

PROPOSAL

§ 999.315. Requests to Opt-Out

(i) A request to opt-out does not apply when information is exchanged for the provision of emergency response services.

ISSUE 16: The regulations should include an exception for sharing between members of the mobility ecosystem and specifically between vehicle manufacturers and dealers.

W250-18

Amendments to the CCPA exempt from the sale opt-out requirements vehicle or ownership information shared between dealers and vehicle manufacturers for the purpose of effectuating "a vehicle repair covered

[25] Cal. Civ. Code § 1798.140(t)(1).

by a vehicle warranty or a recall" if the information is not used for any other purpose.[26] This exemption does not, however, cover sharing between dealers and vehicle manufacturers for non-warranty or non-recall services. Many industries rely on similar data sharing between franchisees and franchisors to obtain an exception for sharing between commonly branded entities for purposes consistent with reasonable consumer expectations.

W250-18 (cont.)

PROPOSAL

§ 999.315. Requests to Opt-Out

(j) A request to opt-out does not apply when information is exchanged between parties whose commercial conduct is related to the degree that informed consumers would reasonably expect the parties to share information for the purposes of benefitting the consumer with regard to safety, security, repair, performance, or efficiency issues.

ISSUE 17: The regulations should include an express exception for retaining vehicle-related data for research or product development regarding safety, quality, performance, efficiency, or security issues.

The CCPA exceptions for deletion include using personal information internally for purposes that are compatible with the context in which the information was collected or for purposes that align with the consumer's expectations.[27] However, given the importance of retaining vehicle-related data for research and product development, it would benefit businesses in the automotive and mobility sectors, as well as consumers, for there to be an express exception for denying deletion requests with respect to information used for such purposes.

W250-19

PROPOSAL

§ 999.313 Responding to Requests to Know and Requests to Delete

(d)(8) The collection and internal use of personal information for analysis related to safety, quality, performance, efficiency, or security by a business or service provider constitutes "solely internal uses that reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business" under California Civil Code §1798.105(d)(7) and therefore shall not be subject to a Request to Delete, as long as this collection and use is disclosed to consumers.

Thank you for your consideration,

Charles H. Haake
Vice President and General Counsel
Alliance for Automotive Innovation

[26] Cal. Civ. Code § 1798.145(g)(1).
[27] Cal. Civ. Code 1798.105(d).

From: Rudolph, Matthew
To: Privacy Regulations
Subject: CCPA Revised Regulations Comments
Date: Tuesday, February 25, 2020 3:07:46 PM
Attachments: image013.png
image015.png
HERE Comments to Revised CCPA Regulations.pdf

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

We respectfully submit the attached comments pertaining to the proposed revised regulations concerning the California Consumer Privacy Act.

Should you require any further information, please do not hesitate to let us know.

Best Regards,

Matthew Rudolph on behalf of HERE Technologies

Matthew Rudolph
Privacy Officer
HERE Technologies
425 W. Randolph St., Chicago, IL 60606
41° 53' 55" N -87° 38' 19" E

HERE CCPA Regulations Comments

HERE TECHNOLOGIES – COMMENTS ON DRAFT REGULATIONS FOR THE CALIFORNIA CONSUMER PRIVACY ACT

This document outlines the comments of HERE Technologies regarding key aspects of the revised California Consumer Privacy Act (the "CCPA") draft regulations. It expresses our concerns about some crucial elements of the CCPA draft regulations and the negative impact they might have on the functioning of the location services provided by HERE Technologies, their impact on innovation and therefore on the benefits of these services for end users.

About HERE Technologies

HERE Technologies ("HERE") is a global leader in digital location technology. Our products and services enable people, enterprises and cities around the world to harness the power of location and create innovative solutions that make our lives safer, more efficient, productive and sustainable. We transform information from devices, vehicles, infrastructure and many other sources into real-time location services that play a key role in how we move, live and interact with one another. HERE's vision is to create an autonomous world for everyone, based on open availability of the vast amounts of data that will be generated by the hundreds of billions of connected devices in our increasingly connected world.

HERE Technologies is fully committed to respect privacy and to comply with all applicable laws covering data protection and privacy. As a company which is already subject to robust privacy regulations such as the European General Data Protection Regulation (the "GDPR"), we support and are prepared to comply with consumer privacy protections like those represented in the CCPA. We are, however, concerned that some elements of the newly revised draft CCPA regulations will have detrimental effects on the functioning of our location services and on the benefits of these services for our end users. Moreover, some of the proposed requirements risk hampering innovation and may therefore have a negative impact on the further development and maximization of location services in California.

We wish to highlight the following key aspects of the revised CCPA draft regulations that are of particular concern to HERE Technologies and the location services we provide:

I. Restrictions Regarding Service Providers

Clarification regarding use of personal information for product improvement purposes

HERE applauds the addition of 999.314(c)(3), which permits service providers to use personal information for internal product improvement purposes. We believe this inclusion is ultimately

W251-1

beneficial to both companies and consumers. It allows non-offensive product improvement activities to take place to the benefit of all parties, and will ultimately simplify the privacy landscape which consumers face. If product improvement were not allowed, more companies would insist on acting as businesses, which would disadvantage consumers by multiplying the number of independent parties involved in a given service.

However, HERE has concerns about the revised section 999.314(c)(3). The final clause "...or cleaning or augmenting data acquired from another source" is likely to have unintended impacts on platform business models, where product improvement data is derived from multiple customers' use of the same platform. The language as written is also over-inclusive, in that it forbids augmenting data in general, rather than only personal information. HERE would propose the following modifications:

W251-1 (cont.)

> "(3) [...] or cleaning or augmenting ~~data~~ personal information acquired from another source for purposes of building or modifying household or consumer profiles, or to re-identify any previously de-identified information."

<u>Authorization of service providers to process personal information for de-identification purposes</u>

Section 999.314(c)(5) should be modified to include Civil Code section 1798.145(a)(5) in addition to the code sections currently included. This would clarify that service providers are permitted to collect and use de-identified and aggregated information. We believe that this change would ultimately be a benefit both for consumers and for businesses. We believe that explicitly including collection and use of this information will benefit businesses by addressing confusion we have observed among many companies working to implement the CCPA, who are concerned that processing for de-identification purposes represents a separate processing purpose not permitted by the CCPA. We believe that it will benefit consumers by further incentivizing companies to develop anonymization technologies.

W251-2

<u>Service provider liability for data sales</u>

The revisions to Section 999.314(d) of the draft regulations stipulate that a service provider must not sell data on behalf of a business when a consumer has opted out. While HERE agrees with what it understands to be the spirit of the requirement (ensuring service providers comply with opt-out requests), we are concerned that as written, this requirement may impose liability on service providers where they have not been informed by the business that the individual has opted out. A service provider should not be independently liable where it is simply following the instructions of the responsible business.

W251-3

A service provider is already obligated under the revised section 999.314(c) not to use or disclose personal information except as contracted with the business. To the extent that a service provider exceeds or violates the business's directions regarding sale of data, the service provider has already violated its obligations under the CCPA. Accordingly, HERE believes that this section 999.314(d) should be deleted.

II. Methods of Exercising Opt-Out Rights

<u>"Browser Setting" as Opt-Out Request</u>

W251-4

HERE remains concerned regarding the requirement in § 999.315(c) related to treating a browser plugin or privacy setting as an effective opt-out request. While the rationale stipulated within the Initial Statement of Reasons regarding businesses ignoring or rejecting consumer tools is appreciated, we do not believe that this requirement is feasible as formulated. Any moderately experienced developer can create a browser plugin which provides a signal purporting to be an opt-out request. This may result in businesses being forced to pursue multiple unclear, non-standardized functionalities, which becomes more complicated as more groups propose new standards. Simply put, it should take more than an isolated party merely introducing a technology to make adoption of that specific technology legally mandatory for all businesses operating in California.

W251-4 (cont.)

As an alternative, HERE would propose establishment of a certification program for global opt-out technologies. This would allow consumer and industry groups to collaboratively establish opt-out frameworks and technologies, which upon a reasonable time period after certification would constitute a mandatory opt-out request. These could be structured to be global in nature, or tailored to specific technologies, use cases, or industries. Potential language to establish this program is proposed in Exhibit 1 to these comments. Additional language has been included in the proposal to address practical issues HERE anticipates in the design, deployment and ongoing maintenance of the opt-out technology, which HERE believes would become critical problems if mandatory opt-out mechanisms are not managed in a controlled manner.

Subversion of opt-out requests

In many instances an individual's opt-out decision may be implemented through a device-based control, such as an in-application setting or browser cookie. Where a user submits an opt-out request through a webform, toll free number, or email address, where the opt-out setting is a device-based control it will not be possible for the business to directly change the control. Rather, the user must alter the setting on their device. HERE requests clarity on this point in new section 999.315(c). Data which is collected and sold based on the ordinary operation of the prior setting while the user navigates to that setting to modify it should not be considered subverting or impairing the consumer's decision. HERE respectfully requests that the following language be added to the end of section 999.315(c): "Where a business has utilized a user-enabled privacy control, such as a privacy or device setting, the business may instruct consumers who submit an opt-out request via other methods regarding how to modify the relevant setting. Continued operation of the prior privacy or device setting before the consumer changes the prior setting is not considered a subversion or impairment of the consumer's decision to opt out."

W251-5

HERE is pleased to submit these comments on the Draft Regulations for the California Consumer Privacy Act and we would be happy to provide additional information or to answer any questions the Attorney General's Office may have.

For further information or queries, please contact Leo Fitzsimon at [redacted] or the HERE Technologies privacy team at privacy@here.com.

Exhibit 1: Certification of Privacy Controls

Proposed text to modify Section 999.315 by replacing subsections (c), (d), and (e) is as follows:

(c) Approval of Opt-Out Privacy Controls

(1) Submission of privacy controls. Industry groups or other interested persons may apply to the Attorney General for approval of proposed standardized opt-out privacy controls. If the Attorney General chooses to advance a proposal for potential certification, the Attorney General will publish a document seeking public comment on the application.

(2) Submission guidelines. A proposed opt-out mechanism's request for approval shall be accompanied by the following:

(i) A detailed explanation of the mechanism's technical capabilities and mechanisms that will be used to ensure that the actions requested are communicated to consumers and businesses in a manner that is clear, comprehensive, and actionable;

W251-4 (cont.)

(ii) A copy of the full technical specifications of the privacy control for which approval is sought and any accompanying commentary;

(iii) A statement explaining:

(1) How the privacy control, including the technical specifications, meets the requirements of this section;
(2) How the privacy control provides effective enforcement of the requirements;
(3) How the privacy control is designed in a manner to ensure ease of integration and interoperability with the software and systems of potentially impacted businesses;
(4) How the future maintenance and development of the privacy control will be accounted for; and
(5) What consumer need the privacy control will fulfill, why the control is better suited to fulfill that need than other existing opt-out mechanisms, any what differentiates the control from other privacy controls which have already been approved.

(3) Criteria for approval of privacy controls. Proposed privacy control must meet the following performance standards:

(i) The privacy control must clearly communicate or signal that a consumer intends to opt out of the sale of personal information. The privacy control shall require that the consumer affirmatively select their choice to opt-out and shall not be designed with any pre-selected settings.

(ii) The privacy control must be designed to readily integrate with existing technologies in a way which is not unreasonably burdensome for impacted businesses to implement;

(iii) There must be a reasonable plan for the ongoing support and development of the privacy control to ensure its continued applicability and interoperability with relevant technologies; and

(iv) There must be a compelling, unmet consumer need which is fulfilled by the privacy control.

(4) Post-approval modifications to privacy controls. Proposals for changes to approved privacy controls must be submitted for approval in the manner required for initial approval under this section. The statement required under paragraph (c)(2) of this section must describe how the proposed changes affect existing functionality of the privacy controls.

W251-4 (cont.)

(5) Publication and revocation of approval. The Attorney General shall maintain a publicly available list of approved privacy controls. The Attorney General may at any time upon request or upon its own initiative remove a privacy control from its list, upon which event the privacy control will no longer be considered an approved privacy control pursuant to this section.

(6) Implementation period for approved privacy controls. Effective one year following the date approval of the privacy control is published by the Attorney General, opt-out signals communicated by the privacy control will be considered valid requests submitted pursuant to Civil Code section 1798.120 for the browser or device communicating the opt-out signal.

(7) Exemptions. A business is excused for failure to comply with an approved privacy control in the following circumstances:

(i) Where the business has made available an updated version or feature which would enable compliance with the approved privacy control, but the consumer has failed to use the updated version or feature; and

W251-5 (cont.)

(ii) Where the software or device which receives the communication from the privacy control was created prior to the effective date of the privacy control, and the software or device cannot be updated through reasonable efforts to accommodate the privacy control, including where the software or device is deployed remotely in a manner which impedes delivery of updates.

From:	Matt Akin
To:	Privacy Regulations
Subject:	Comments on Proposed California Consumer Privacy Act Regulations (ACLHIC - ACLI)
Date:	Tuesday, February 25, 2020 3:03:53 PM
Attachments:	ACLHIC - ACLI CCPA Regs Letter.pdf

Dear Attorney General Becerra:

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

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

Sincerely,

Matt Akin
Political Director
ACLHIC
1201 K Street, Suite 1820
Sacramento, CA 95814
PH: [redacted]
FX: (916) 442-1730
Website: www.aclhic.com

February 25, 2020

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

Re: *Comments on Proposed California Consumer Privacy Act Regulations (February 10, 2020)*

Dear Attorney General Becerra:

The American Council of Life Insurers ("ACLI") and the Association of California Life and Health Insurance Companies ("ACLHIC") respectfully submit the following comments on behalf of our members. We appreciate the thoughtful and deliberative process your office has undertaken for the development of the proposed regulations and welcome the modifications and improvements in the second draft of the proposed regulations released February 10, 2020.

As we mentioned in our initial letter, life insurers have historically served as conscientious stewards of our customers' highly sensitive personal information. We abide by and support strong consumer privacy laws. We have managed consumers' confidential medical and financial information appropriately for decades, and in the instance of several our member companies, a couple of centuries. We look forward to working with you and lending our industry's historical expertise to this weighty issue.

Executive Summary

- *Insurers have a strong and historic consumer privacy track record*
- *Sufficient time is needed for regulatory compliance*
- *The regulations should be harmonized with existing privacy laws and regulations*
- *Regulatory enforcement must be prospective*

The California Consumer Privacy Act of 2018 ("CCPA") is a complex and comprehensive law. We appreciate the clarification and guidance provided by the proposed re-drafted regulations. The amendments in the latest draft were responsive to many stakeholder concerns. We have a few remaining issues outlined below which we believe will make the regulation workable for businesses and ultimately easier for consumers.

Compliance Deadline

As we stated in our December 5, 2019 letter, we strongly believe that the date for compliance with these rules should be at least 2 years after they have been finalized and that the rules should be enforced solely on a prospective basis and not be retroactively applied. The underlying California privacy law has not yet stabilized as borne out by the number of legislative proposals currently being considered in Sacramento and by the

W252-1

comprehensive and material new changes proposed in the *California Privacy Rights Act of 2020* ballot initiative. It is possible numerous provisions of the underlying law will be materially changed if the ballot initiative passes this year, potentially resulting in the regulations being rendered wholly or in part unenforceable. Moreover, the proposed regulations are broad and contain new substantive provisions. Companies must be provided with reasonable time to come into compliance with these comprehensive rules. W252-1 (cont.)

Article 1: General Provisions

The many clarifications to the requirements under the general provisions in the most recent draft regulations have been very helpful. We appreciate the distinction made between employee information and personal information with the addition of the definitions of "Employment-related information" and "Employment benefits" in §999.301 (h) and §999.301 (i). Our members provide a variety of employee benefits for which personal information is needed, including beneficiary information and in some instances information about an employee's dependent. While the definition of "employment benefits" includes beneficiaries, it does not mention spouses and children. We think that the definition could be clarified with an addition for "dependents" to read: W252-2

> §999.301(h) "'Employment benefits'" means retirement, health, and other benefit programs, services, or products to which a consumer and their dependents or their beneficiaries receive access through the consumer's employer."

We think this addition brings clarification to the scope of information under employment benefits and assures the smooth operation of needed employer-provided benefit plans.

Article 2: Notice

We appreciate that the new draft regulations take a more flexible approach to consumer notice and have a couple of additional clarifications which we believe will improve the notice provisions.

Timing of Notice

Subsection 999.305(d) appears to be an attempt to clarify who provides notice when the information is not collected directly by a business from a consumer and to ensure that notice is provided in all instances. The revised language which adds the concept of registered data brokers was not quite clear and, therefore, we would suggest deletion of the current language in (d) and the substitution of the following, which is we believe a clearer representation of the intent of the provision:

> §999.305(d) (1) A business that does not collect information directly from consumers must still provide a notice to the consumer at the time the business collects consumer information from a third party. This section does not apply to:
>
> > (a) A business that is registered with the Attorney General as a Data Broker, pursuant to Civil Code section 1798.99.80 *et seq*, if the business included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out; or
> >
> > (b) A business that collects consumer information from a Data Broker who is registered with the Attorney General and provided the required instructions to consumers in compliance with subsection (a).
>
> (2) A business that is not required to provide notice to consumers at the time of collection under subsection (d)(1)(b), above, is subsequently required to provide notice to consumer of their right to opt-out in accordance with section 999.306, prior to the resale of consumer personal information.

W252-3

We believe the language above clarifies the intent of §999.305(d).

Privacy Policy

Consumers have been receiving privacy notices in established, limited and stabilized formats, such as under Gramm-Leach-Bliley, for years. We appreciate the flexibility in the current draft regulations which would permit companies to use existing, well tested, formats for compliance with CCPA making new notices more understandable. It is beneficial to both companies and consumers for businesses to use appropriately modified existing and familiar formats. W252-4

Article 3: Business Practices for Handling Consumer Requests

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

Responding to Requests to Know and Requests to Delete

While we still assert that the requirement in §999.313(a) to confirm the receipt of a request to know or delete personal information is inconsistent with the CCPA and overly burdensome to businesses, the change made to the most recent draft regulations, permitting the confirmation to be made in the same manner as the request, makes this requirement more workable. In many instances if the consumer has submitted a request, then they have already been verified (e.g. they have logged in to their online account). However, we are seeking additional clarification in §999.313(b) regarding the timeframe for a submitted request. Under the current language in the regulation, the 45-day clock starts as soon as a request is submitted. Early experience with CCPA has shown that there can be questions as to what constitutes a request. To clarify for consumers and businesses, the 45-day clock should start when a request is submitted via "designated methods". W252-5 W252-6

In addition, Section 999.313(c)(2) permits a business to deny a consumer's request to disclose categories of information if it cannot verify the person making the request. If a company denies a request, the subsection requires that the business provide the person with the company's general business practices regarding collection, maintenance and sale of personal information. As we mentioned in our December 5, 2019 letter, this is an example of why one, single, comprehensive notice makes sense. With one notice, the consumer can find everything in one place, including the general business practices and how to submit a request. Repeating information, or putting additional information in the communication denying a request, is unnecessary and bureaucratic. We would therefore suggest the deletion of the last sentence in §999.313(c)(2). W252-7

The clarification to the language in §999.313(d)(1) regarding responding to requests to delete is helpful, however we believe the requirement regarding a business's obligation to ask the consumer if they would like to opt-out of the sale of their personal information should be moved to §999.313(d)(2) with the other requirements regarding a consumer's request to delete. W252-8

While we also appreciate the clarification to §999.313(d)(5), we believe the way the language is currently drafted could create confusion. We do not believe it is the intent of the drafters, however the new language may be read to suggest that a business has an ongoing obligation to ensure any data collected after the deletion request is then deleted under a past request. Obviously, there could be circumstances in the future, e.g., a new business relationship with the consumer, in which it would be appropriate for a business to retain the consumer's personal information. The solution to this inadvertent confusion might be to delete the last sentence under §999.313(d)(5). W252-9

As we stated in our December 5, 2019 comment letter, to achieve functional efficiencies, compliance with CCPA should be easy to automate and standardize. Unfortunately, a number of provisions in the draft regulations continue to make the development of productive compliance systems difficult. An example is §999.313(d)(6) which requires businesses to provide a detailed explanation when they deny a consumer's request to delete personal information. If a consumer believes a denial is inappropriate, they can exercise administrative remedies, for instance with the California Department of Insurance. And, if a business does not comply with the law, there are appropriate regulatory enforcement mechanisms. It is our position that §999.313(d)(6)(c) exceeds the scope of the CCPA and, therefore, should be deleted. W252-10

Conclusion

As we mentioned in our December 5, 2019 letter, not only is our industry a robust contributing member of the California economy, we are proud of the fact that the financial services industry has traditionally been a conscientious and responsible guardian of customers highly vulnerable personal information. Our industry has appropriately managed consumers' confidential medical and financial information for decades and is supportive of robust and sensible consumer privacy requirements.

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

Sincerely,

John W. Mangan
Regional Vice President, State Relations
American Council of Life Insurers

Matthew R. Powers
Vice President
Association of California Life and Health Insurance Companies

From: Kyla Christoffersen Powell
To: Privacy Regulations
Subject: CJAC comments on CCPA regulations as revised 2-10-20
Date: Tuesday, February 25, 2020 2:48:34 PM
Attachments: image001.png
CJAC Comments CCPA Revised Regulations 2-25-20.pdf

Dear Attorney General Becerra and Ms. Kim,

Attached are Civil Justice Association of California's comments on the proposed CCPA regulations, as revised February 10, 2020.

Thank you,

Kyla Christoffersen Powell
President and Chief Executive Officer
Mobile [redacted] | www.cjac.org

CIVIL JUSTICE
ASSOCIATION OF CALIFORNIA

CIVIL JUSTICE
ASSOCIATION OF CALIFORNIA

February 25, 2020

Xavier Becerra, Attorney General
California Department of Justice
1300 I Street, Suite 1740
Sacramento, CA 95814

Lisa B. Kim, Privacy Regulations Coordinator
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 by the Civil Justice Association of California on Proposed Regulations for the California Consumer Privacy Act, as revised February 10, 2020*

Dear Attorney General Becerra:

The Civil Justice Association of California ("CJAC") is a more than 40-year-old nonprofit organization representing a broad and diverse array of businesses and professional associations. A trusted source of expertise in legal reform and advocacy, we confront legislation, laws, and regulations that create unfair litigation burdens on California businesses, employees, and communities.

As noted in our prior comments, many businesses attempting to comply with the CCPA find it complex and vague, making implementation difficult. CJAC appreciates the additional clarifications the Office of the Attorney General provided in the February 10, 2020 revisions, such as clarifying the definition of personal information, but we are concerned the revised regulations still have gaps or impose unnecessary burdens. Below, we itemize our concerns and requests.

1. **The regulations should provide that enforcement is effective on January 1, 2022 and prospective only given the complexity and burden of implementation.**

CJAC reiterates our request for additional time for businesses to implement the regulations before they are enforced, to January 1, 2022. The latest revision does not specify an extended effective date for enforcement purposes, notwithstanding requests from CJAC and a multitude of other commenters to so do.

W253-1

While the CCPA states the Attorney General should adopt regulations by July 1, 2020 and enforce no earlier than that date, there is nothing limiting the Attorney General from specifying an extended enforcement date. Given the complexity of the CCPA and the proposed regulations and the substantial compliance burden on businesses, a delayed enforcement date is necessary and justified. For the same reasons, the regulations should also provide that all enforcement of the CCPA and the regulations is prospective only, from the extended enforcement date.

If not an overall extension, at a very minimum, the Attorney General should provide delayed enforcement for the regulations that are more burdensome and complex to implement, such as the requirement to treat global controls as opt-out requests under section 999.315. W253-2

2. Businesses should not be required to treat global privacy controls as opt-out requests because it is technologically unworkable and limits consumer choice. (Section 999.315(a), (d).)

We continue to oppose the requirement that a business detect and treat global privacy controls, such as browser plug-ins or device settings, as valid consumer requests to opt out of the sale of personal information. This requirement is not feasible from a technology standpoint and limits consumer choice.

These global control technologies were designed for other contexts that are not compatible with the CCPA's complex and extremely broad definitions of "sale" and "personal information." As a result, this regulation will be very difficult to operationalize and will lead to inconsistent approaches. One reason is lack of uniformity in what constitutes a browser setting or plug-in and which mechanisms reflect genuine user intent. Also, not every browser communicates clearly which users are in California. Finally, there is insufficient interoperability among the technologies to be workable. W253-3

This requirement also runs contrary to consumer choice. Plug-ins and device settings do not clearly convey whether a consumer truly wants to opt out of the sale of personal information in every context. Moreover, treating global controls as opt-outs will also harm competition by favoring a few large advertisers who have direct relationships with consumers. This will lead to lower revenues and higher costs for smaller operators. Ultimately, the result will be less free and beneficial content online for consumers. Consumers will not be aware of these trade-offs when they click on a global device setting.

Alternatively, if the Attorney General continues to require treatment of these technologies as opt-outs, then the regulations should provide industry with additional time, until January 1, 2022, to implement this requirement so that industry can work to develop consistent and accurate technical signals that truly reflect consumer choice.

3. The record-keeping requirements are unduly burdensome and need to be simplified. (Section 999.317(g).)

While CJAC appreciates that the revised regulations narrowed the category of businesses that must comply with record keeping requirements, unfortunately, the revisions also created new reporting requirements making them even more onerous. The costs and burden associated with these record-keeping requirements far outweigh any possible benefit to consumers. These requirements need to be simplified rather than expanded. W253-4

4. **The requirement to quantify financial incentives and the value of consumer data should be eliminated as impractical and misleading. (Sections 999.307(b), 999.336, and 999.337.)**

Rather than require businesses to make calculations about financial incentives and data value, the Attorney General should simply require businesses to disclose whether they have a financial incentive or whether the data has value. Most consumers are savvy enough to know this is often the case in any event.

Requiring businesses to assign a number to incentives and data value provides little or no consumer benefit and could be misleading. Any metric or value assignment is subject to numerous variables that can change from day to day, such as a business's operational changes and market fluctuations. Additionally, financial incentive programs are often based on a complex calculation of costs to the business and market comparisons, and they are designed to reward loyal customers rather than to serve as a value exchange. Finally, a single customer's business or data holds little independent "value," since data gains value when it is aggregated. These factors render any attempt to quantify and disclose financial incentives or data values an unreliable and unproductive exercise. W253-5

The Attorney General should remove this quantification requirement from the regulations.

5. **The regulations need to further clarify and define information exempted from disclosure and deletion requests for security and other reasons. (Sections 999.302, 999. 313(c)(3), 999. 313(d)(3).)**

CJAC welcomes the Attorney General's added guidance recognizing that certain information should not be provided upon request, for consumer protection and other important reasons. However, this guidance needs further clarification and expansion to recognize other circumstances in which personal information should not be provided, including the following:

- The new guidance provided in section 999.302 for interpreting the term "personal information" is helpful but should be expanded to include pseudonymous or de-identified information. While such information could be linked to an individual, it is not in practice. A business often maintains such information in de-identified fashion as a privacy safeguard, using technical and administrative controls such as hashing, encryption, and contractual safeguards to prevent its linkage to an individual. The European Union's General Data Protection Regulation recognizes this as a good practice. Thus, we propose the following edit to section 999.302: W253-6

  > Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "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." For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, ~~and could not reasonably link the IP address with a particular consumer or household,~~ then the IP address would not be "personal information."

- Similarly, the clarifications in section 999.313(c)(3) are helpful in exempting from right to know requests personal information that a business maintains in backup or archive systems. However, the deleted portion that allowed a business to forgo disclosure if it "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" should be restored. This is a critical basis for not disclosing information and is in the public interest. W253-7

- Finally, the clarifications a.-d. added in the revisions to section 999.313(c)(3) are also applicable to, and should be added to, deletion requests in section 999.313(d)(3). W253-8

6. **The regulations should recognize WCAG version 2.0, in addition to version 2.1, as an acceptable standard for accessibility of online notices. (Sections 999.305(a)(2)d., 999.306(a)(2)d., 999.307(a)(2)d., and 999.308(a)(2)d.)**

The notice sections of the revised regulations newly require businesses to follow generally recognized industry standards for web accessibility. CJAC agrees with this requirement, but it is now unclear whether the Attorney General will enforce the provided example of industry standards – Website Content Accessibility Guidelines (WCAG), version 2.1, recently adopted on June 5, 2018.

CJAC agrees that 2.1 is a recognized industry standard, but so too is the earlier 2.0 standard. The United States Access Board recently adopted and applied 2.0 in the latest refresh of Section 508 of the Rehabilitation Act of 1973. While the 2.1 standard is the most recent issued by the World Wide Web Consortium, many businesses are already in the process of bringing their website accessibility up to the 2.0 standards. Web updates are a lengthy and costly undertaking for small businesses in particular. If they must now pivot their development to 2.1, this will require substantial new development which will be a heavy burden, especially when combined with the other weighty burdens of complying with CCPA. W253-9

Therefore, we request the Attorney General to revise these sections to specify WCAG version 2.0 and above as the example of an acceptable industry standard. Alternatively, the Attorney General should provide a delayed enforcement date of January 1, 2022 before holding any business to the 2.1 standard.

7. **The Attorney General should provide more flexibility for what is required in the notice at collection to allow for a better customer experience. (Section 999.305(a), (b).)**

The requirements of additional detail that must be included at the notice of collection in the revised regulations under section 999.305(a)(3)-(4) and (b) are burdensome and do not leave enough flexibility for businesses to provide a good customer experience. Most online users want their experience to be seamless, quick, and simple. The additional requirements will create a cumbersome and clunky customer experience. We ask the Attorney General to revisit these requirements and either scale them back or build in flexibility so that consumers get the notification they need without compromising their user experience. W253-10

8. The requirement that businesses reimburse consumers for costs associated with verification is unworkable. (Section 999.323.)

Section 999.323 prohibits a business from requiring the consumer to pay a fee for verification. While CJAC does not oppose a prohibition on businesses collecting a fee, we do object to businesses having to provide reimbursement for steps individuals may need to take to verify their identity.

W253-11

For example, this section provides obtaining a notarized affidavit as an example of verification that a business must reimburse. In some cases, such as when the individual does not have an account or sufficient information on-hand, securing a notarized document may be the only way to verify identity. As another example, if a consumer decides to verify by providing a copy of a government record, should a business be required to reimburse the cost of obtaining the record?

Requiring businesses to provide reimbursement for all the ways in which consumers may verify their identity overlooks the potential volume of these requests and will create tremendous operational challenges for businesses.

9. The Attorney General needs to mitigate the potential for unwarranted private rights of action.

CJAC is extremely disappointed the revisions do not respond to a major concern expressed by the business community – mitigation of unwarranted and unnecessary litigation under the CCPA's private right of action provisions. The Attorney General, though regulations, is well-positioned to promote adoption of security practices that protect consumers by providing clarity on security standards that satisfy CCPA and incentivizing businesses to meet these security standards.

There are several ways the Attorney General can accomplish this, including:

- First, the Attorney General should define security standards, such as industry-established standards, that, if met or exceeded by businesses, would serve as a safe harbor from private rights of action under the CCPA. This is critical considering the potential for liquidated damages under the CCPA between $100 and $750 "per incident," without a clear requirement of showing of harm. If the policy goal of the CCPA is to discourage consumer data breaches, and the way to prevent data breaches is reasonable security measures, then the regulations should recognize and incentivize this desired behavior. If businesses are subject to private rights of actions and penalties regardless of security steps they take, then the lawsuits and penalties are meaningless hammers and ripe for abuse.

W253-12

- On a related note, the Attorney General should define what constitutes a "cure" as it is not defined in the CCPA. CJAC proposes that implementation of reasonable security measures should be recognized in the regulations as a cure. If not that, what else qualifies as a cure?

W253-13

CJAC urges the Attorney General to mitigate potential abuses of the private right of action and to promote ubiquitous adoption of best security practices through these additional revisions to the regulations.

Conclusion

CCPA regulations that are unworkable or unduly burdensome will give rise to unnecessary and unproductive enforcement actions and litigation. The goal of the regulations should be to facilitate implementation of and compliance with the CCPA. This is a win-win for consumers and businesses – not to mention a reduced enforcement burden for your Office.

We are happy to answer any questions you may have and look forward to the opportunity to work with your Office on improvements to the regulations.

Thank you for your consideration,

Kyla Christoffersen Powell
President and Chief Executive Officer

From:	Howard Fienberg
To:	Privacy Regulations
Cc:	Stuart L. Pardau; Blake Edwards
Subject:	Comments on 2nd draft of CCPA regulations
Date:	Tuesday, February 25, 2020 2:46:21 PM
Attachments:	Insights Association CCPA comments to AG 2-25-20.pdf

Attached are the comments of the Insights Association in response to the second draft of CCPA regulations. They're also available online at https://www.insightsassociation.org/sites/default/files/misc_files/insights_association_ccpa_comments_to_ag_2-25-20.pdf

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
1300 I Street
Sacramento, CA 95814

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

Email: privacyregulations@doj.ca.gov

February 25, 2020

Dear Attorney General Becerra

The Insights Association ("IA") submits the following comments regarding the proposed regulations implementing the California Consumer Privacy Act ("CCPA") (CAL. CIV. CODE, § 1798.100 et seq.), particularly the most recent edits to the regulations circulated by your office on February 10, 2020.[1]

IA represents more than 545 individual and company members in California, with more than 5,500 members in total (and many of those non-California-based businesses driving revenue for the state through investment, travel and research and analytics studies in California). 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 include both marketing research and data analytics companies and organizations, as well as the research and analytics professionals and departments inside of non-research companies and organizations. They 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,

[1] https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-redline-020720.pdf

INSIGHTS ASSOCIATION
1156 15TH ST, NW, SUITE 700, WASHINGTON, DC 20005 • PH: [redacted]
WEBSITE: www.InsightsAssociation.org • EMAIL: [redacted].

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."

As IA indicated in comments submitted on December 6, 2019 regarding the first draft of CCPA regulation,[2] the CCPA will have a profound impact on the business community, including the marketing research and data analytics industry. In this regard, we appreciate the opportunity to submit additional recommendations on the latest draft CCPA regulations.

1. Promulgate additional clarification on telephone notices, including a short-form option.

The most recent edits to the regulations clarify in § 999.305(a)(3)(d) that, "[w]hen a business collects personal information over the telephone or in person, it may provide the [collection] notice orally."

As we argued in previous comments, in many cases the notices required to be read over the phone would include not only collection notices, but also opt-out notices and, potentially, financial incentive notices as well. This extended "preamble" to a phone call would be significantly detrimental to phone researchers. Response rates for U.S. telephone surveys rarely exceeds ten (10) percent. The addition of an extended notice to the front-end of all calls will likely result in significant drop-off rates from these already low rates. It would likely prove impossible to find respondents willing to sit through such a preamble before finally being given an opportunity to provide their opinion for a public opinion or political poll or in response to a government-sponsored survey. W254-1

As such, we urgently request that the finalized regulations allow for a short-form collection and opt-out notice for telephone interactions. For example, a short-form notice might, in simple straightforward terms: (i) alert the consumer that personal information will be collected; (ii) alert consumers of their right to opt out; and (iii) direct users to a privacy policy (likely online) where more information can be found or provide them the opportunity to give their email address and receive it via email.

We believe such a short-form notice would, by shortening the amount of "legalese" confronting consumers, better further the goals of the CCPA without unnecessarily inhibiting legitimate research.

2. Expand the email-only option for all requests, and apply to all relationships with consumers that are "exclusively online."

The recent edits also stipulate in § 999.312(a) that "[a] business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to know."

While IA lauds this edit, we suggest the following two additional changes which would better streamline the request process for both consumers and businesses: W254-2

First, this email-only option should be expanded to all requests, not just requests to know.

Second, the email-only option should be expanded to all *relationships* between consumers and businesses that are exclusively online, even if the business itself operates separately in a non-online context.

[2] https://www.insightsassociation.org/sites/default/files/misc_files/insights_assoc_ccpa_reg_comments_12-6-19.pdf

INSIGHTS ASSOCIATION
1156 15TH ST, NW, SUITE 700, WASHINGTON, DC 20005 • PH: [redacted]
WEBSITE: www.InsightsAssociation.org • EMAIL: [redacted].

The reason for this second request is simple. In the marketing research and data analytics industry, as many other industries, firms often have relationships with individual consumers that are exclusively online, but relationships with other consumers that are not. For example, a marketing research firm may operate an online survey panel, but also conduct phone research. As the regulations are currently drafted, a firm that engaged both these modalities would not be able to avail itself of the email-only option with respect to its online survey panel, even though email is a perfectly viable, and indeed the most appropriate, option for communicating with those panel members, who are already accustomed to online interaction with the firm.

W254-2 (cont.)

3. Broaden financial incentive disclosure guidance to contemplate situations where additional, non-monetary consideration is given in exchange for personal information.

Following the latest edits to the draft regulations, the financial incentive notice remains problematic for the marketing research and data analytics industry. In particular, the "value" calculation imposes an unrealistic and poorly-suited requirement in situations where financial incentives are not being given in a simple *quid pro quo* for personal information, as in a traditional loyalty program.

In our industry, financial incentives, such as a gift card or reward points (which are usually small in value), are frequently offered to encourage participation in a survey or other research study. These incentives are *not* designed to be simple compensation for a participant's services or his or her personal information. Instead, these small incentives are designed to sweeten the value proposition for a potential participant just slightly in an effort to bolster participation rates. Participants generally enjoy participating in research studies and giving their opinions. Indeed, participants often elect to respond without additional financial incentive at all.

W254-3

In other words, there is a more complicated mix of motivations or "consideration" at play when a person chooses to participate in research. The finalized CCPA regulations should reflect this reality. While the Insights Association understands the need for some kind of notice, such notice should be flexible enough to accommodate more complex situations. For example, the following text could be added at the end of your most recent addition at § 999.337(b) of the draft regulations: "*In its notice of financial incentive, a business may also identify any additional consideration the consumer is receiving aside from the incentive, and request the consumer's acknowledgement that the incentive and additional consideration together constitute fair value for the personal information."*

Insights produced by our industry, often utilizing participant incentives in the development process, drive decisions across all sectors of the economy, including government.

4. Clarify mobile notice requirements, particularly the meanings of "reasonably expect" and "just-in-time."

The updated draft regulations specify in § 999.305(a)(4) that "[w]hen a business collects personal information from a consumer's mobile device for a purpose that the consumer would not *reasonably expect*, it shall provide a *just-in-time notice* containing a summary of the categories of personal information being collected and a link to the full notice at collection."

W254-4

The Insights Association respectfully requests that your office further clarify the meaning of "reasonably expect" in the above edit. The example added in the latest edits, related to the flashlight application, is helpful, but still incomplete and therefore unsatisfactory. For example, must the notification appear each time the app is used? Solely the first instance of collection?

INSIGHTS ASSOCIATION
1156 15TH ST, NW, SUITE 700, WASHINGTON, DC 20005 • PH: [redacted]
WEBSITE: www.InsightsAssociation.org • [redacted].

Likewise, IA requests further clarification on the meaning of "just-in-time." Is a pop-up notification the only way to comply with this requirement? Does the notification need to be presented every time an application is opened, or only the first time a consumer uses the application? We believe these and similar questions remain open, after the edits.

W254-4 (cont.)

5. Loosen restriction on passing through costs of verification to accommodate special circumstances.

The draft regulations also now prohibit businesses in § 999.233(d) from "requir[ing] the consumer to pay a fee for the verification of their request to know or request to delete." The regulations go on to explain that a business may not, for example, "require a consumer to provide a notarized affidavit to verify their identity unless the business compensates the consumer for the cost of notarization."

While this requirement is perhaps necessary as a general rule, it may also be problematic for businesses in certain special cases where the only way to verify a person's identity or an authorized agent's authority is through a notarized document. In cases of death, for example, this provision may unnecessarily increase costs for businesses when dealing with executors, relatives or loved ones who are making requests under CCPA on behalf of the deceased, where such dealings regularly require the provision of a notarized death certificate and executor short form.

W254-5

This provision is also potentially ripe for abuse. When a consumer submits an erasure request on behalf of a friend or relative, for example, how would the consumer prove they are who they claim to be and that they are in fact acting on behalf of another consumer? All of this would require official documents of some form, such as a birth certificate (or a death certificate, as in the prior example), and would require authentication via an apostile or notary, the services of which will not be provided for free. Since the regulations prevent passing such costs on to the party seeking verification, this could quickly become an undue burden on businesses.

6. Provide Time for Businesses to Comply Before Enforcement.

Given the absence of lag time between the release of final CCPA regulations and the onset of CCPA enforcement this summer, the Insights Association urges that CCPA enforcement be delayed until January 1, 2021. This would give businesses the minimum amount of time to comply with these complex new privacy requirements – many of which were not in the original statute or were changed in various ways by the regulation – and ensure that consumers are duly protected and accommodated.

W254-6

Conclusion

The Insights Association hopes the above comments will be useful to you and your staff. We look forward to answering any questions you may have about the marketing research and data analytics industry and working with you and your office in furtherance of consumer privacy in California and streamlining CCPA compliance for both businesses and consumers.

Sincerely,

Howard Fienberg
Vice President, Advocacy
Insights Association

Stuart L. Pardau
Outside General Counsel
The Insights Association and Ponemon Institute Fellow

INSIGHTS ASSOCIATION
1156 15TH ST, NW, SUITE 700, WASHINGTON, DC 20005 • PH: [redacted]
WEBSITE: www.InsightsAssociation.org • EMAIL: [redacted].

From: Emery, Emily
To: Privacy Regulations
Cc: Emery, Emily
Subject: MPA Comments on the Modifications to the Proposed Text on CCPA
Date: Tuesday, February 25, 2020 2:22:39 PM
Attachments: MPA Comments on Modifications to the Proposed Text on CCPA 02.25.2020.pdf

---

Attached, please find comments on the modified proposed text of regulations implementing CCPA submitted on behalf of MPA - The Association of Magazine Media.

We appreciate the opportunity to provide the attached commentary for your consideration.

Please contact us if we can be of assistance.

Emily Emery
Director of Digital Policy
MPA - The Association of Magazine Media
Cell: [redacted]
Office: [redacted]

MPA THE ASSOCIATION OF MAGAZINE MEDIA

February 25, 2019

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

Submitted via email to PrivacyRegulations@doj.ca.gov

RE: Comments from MPA – the Association of Magazine Media on Modifications to the Proposed Text of Regulations Implementing the California Consumer Privacy Act (CCPA) OAL File No. 2019-1001-05

Dear Attorney General Becerra:

MPA – the Association of Magazine Media (MPA) appreciates the opportunity to submit comments on the modifications to the proposed text of the regulations implementing the California Consumer Privacy Act ("CCPA").[1] MPA submits these comments on behalf of its members, who represent more than 500 magazine media brands that span a vast range of genres across print, digital, mobile, and video media.

Magazine media brands depend on consumer data to deliver to readers the enriching, educational, and entertaining content they value and expect. The responsible use of data enables magazine media brands to personalize content, understand user preferences and interests, reach new readers, and create new offerings so that the magazine media industry remains accessible to consumers.

Reader trust is critical to the magazine media industry. Consistent with maintaining reader trust, MPA and its members believe that consumers should have meaningful privacy protections, control over the use of personal information, and transparency into businesses' data practices. The success of consumer data privacy protections relies on the ability of businesses to correctly interpret reasonable regulations and implement them into their processes for managing consumer data. MPA, therefore, appreciates the effort undertaken by OAG to clarify several regulatory requirements in its recent modifications to the proposed rules implementing the CCPA.

[1] MPA also filed comments in response to the October 11, 2019 request for comment from the California Office of the Attorney General ("OAG") on the initial draft of the proposed rules implementing the CCPA. *See* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-comments-45day-pt6.pdf at CCPA_45DAY_01381 - 01387.

However, ongoing uncertainty about certain CCPA rulemaking provisions would pose considerable implementation challenges for businesses, including magazine publishers. The lack of further clarification from the OAG on the modified proposed rules could inadvertently pose a risk to consumer privacy and data security, diminish consumer well-being, and possibly threaten the viability of magazine media brands and their offerings to readers.

Further, such ongoing uncertainty could have a significant impact on the consumers of magazine media by potentially limiting their ability to make choices in the marketplace, and by potentially diminishing their access to the trusted, valuable content they enjoy and expect to receive.

Accordingly, MPA raises the following concerns about select provisions of the modified proposed rules: MPA urges the OAG to issue further guidance on global browser settings and user-enabled privacy controls, third party opt-out notification requirements, and outstanding privacy and security concerns regarding authorized agents. MPA then asks the OAG to allow a reasonable amount of time for magazine publishers to adjust their practices in accordance with the proposed rules' new requirements before bringing an enforcement action under the CCPA.

I. The OAG should clarify that browser settings and user-enabled global privacy controls outlined in 999.315 do not supersede the preferences consumers express to individual businesses.

In comments submitted in December, MPA urged the OAG to issue further clarifications on the draft rules' requirement that businesses must honor browser-level opt-out signals.[2] MPA appreciates the clarifications issued in the modified proposed rules that user-enabled privacy controls "shall require that the consumer affirmatively select their choice to opt-out and shall not be designed with any pre-selected settings."[3]

However, the requirement to honor user-enabled global privacy controls, such as browser plugins or privacy settings, still stands in the way of consumers' ability to make individualized choices about which magazine publishers or businesses can and cannot sell personal information. MPA therefore respectfully asks the OAG to remove the requirement, which is outside of the scope of the CCPA and not in line with legislative intent. In the alternative, the OAG should clarify that a business *may* honor user-enabled privacy controls *or* provide another mechanism for consumers to submit a request to opt-out of the sale of personal information, such as a "Do Not Sell My Personal Information" link. W255-1

Browser settings broadcast a single opt-out signal to the entire internet marketplace, thereby inadvertently turning the CCPA's opt-out system into a *de facto* opt-in system, because individual businesses and magazine publishers would be required to ask consumers to opt-in to the sale of personal information after receiving a global privacy setting. This result is clearly outside of the scope of what the California legislature intended in providing an opt-out right in

[2] Cal. Code Regs. tit. 11, § 999.315(d) (proposed Feb. 10, 2020).
[3] *Id*. at § 999.315(d)(1).

the CCPA.[4] MPA would further note that the user-enabled privacy control browser directive is not supported by the CCPA statute itself.

In theory, the ability of a business to notify the consumer of a conflict with a global privacy setting appears to be helpful.[5] In technical practice, however, even if consumers wish to undo a default browser setting, at best they may find a frustrating repeated user interface experience, and at worst, they may find the process technically impossible to execute. Because businesses must "respect the global privacy setting" regardless of the consumer's actual expressed preference, businesses will be forced to act on global privacy settings before they can confirm the consumer's choice. The *de facto* result would deprive consumers of their access to valuable content magazine publishers provide, thereby diminishing the reader experience.

W255-1 (cont.)

MPA recommends striking the section requiring businesses to respect user-enabled global privacy controls, or at a minimum, give businesses the option to honor such settings or offer another, equally effective method for the consumer to opt-out of the sale of personal information.

II. The OAG should consider a reasonable grace period for requiring the notice of a consumer opt-out request to third parties as soon as feasibly possible.

MPA appreciates the clarification in modified draft rules in Section 999.315.(f) that remove the requirement to notify all third parties of an opt-out within 90 days prior to the customer's submission.[6]

However, the new, additional, requirement that businesses notify third parties that the consumer has exercised their right to opt-out and the requirement to direct the third parties not to sell that consumer's information imposes a significant operational, logistical and technical challenge for businesses. In practice, the new language of the modified rules would require businesses to create an entirely new tracking and notification process solely to administer a timed notice that could otherwise be administered in a timely but not near-instantaneous fashion, and could otherwise be determined by the third parties through global browser settings.

W255-2

The extensive technical infrastructure required to create an operable system to accomplish this requirement further supports why a reasonable amount of additional implementation time is needed by magazine publishers and other businesses to understand and effectively and consistently operationalize the modified rules.

MPA recommends striking the notification portion of 999.315(f) while retaining the requirement to comply with the request within 15 business days: "A business shall comply with a request to opt-out as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. ~~If a business sells a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request, it shall notify those third parties that the consumer has exercised their right to opt-out and shall direct those third parties not to sell that consumer's information.~~"

[4] Cal. Civ Code § 1798.120.
[5] Cal. Code Regs. tit. 11, § 999.315(d)(2) (proposed Feb. 10, 2020).
[6] Cal. Code Regs. tit. 11, § 999.315(f) (proposed Feb. 10, 2020).

III. The OAG should expand exceptions to allow businesses to reasonably deny requests from authorized agents that do not employ reasonable security measures.

Given the unique and long-standing first-party relationship between a magazine brand and its reader, MPA takes particular notice of the role of authorized agents in the CCPA. The introduction of an unknown party into consumer rights requests creates implementation obstacles for magazine publishers. Therefore, MPA appreciates the further clarification offered by the OAG on verification steps businesses may take to ensure agents have been appropriately authorized to submit requests on behalf of consumers.

However, MPA is concerned that without further clarity from the OAG, requests from authorized agents could introduce significant data privacy and security risk to unwitting consumers. W255-3

MPA urges the OAG to add language to the rules that explicitly permits a business to deny a request from an authorized agent if the business suspects the requestor fails to "implement and maintain reasonable security procedures and practices." As an example, if a requestor lacks a secure method for receiving the personal information, or has had prior known cases of data breaches, a business should be permitted to deny the request. Additionally, the OAG should further require that an authorized agent certify that it maintains reasonable data security practices before being permitted to make rights requests on behalf of consumers.

In a similar vein, the OAG should restore the deleted exception language in Section 999.313(c)(3) against disclosing specific pieces of personal information where there is a substantial, articulable and unreasonable risk to the security of the personal information. W255-4

Finally, the OAG should allow businesses discretion in Section 999.315(h) by including language to permit the business to notify the consumer directly, and not the requestor, in instances where there exists a good-faith belief that the request to opt-out is fraudulent. Such a change would help ensure that consumers themselves receive notice of fraudulent requests so they can take steps to protect information associated with them from nefarious parties who may be attempting to access it. W255-5

IV. The OAG should provide a reasonable amount of time for businesses to update their practices for the revised regulations prior to enforcing the law.

The CCPA became operative on January 1, 2020, but regulated entities still do not have access to finalized regulations to implement the law. As a result, businesses, including magazine publishers, are attempting to structure processes, policies, and systems to further compliance efforts with regulations that continue to reflect significant changes and increase in complexity. W255-6

The CCPA's complexity and the possibility that the implementing rules could materially change again in further revisions before the law's enforcement date of July 1, 2020 suggest that there will not be enough time for businesses to effectively operationalize the final rules prior to enforcement, despite making significant investments toward good-faith efforts to uphold consumer data protections and to comply with the law. As a result, MPA respectfully asks the

OAG to postpone enforcement of the CCPA until January 1, 2021 so businesses like magazine publishers can have time to implement the final regulatory requirements in ways that will ensure consumers' rights requests are appropriately honored.

MPA members strongly support the underlying goals of the CCPA. However, the amount of time is limited for well-intentioned businesses, including magazine publishers, to structure processes to further compliance before the enforcement date. It is presently not clear if the rules will be finalized before July 1, 2020 or whether they will be further amended and thus require another comment period before the review and approval by California's Office of Administrative Law ("OAL"). The time frame for each of these steps are uncertain, but each would significantly reduce the time businesses will have to implement the finalized regulations. W255-6 (cont.)

The rapidly approaching enforcement data coupled with the in-flux legal regime may result in confusing and changing compliance solutions that lead to significant consumer frustration. In the absence of time to develop industry-wide best practices and consistent internal tooling offerings, different magazine publishers' strategies for implementing the CCPA may look and feel different to consumers who will submit rights requests under the law.

The CCPA states that the OAG may not bring any enforcement action prior to July 1, 2020.[7] However, the OAG could exercise discretion and allow a reasonable amount of additional time for businesses, including magazine publishers, to review and operationalize the final rules before enforcement begins. Providing a reasonable amount of additional implementation time will give businesses like magazine publishers much-needed time they need to understand and effectively operationalize the rules helping consumers to more seamlessly exercise the rights afforded under the new law.

To avoid unfavorable outcomes for consumers and businesses, MPA asks that the OAG postpone enforcement of the law until January 1, 2021.

* * *

MPA commends the OAG's thoughtful approach to promulgating rules to implement the CCPA and soliciting diverse viewpoints on outstanding CCPA implementation concerns. In each of the sections identified above, MPA believes that greater clarity is needed to ensure that businesses like magazine publishers can identify privacy-protective ways to comply with the law, uphold reader trust, and preserve the viability of the magazine media brands that consumers enjoy.

The new requirements set forth by the OAG's proposed rulemaking are significant, and the time frame for implantation is minimal. Therefore, further guidance from the OAG is imperative to ensure consistent application of the CCPA across businesses and enhance the data-driven content and offerings that consumers value and expect to experience online.

MPA and our members appreciate the opportunity to provide our views for your consideration, and we look forward to working with you and your staff to address the concerns outlined above.

[7] Cal. Civ. Code § 1798.185(c).

Sincerely,

Brigitte Schmidt Gwyn
President & CEO
MPA – The Association of Magazine Media

Emily Emery
Director, Digital Policy
MPA – The Association of Magazine Media

From: Jennifer Peters
To: Privacy Regulations
Cc: Elizabeth Hegarty; Ariel Fox Johnson
Subject: Comments regarding the CCPA Revised Proposed Regulations
Date: Tuesday, February 25, 2020 2:13:48 PM
Attachments: 2020.02.25 -- CCPA comments.pdf

Good Afternoon,

Please see the attached comments regarding the CCPA Revised Proposed Regulations.

Thank you for the opportunity to submit these remarks. If you have any questions or concerns, please feel free to contact us directly.

Best,
--

Jen Peters
Advocacy Manager | **Common Sense** Kids Action | She/Her
e: [redacted]
p: [redacted]

Comments to the

Office of the Attorney General of California

Notice of Modifications to Proposed Rulemaking

The California Consumer Privacy Act

Submitted via Email to PrivacyRegulations@doj.ca.gov

February 25, 2020

On Behalf of the Following Organizations:

ACLU California

Electronic Frontier Foundation

common sense

Privacy Rights Clearinghouse

Media Alliance

CFA

ccfc Campaign for a Commercial-Free Childhood

Oakland Privacy

Table of Contents

Introduction

The undersigned privacy and civil-liberties organizations thank the Office of the Attorney General for its continued work on consumer privacy. We are disappointed that the Modified Regulations (Mod. Reg.) are largely a step backwards for protecting consumers' privacy, particularly in terms of consumers' attempting to stop the sale of their information. Most problematically, the proposed Modified Regulations limit the protections offered by the law by improperly reducing the information covered by CCPA and making it harder for consumers to exercise a key affirmative right—opting out of the sale of personal information. The proposed opt-out icon is rather confusing. And the proposed Modified Regulations also make a number of changes to the original draft that are business-friendly at consumers' expense. W256-1

The proposed Modified Regulations make it more difficult for consumers to effectively opt-out of sale of their personal information, by failing to recognize widely known signals as a request to opt-out and by placing even more burdens on consumers W256-2

The proposed Modified Regulations improperly limit the law's protective reach, by narrowing the definition of personal information and trying to carve out certain identifiers (including IP addresses) from that definition under certain circumstances. W256-3

The proposed icon for "Do Not Sell" may inadvertently lead to consumer confusion. The choice of color and the implication of a toggle function may lead to consumers believing their information is not being sold when in fact it is. We understand any confusion to be the opposite of the Attorney General's goals. W256-1 (cont.)

The proposed change to not require businesses to treat an unverified deletion request as an opt-out request creates an additional hurdle to jump through for consumers who are at bottom seeking to have their information out of a company and an online ecosystem. W256-4

Proposed reporting requirements are applicable to an even smaller subset of companies, instead of acknowledging that small companies who build a model on data collection and sharing can cause real privacy harms to individuals as well. W256-5

The enumeration of new rights of service providers to use personal information for their own purposes, including any contractual purposes they may have chosen to insert, blurs the line between business and service provider. Given that service provider sharing falls outside the CCPA definition of "sale" and consumers have no say over such transfers, any receiving service provider's use of such information must be limited. W256-6

Signing Organizations

The American Civil Liberties Union is a national, non-profit, non-partisan civil liberties organization with more than 1.6 million members dedicated to the principles of liberty and equality embodied in both the United States and California constitutions. The ACLU of California is composed of three state affiliates, the ACLU of Northern California, Southern California, and San Diego and Imperial Counties. The ACLU California operates a statewide Technology and Civil Liberties Project, founded in 2004, which works specifically on legal and policy issues at the intersection of new technology and privacy, free speech, and other civil liberties and civil rights.

Common Sense Media, and its policy arm Common Sense Kids Action, is dedicated to helping kids and families thrive in a rapidly changing digital world. Since launching in 2003, Common Sense has helped millions of families and kids think critically and make smart choices about the media they create and consume, offering age-appropriate family media ratings and reviews that reach over 110 million users across the country, a digital citizenship curriculum for schools, and research reports that fuel discussions of how media and tech impact kids today. Common Sense also educates legislators across the country about children's unique vulnerabilities online.

The Electronic Frontier Foundation works to ensure that technology supports freedom, justice, and innovation for all the people of the world. Founded in 1990, EFF is a non-profit organization supported by more than 30,000 members.

Privacy Rights Clearinghouse is dedicated to improving privacy for all by empowering individuals and advocating for positive change. Founded in 1992, Privacy Rights Clearinghouse has focused exclusively on consumer privacy issues and rights. Privacy Rights Clearinghouse strives to provide clarity on complex topics by publishing extensive educational materials and directly answering people's questions. It also amplifies the public's voice in work championing strong privacy protections.

Oakland Privacy is a citizen's coalition that works regionally to defend the right to privacy, enhance public transparency, and increase oversight of law enforcement, particularly regarding the use of surveillance techniques and equipment. As experts on municipal privacy reform, Oakland Privacy has written use policies and impact reports for a variety of surveillance technologies, conducted research and investigations, and developed frameworks for the implementation of equipment with respect for civil rights, privacy protections and community control.

Campaign for a Commercial-Free Childhood is a nonprofit organization committed to helping children thrive in an increasingly commercialized, screen-obsessed culture, and the only organization dedicated to ending marketing to children. Its advocacy is

grounded in the overwhelming evidence that child-targeted marketing – and the excessive screen time it encourages – undermines kids' healthy development.

The Consumer Federation of America (CFA) is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education.

Media Alliance is a Bay Area democratic communications advocate. Media Alliance members include professional and citizen journalists and community-based communications professionals who work with the media. Its work is focused on an accessible, affordable and reliable flow of information to enable civic engagement, meaningful debate and a safe and aware populace. Many of Media Alliance's members work on hot-button issues and with sensitive materials, and those members' online privacy is a matter of great professional and personal concern.

Section 315(c). Do Not Track & Do Not Sell.

The modified regulations would hinder the exercise of consumer rights.

The modified draft regulations would make it harder for consumers to use browser headers to opt-out from the sale of their personal information. The coalition objects to this step backwards from the original draft regulations.

The original draft regulations required businesses that collect consumer data online to treat the following as an opt-out: "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." *See* Original Draft Regulations § 315(c). The coalition supported this rule, because it would make it easier for consumers to exercise their right to opt-out.

W256-2 (cont.)

Unfortunately, the modified draft regulations would add the following: "Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information. The privacy control shall require that the consumer affirmatively select their choice to opt-out and shall not be designed with any pre-selected settings." *See* Mod. Reg. Sec. 315(d)(1).

As the coalition explained in our initial comments, thousands of Californians have already installed tools that send "do not track" browsing headers to the sites they visit. Many major web browsers already include settings by which users can easily choose to send "do not track" headers with all of their web traffic. A business that cannot collect a person's information cannot sell that information. The greater (do not collect) includes the lesser (do not sell). So businesses should treat "do not track" headers as requests to opt-out of sale.

Yet "do not track" headers might not fit into the new draft rule. First, some of these systems come with the pre-selected privacy settings that the consumer does not manually select. A consumer's choice to use tools that are privacy protective by default should not mean they have fewer protections, and any pro-consumer privacy regulation should not incentivize companies to not protect privacy by default—that is an absurd consequence. Second, businesses may argue that "do not track" headers do not "clearly communicate or signal that a consumer intends to opt-out of the sale of personal information." As detailed in previous comments, a desire to not have one's information tracked encompasses a desire not to have one's information sold.

Please withdraw this new Mod. Reg. Sec. 315(d)(1). And per our earlier set of comments, please add this clause to the end of Mod. Reg. Sec. 315(c):

A business shall treat a "do not track" browsing header as such a choice.

Section 302(a). Interpretation of "Personal Information."

The modified regulations are inconsistent with both the language and the fundamental purpose of the CCPA.

Section 999.302 of the draft regulations states that information including but not limited to IP addresses is not personal information if "the business does not link the [information] to any particular consumer or household, and could not reasonably link the [information] with a particular consumer or household." As drafted, Mod. Reg. Sec. 302 is inconsistent with the statute's language and in irreconcilable conflict with one fundamental purpose of the CCPA: to give consumers control over how they are tracked online. This problem is amplified by its explicit application to IP addresses.

First, the proposed regulation is contrary to the CCPA's core definition of "personal information." Under the CCPA, information qualifies as "personal information" if it "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." That definition does not refer to the possessor's specific actions or capabilities because whether information is PI or not is a property of *the information itself*, and does not depend on its possessor. This is directly contrary to the proposed regulation, under which certain information may be PI if possessed by one business but not by another business.

W256-3 (cont.)

This interpretation is shared by other provisions of the CCPA which are explicitly designed to address related sets of personal information which would be undermined by the proposed regulation. In particular, the proposed regulation would supplant the CCPA definition of "deidentified" information, an exception to personal information that applies exclusively to information that "cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer," with a far broader exception to personal information, excluded from the procedural safeguards applicable to deidentified information, that apples any time the *current possessor* lacks the capability to link or associate the information.

As a result, under the proposed regulation, a business would be free to sell information that its recipient could easily reidentify as long as the business itself was unable to do so. This would broadly undermine the purpose of the CCPA and the practical exercise of the rights it grants to consumers..

Instead, privacy laws must—and the CCPA does—take into account the modern reality that information is not "anonymous" and thus not personal merely because its current possessor lacks the capacity to associate it with a specific person.[1] For example,

[1] Nate Anderson, *Anonymized" data really isn't—and here's why not*, Ars Technica, September 8, 2009 (available at https://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/); *see also* Ohm, Paul, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*,

"anonymized" search queries released by AOL were nonetheless associated with particular individuals,[2] and Twitter users were unmasked by leveraging the structure of social relationships.[3] Machine learning techniques can significantly reduce the difficulty of re-identifying personal information over time.[4] Signaling the maturity of these re-identification techniques, data brokers are even offering what is effectively re-identification as a service, promising the ability to "reach customers, not cookies."[5] By excluding information from the CCPA solely because the current possessor lacks the capacity to connect it to a specific consumer, the draft regulations threaten to eliminate protections for information that has immense potential to violate people's privacy.

In addition, the regulation is particularly problematic in its application to IP addresses, which deserve and enjoy particular protection under the CCPA. W256-3 (cont.)

Under the CCPA, IP addresses belong to the same category of "identifiers" as a real name, an email or postal address, an account name, or a social security number.[6] The fact that multiple consumers may have the same or similar names, share email addresses or online accounts, or live at the same postal address with others does not change the fact that labelling information with a name, email address or postal address serves to "identify" the data subject, thus rendering it personal information under the CCPA. The same is true of IP addresses, which in and of themselves identify a particular consumer or device, even if they do not do so with perfect accuracy.[7]

Moreover, protecting information like IP addresses that can be used to track consumers' online activity is the goal of modern privacy laws including the CCPA. A 2019 poll of

---

August 13, 2009. UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12 (available at SSRN: https://ssrn.com/abstract=1450006).

[2] Eric Bangeman, *AOL subscribers sue over data leak*, Ars Technica, September 26, 2006 (available at https://arstechnica.com/information-technology/2006/09/7835/).

[3] Nate Anderson, *Pulling back the curtain on "anonymous" Twitterers*, Ars Technica, March 31, 2009 (available at https://arstechnica.com/tech-policy/2009/03/pulling-back-the-curtain-on-anonymous-twitterers/).

[4] Gina Kolata, *Your Data Were 'Anonymized'? These Scientists Can Still Identify You*, The New York Times, July 23, 2019 (available at https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html).

[5] *Reach Customers, Not Just Cookies*, LiveRamp Blog, September 10, 2015 (available at https://liveramp.com/blog/reach-customers-not-just-cookies/) ("Cookies are like an anonymous ID that cannot identify you as a person.").

[6] Civ. Code § 1798.140(o)(1)(A) specifies that personal information includes "identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers."

[7] For the same reason, IP addresses also explicitly appear in the definition of "unique identifier," which is "a persistent identifier that can be used to recognize a consumer, a family, or a device … including, but not limited to… an Internet Protocol address." Civ. Code 1798.140(x).

likely California voters showed that Californians overwhelmingly support a definition of personal information that encompasses all information about them, their households and their electronic devices.[8] Over 90% of voters, spanning across age, gender, party, and region of California, said it was important to be able to control their personal information in each of the following areas:

- Information collected about your computer, phone or other device that could be identified by an IP address.
- Information related to or collected about a household, including from a device in the home such as Alexa, a baby monitor, or a "smart" TV or refrigerator, that could be compiled with the use of a household IP address.
- Location information, including the history of where you've been, that could be connected to or even derived from an IP address.

W256-3 (cont.)

The legislature's intention that an IP address qualify as personal information is further reflected in its rejection of AB 873 (2019). According to both its author[9] and proponents[10], AB 873 was intended to expand the definition of "deidentified" information with the explicit purpose of exempting IP addresses from the CCPA in the same manner as the draft regulation.[11] The legislature properly rejected that proposal. The Attorney General should not undo that decision by incorporating it into regulations that undermine the purpose of the CCPA.

We support the Attorney General's desire to add clarity to the CCPA. But the proposed regulation would undermine rather than clarify the definition of personal information. Information that can be connected to a specific consumer should be within the scope of

---

[8] *Will California lawmakers vote to protect Californians' privacy or tech industry profits?* ACLU of Northern California, March 27, 2019 (available at https://www.aclunc.org/blog/will-california-lawmakers-vote-protect-californians-privacy-or-tech-industry-profits).

[9] Asm. Irwin, the author of AB 873, asserted that "if a store keeps IP address for web analytics, but it doesn't link that data back with a person," the IP address would still be subject to the CCPA, and that changing that was a key goal of AB 873. *See* Assembly Committee on Privacy and Consumer Protection, California Consumer Privacy Act of 2018, Mar. 25, 2019, http://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201920200AB873.

[10] Jim Halpert, who testified on behalf of the sponsors of the bill, wrote that AB 873 "would very likely have the effect of exempting IP addresses and device IDs that are maintained separately from personal data and cannot be queried or accessed by employees or third parties who could link the data." Jim Halpert, California Lawmakers Smooth Over Some of the CCPA's Rough Edges, IAPP Privacy Tracker, https://iapp.org/news/a/california-lawmakers-smooth-over-some-of-the-ccpas-rough-edges/.

[11] AB 873, much like the proposed regulation, would have excepted information from personal information (by way of categorizing it as deidentified) if the information "does not identify and is not reasonably linkable, directly or indirectly, to a particular consumer." "Reasonably linkable" appears verbatim in the proposed regulation as a necessary rather than sufficient attribute of personal information.

the CCPA even if its possessor currently lacks that capacity. And IP addresses in particular are online identifiers, both in practice and in the language of the CCPA, that inherently identify and are capable of being associated with or linked to a specific consumer, satisfying the definition of "personal information." Any contrary guidance or regulation is inconsistent with the goals and express language of the CCPA.

W256-3 (cont.)

We therefore respectfully request that Mod. Reg. Sec. 999.302 be deleted in its entirety.

Section 306(f). "Do Not Sell My Personal Information" Button.

The recommended toggle icon would lead to consumer confusion.

Mod. Regs. Sec. 999.306(f) recommends a CCPA opt-out button and accompanying tagline that will lead to consumer confusion. The recommended icon does not clearly convey the presence of a choice and may discourage consumers from exercising their opt-out right. The coalition urges the Attorney General to modify its recommended icon to reduce the possibility of confusion.

The Attorney General should follow the recommendations outlined by Lorrie Cranor and her team of researchers and designers that developed and tested combinations of icons and taglines to signal opt-out request. Cranor et al. found that a "toggle" icon most clearly conveys to consumers the presence of privacy choices, however the icon that the Attorney General recommends in the modified draft regulations is significantly different from the icon recommended in the Cranor study, and does not clearly convey the same information.[12]

W256-1 (cont.)

The toggle icon tested in Cranor's research is a rounded, pill shaped button divided vertically, with the left portion of the button displaying a blue checkmark on a white background, and the right portion of the icon showing a white "x" mark on a blue background (*see* Fig. 1). Every "toggle" icon tested in the Cranor study included some combination of two elements that help convey a binary decision (e.g. a +/-, a ✓/x, ✓/-, etc.)[13]. When asked to interpret this icon, consumers commonly interpreted it as "Accept/decline something", "activate/deactivate something", "okay/exit" options, or as indicative of the ability to mark something as "true" or "false."

[12] Cranor *et al.*, "Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA", p. 3 (2020) (available at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-cranor.pdf).

[13] *See id.* at 42.

Fig. 1: Toggle Icon Recommended by Cranor et al.[14]

Fig. 2: Toggle Icon Recommended in Mod. Reg. Sec. 906(f).

Conversely, the icon proposed in the modified draft regulations more resembles an interactive toggle switch, with the left half of the button displaying a white circle on a red background, and the right half of the button displaying a white x on that same red background (*see* Fig. 2).The icon appears to be an interactive toggle switch set to the "left", the white "x" seeming to indicate that whatever option was just selected is a negative option. The fact that the icon is red further reinforces this interpretation. W256-1 (cont.)

Cranor *et al* noted that there is already a risk that a toggle icon can be interpreted as an actual control (rather than a static icon), which could deter users from interacting with it.[15] The design recommended by the Attorney General encourages this misinterpretation by resembling an interactive toggle switch rather than an icon visually representing a binary choice.

Recommendations for reducing consumer confusion.

Rather than clearly conveying the presence of an opt-out right, the ambiguous button invites consumers to ask, "Is this an interactive toggle?" "If this is a toggle, is the toggle set to 'yes, sell my personal information' or 'no, do not sell my personal information'?" and "Does the red 'x' mean my information is already being sold, or does it mean I have not yet exercised my right to opt-out of those sales?"

The privacy coalition respectively recommends that the Attorney General redesign the opt-out button to reduce the possibility of confusion by using the toggle icon recommended by Cranor et al.; a blue icon that includes both a check mark and an x mark, to help convey the presence of choice. Further, it is left unclear how this icon will display across mobile devices and different user agents, and so we urge the Office to ensure that their recommendations with regard to the opt-out icon will display clearly and legibly on any device that the consumer uses to access the business's website.

[14] *See id.* at 3.

[15] *See id.* at 31.

Section 313(d)(1). Unverifiable Requests to Delete.

The modified regulations would create additional burdens on the exercise of consumer rights.

The coalition opposes the Attorney General's modified draft rule which would allow a business that cannot verify the identity of a deletion requestor to, instead of treating the request as one to opt-out of sale as initially proposed, instead allow the business to respond by asking the consumer if they would like to opt-out of the sale of their personal data and providing information about opting out. Having businesses add an additional step for consumers to take, versus automatically treating the request as one not to sell, is burdensome on consumers and time-strapped families. Further, consumers may already feel overwhelmed by various "privacy choices" including exercising their rights under the CCPA and this provision adds to the confusion. A Pew Research Center survey, polled U.S. adults on their understanding of the current laws and regulations in place to protect their data privacy and 63% said they understand very little or not at all, so it may be difficult for them to exercise their rights.[16] Thus, the coalition proposes Mod. Reg. Sec. 999.313(d)(1) be revised to the original language, by having a business treat an unverified request to delete as a request to opt-out of sale.

W256-4 (cont.)

Section 314(c)(1). Service Providers Use of Personal Information.

The modified regulations would inappropriately expand the rights of service providers to use personal information.

We appreciate that the modified draft regulations remove the explicit allowance of service providers combining personal information from two different entities for security and fraud purposes. However, we are concerned that the new enumerated list of exceptions still enables service providers to combine information for those purposes (as a "use" of information to protect against security incidents or fraud under Mod. Reg. Sec. 314(c)(4)) as well as a host of other new activities.

W256-6 (cont.)

For example, Mod. Reg. Sec. 314(c)(1) enables service providers to use or share information as long as it is to perform a service specified in a contract. This is not limited to services which benefit the contracting business. Service providers, especially larger ones, can and do specify all manner of activities in a contract, not all of which benefit businesses or consumers.

Mod. Reg. Sec. 314(c)(3) enables service providers to use personal information to build and improve the quality of their products and services, so long as this use "does not include building or modifying household or consumer profiles, or cleaning or augmenting

[16] Brooke Auxier & Lee Rainie, *Key takeaways on Americans' views about privacy, surveillance and data-sharing*, Pew Research Center (Nov. 15, 2019).

data acquired from another source". Presumably, reaching out to consumers directly to advertise or offer new products or seek other feedback would qualify, as long as a "profile" is not created. This stretches the notion of what a consumer expects from a service provider.

We request that Mod. Reg. Sec. 314(c)(1)–(5) be replaced with the text originally proposed:

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.~~

W256-6 (cont.)

Section 317(g). Transparency

The modified regulations would be a step backwards on transparency.

Previous draft regulations called for companies to post metrics about their CCPA compliance if they collected information on over 4 million consumers. The coalition noted that this threshold was too high, and requested that businesses be required to publish metrics on their compliance with CCPA requests to those with either $25 million in annual revenue, or 50% of revenue generated from the sale of personal information. Instead, in a step in the opposite direction, the modified draft regulations require even fewer companies to report--those with over 10 million consumers--even ones whose entire business model may be premised on selling consumers' personal information. This will increase business opacity and make it harder for consumers, as well as legislators, journalists, and public interest advocates, to understand how companies are protecting privacy and complying with the CCPA.

Transparency about compliance is critical, especially given that the Attorney General has noted he has capacity for only a few cases a year. We respectfully request that the regulations be changed per our earlier suggestion:

A business that alone or in combination ~~buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 10,000,000 or more consumers in a calendar year~~ has annual gross revenues in excess of twenty-five million dollars or derives 50 percent or more of its annual revenues from selling consumers' personal information, shall:

W256-5 (cont.)

Conclusion

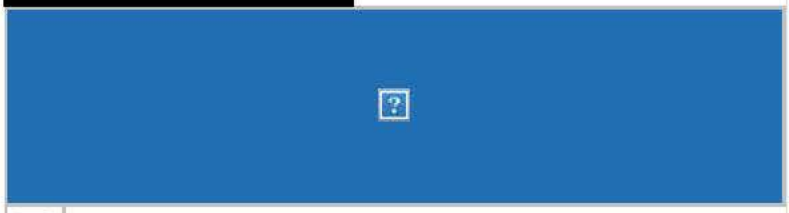
The coalition appreciates the Attorney General's work on these modified proposed rules and urges the Attorney General to take the steps recommended in these comments to ensure that consumers' privacy rights are protected.

From: Lev Sugarman
To: Privacy Regulations
Subject: Workday Comments: CCPA Proposed Regulations
Date: Tuesday, February 25, 2020 2:13:46 PM
Attachments: Workday CCPA Proposed Regulations Comments.pdf

Comments attached.

Best,

Lev Sugarman
Associate Policy Analyst
c: [redacted]
[redacted]



Thank you for considering the environment.

Workday's Comments on the California Attorney General's Proposed California Consumer Privacy Act Regulations

Workday is a leading provider of enterprise cloud applications for finance and human resources. Founded in 2005, Workday delivers financial management, human capital management, planning, and analytics applications designed for the world's largest companies, educational institutions, and government agencies. Workday's applications empower enterprises to process a wide variety of human resources and finance-related transactions, gain new insights into their workforce and financial performance, and manage employee outcomes consistently on a companywide basis.

Workday appreciates the opportunity to comment on the California Attorney General's proposed California Consumer Privacy Act Regulations, as modified on February 10, 2020. We have three technical comments that seek to reduce the possibility of confusion or misapplication of the Regulations:

- *First*, Workday asks that § 999.314(c)(3), related to service provider use of data to build or improve the quality of its service, be modified so that it doesn't inadvertently impede improvement of data used to train machine learning algorithms. As drafted, the provision prohibits a service provider from using data it obtains in providing services to clean or augment data acquired *from another source in general*. Depending on how the provision is interpreted, a service provider might not be able to use machine learning on data obtained in the course of providing a service to improve the quality of that service. Where businesses are trying to use data obtained in the course of providing their services to improve those services, they must be able to look at data from multiple sources. This is particularly true of machine learning, which is powered by training data. However, none of this data use involves building profiles of individuals. This language should therefore be amended to limit the prohibition on using data obtained in the course of providing services to clean or augment data acquired from another source to cases where the purpose of that cleaning or augmentation is to profile individual households or consumers. W257-1

- *Second*, in § 999.314(b) related to service providers, Workday asks that the phrase "second business" be replaced with the word "entity" to avoid potential confusion with the CCPA's definitions of "business" and "service provider" found in California Civil Code § 198.140. As a software-as-a-service provider, Workday processes our customers' data pursuant to our contracts with them and their instructions; thus, we qualify as a service provider under CCPA. Referring to an entity that the Regulations deem a service provider as a "second business," as the current draft does, could result in confusion as to whether the provisions of CCPA that apply to businesses also apply to that entity. Replacing the phrase "second business" with the word "entity" would eliminate this potential for confusion. W257-2

- *Third*, in the definition of employment-related information found at § 999.301(i), Workday asks that the second sentence be removed. The first sentence of this definition sufficiently defines employee data for the purpose of the notice provisions of CCPA, which are the only provisions that apply presently to W257-3

employment-related information. The inclusion of the second sentence doesn't add to or clarify the definition, and thus is unnecessary. W257-3 (cont.)

* * *

Workday appreciates the opportunity to provide comments on the proposed Regulations, and we would welcome the opportunity to discuss these comments further. Please do not hesitate to contact Jason Albert, Managing Director of Public Policy, at [redacted], with any questions or if we can provide further information.

From:	Gilbert Lara
To:	Privacy Regulations
Cc:	David Nelson
Subject:	Privacy Act Regulations - California Asian Chamber of Commerce
Date:	Tuesday, February 25, 2020 2:10:43 PM
Attachments:	image001.png image002.png image003.png CCPA Letter PDF.pdf

Dear Attorney General Xavier Becerra,

On behalf of the California Asian Chamber of Commerce we are respectfully submitting our comments related to implementation related to the California Privacy Act.

Respectfully

Gilbert Lara
Public Policy Coordinator

CALASIAN chamber of commerce

2331 Alhambra Blvd, Suite 100, Sacramento, CA 95817
P [redacted] | F (916) 446-7098 | calasiancc.org

February 25, 2020

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

Re: California Consumer Privacy Act (CCPA)

Dear Attorney General Becerra:

On behalf of the over 600,000 API small businesses in the State of California trying to comply with the ever-changing laws and regulations enacted upon them by the State Legislature, the California Asian (CalAsian) Chamber of Commerce is submitting comments in regards to the California Consumer Privacy Act (CCPA), of which you have extended the public comment window to today.

Upon talking with our members, our Board, and other industry groups, the CalAsian Chamber is very concerned about the education and outreach component of the CCPA, especially as it relates to compliance. Coming off the heels of the enacting of Assembly Bill 5, and the confusion and fear that still ensues with business owners as to how to comply, we are extremely mindful and aware of how effective education and outreach is necessary with major law changes, and how the lack thereof can negatively affect the day-to-day business operations of entrepreneurs across the State, **disproportionally affecting minority and immigrant business communities**.

This is why we are asking for your Department to take seriously the need for a proactive and assertive, in-language, statewide education and outreach compliance campaign for the implementation of the CCPA.

As you know, compliance is more cost-effective than enforcement, and enforcement without education is not only exorbitantly expensive for businesses, especially business owners of color, it is extremely damaging to the morale of a business owner simply trying to abide by the rules. Enforcement without compliance awareness is devastating to the spirit and drive of the entrepreneur, and California cannot afford to lose successful business activity for the lack of proper compliance education and outreach. It is incumbent upon the Government to provide the education and means to proactively understand compliance of laws they will be enforcing. W258-1

So as you review the many comments that have been submitted to your office regarding the implementation of the CCPA, and carefully consider *what* regulations to write to uphold the law, please be extremely mindful of *how* businesses will know how to be in compliance of those regulations, and what tools and resources your office will use to effectively communicate to the all businesses in the State, and especially API-owned businesses in California. The CalAsian Chamber of Commerce stands at the ready to assist with any proactive outreach necessary on this important issue.

Respectfully,

Pat Fong Kushida

Pat Fong Kushida
President/CEO

From: Jennifer Peters
To: Privacy Regulations
Subject: CCPA Revised Proposed Regulations Comments
Date: Tuesday, February 25, 2020 2:10:02 PM
Attachments: CCPA AG Regs Comments re KIDS (1).pdf

Hello,

Please see our comments related to Modified Regulation Section 308(c)(1)(e)(3) of the CCPA.

Thank you for the opportunity to submit our remarks, please feel free to reach out directly if you have any further questions.

Best,
--

Jen Peters
Advocacy Manager | **Common Sense** Kids Action | She/Her
e: [redacted]
p: [redacted]

Submitted via email February 25, 2020

To: PrivacyRegulations@doj.ca.gov

From: ACLU of Northern California

Campaign for a Commercial-Free Childhood

Common Sense Media

Consumer Federation of America

Privacy Rights Clearinghouse

Comments re Modified Regulation Section 308(c)(1)(e)(3)

The above listed privacy and civil-liberties organizations thank the Office of the Attorney General for its work on these regulations. In addition to broader coalition comments we have submitted separately, we have concerns about the Modified Regulations' requirements regarding privacy policy statements about the sale of minors' information (Section 308(c)(1)(e)(3)).

The change in Mod. Reg. Sec. 308(c)(1)(e)(3) does not advance minors' privacy--rather, to the extent it does anything, it offers an opportunity for companies to try and get out of their CCPA obligations. It is confusing for families what the statement means; it is unusual to have a statement in a privacy policy be made upon a different knowledge standard than other sentences in a privacy policy (which this may be construed as); and to the extent the statement does anything it could permit companies to claim they are in the clear just because they made this statement. A more helpful notice to minors and families that will enable them to learn if a company permits opt-ins to sales, and which also avoids concerns raised by businesses to the initial draft, is to replace Mod. Reg. Section 308(c)(1)(e)(3) as follows: W259-1

"State whether the business permits minors under 16 years of age, or parents of children under 13 years of age, to opt-in to the sale of personal information and describe any mechanism for opting in."

From: Eric Goldman
To: Privacy Regulations
Subject: Eric Goldman Comments on the CCPA Regulations Proposed Modifications
Date: Tuesday, February 25, 2020 2:06:28 PM
Attachments: Eric Goldman Comments to CCPA Regulations Feb 2020.pdf

---

PDF attached. Also available at https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=3156&context=historical Please let me know if you have any problems with it.
Regards, Eric.

Eric Goldman
Professor, Santa Clara University School of Law
Co-Director, High Tech Law Institute & Supervisor, Privacy Law Certificate
Email: [redacted]
Personal website: [redacted]
Blogs: [redacted] & [redacted]
Twitter: [redacted]

Santa Clara University

Comments to the California Department of Justice's (DOJ) Draft Modifications to the California Consumer Protection Act (CCPA) Regulations

February 25, 2020

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

By email: PrivacyRevisions@doj.ca.gov

I am a tenured law professor at Santa Clara University School of Law, where I teach Internet Law. I submit these comments on the "Modifications" to the CCPA proposed regulations (the "revisions") published by the California Department of Justice (DOJ) on February 10, 2020. These comments supplement my prior comments on the proposed regulations that I submitted on December 6, 2019, available at https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=3093&context=historical. These comments represent only my views and not the views of my employer or any third party.

* * *

Notice at Collection

Several sections refer to notice being given to consumers "at or before the point" businesses collect their information. I do not understand the phrase "before the point." I'm not clear how a business could give notice only "before the point" of collection and still satisfy all of the regulations. The DOJ should clarify the phrase. W260-1

IP Addresses as Personal Information

The overbreadth of the CCPA's "personal information" definition—which inherently includes IP addresses—causes the CCPA to unintentionally apply to too many small businesses. Thus, I was pleased to see 999.302 propose to exclude IP addresses from the definition of "personal information," at least in some circumstances. That is an excellent policy goal, and I commend the DOJ for pursuing it. W260-2

However, the revisions' language doesn't achieve its apparent goal. The qualifier "could…reasonably link the IP address with a particular consumer or household" swallows up the exception. IP addresses almost always *could* be reasonably linked to an individual consumer

in the future—even if the service currently lacks the technology to do so and never plans to attempt the linkage.

To eliminate these inconsequential scenarios, the DOJ should delete the words "and could not reasonably link the IP address with a particular consumer or household." With that change, IP addresses automatically would become "personal information" only when a business links them to particular consumers or households. That way, possession of IP addresses in the abstract would remain outside the CCPA, and that would helpfully correct the CCPA's overreach.

W260-2 (cont.)

Oral Disclosures

999.305(a)(3)d contemplates oral disclosures will be made via phone calls and face-to-face conversations. How will such disclosures work? Can the disclosures be highly abstract, such as "we collect your information, check our website for details"? Or will they need to be so detailed that disclosers will need to follow a written script?

W260-3

The Opt-Out Button

The opt-out button in 999.306(f) has at least three problems:

- The iconography sends mixed messages to consumers who want to opt-out. Consumers won't know if they should want to toggle (the circle), cancel (the X), or not act at all because they are OK with the default state.
- The red color warns consumers to stay away.
- Despite the iconography looking like a functional button, a consumer who clicks on the button doesn't actually complete the action. The button just links consumers to a page with more information (999.306(f)(3)). Consumers may not realize that they need to take additional steps to effectuate an opt-out.

W260-4

User-Enabled Global Privacy Controls

The revisions made some improvements on the topic of user-enabled global privacy controls, but the provisions still are not administrable by businesses. Businesses need specific and unambiguous guidance about which versions of which software programs constitute a "user-enabled global privacy control"—due to the extraordinary diversity of browser software (and setting options) as well as plug-ins, plus the fact that these programs change from version to version.

W260-5

I continue to believe the DOJ should revisit this issue in future regulations rather than impose any obligations now, when the technology does not currently exist and businesses are scrambling to comply with other aspects of the law and regulations. If the DOJ insists on pushing the issue now, the DOJ should run a certification process to validate the specific program versions that qualify with the regulations' standards; coupled with an adequate phase-in period to let businesses update their systems. Anything else, such as the ill-defined standards in the revisions, does not put businesses on fair notice of what they must do to comply, and it imposes

unreasonable obligations on businesses to monitor and instantly respond to a vast ecosystem of software programs. W260-5 (cont.)

CCPA Compliance Transparency Reports

I reiterate my prior comments about the utility and cost of these transparency reports. The raised threshold to 10M+ consumers helps reduce the pernicious effects of these requirements. However, the DOJ still has not adequately justified imposing the requirement on any businesses at all. W260-6

Minor Typos

- 999.313(c)(5): "doings" should be "doing." W260-7
- 999.318(a): "deleted" should be "delete." W260-8

What's Missing from the Revisions

A few points from my prior comments that I reiterate:

- The provisions for verifying consumer requests remain too much like standards and don't have enough bright-line safe harbors. W260-9
- The DOJ should commit resources towards prosecuting "perjured" consumer requests per 999.325(c). W260-10
- The CCPA should provide a safe harbor for GDPR-compliant businesses. W260-11
- The $25M threshold in the definition of "business" should be limited to revenues generated in California. W260-12
- The regulations should provide a phase-in period for all businesses that newly cross a numerical threshold in the statute or regulations, rather than forcing unregulated businesses to be 100% compliant in case they possibly cross the threshold. W260-13

Delay in Enforcement

CCPA compliance has been mandatory for 2 months, and the DOJ can start enforcement in 4 months. Despite that, the draft regulations remain a moving target for businesses. The February modifications introduced hundreds of new changes to the draft regulations, many of which have substantial financial implications (such as revisions to the definitions of "personal information" and "households" and the transparency reporting thresholds).

At this point, the DOJ will not be able to give businesses more than a few weeks' notice of the final regulations' text before the DOJ can commence enforcement, and well-meaning businesses cannot anticipate what the final regulations will say or how the goalposts might move again. This uncertainty imposes avoidable expenses and confusion, none of which can be mitigated by well-meaning businesses doing their best to comply with the unfinished law. W260-14

Thus, the DOJ should provide an adequate advance notice period for businesses to comply with the final regulations, instead of requiring 100% compliance on July 1, 2020. Not extending the

deadline would be grossly unfair to businesses that can't comply with regulations that are still evolving.

W260-14 (cont.)

Thank you for considering my comments.

Professor Eric Goldman
Co-Director, High Tech Law Institute
Supervisor, Privacy Law Certificate
Santa Clara University School of Law
500 El Camino Real
Santa Clara, CA 95053
[redacted]

From: Scott Stewart
To: Privacy Regulations
Subject: Innovative Lending Platform Association Comments on Proposed CCPA Regulations
Date: Tuesday, February 25, 2020 2:04:37 PM
Attachments: ILPA Comments on CCPA Proposed Regulations - 2-25-20.pdf

---

Please find comments attached.

Innovative Lending Platform Association

February 25, 2020

VIA EMAIL to PrivacyRegulations@doj.ca.gov

Attorney General Xavier Becerra
c/o Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Dear General Becerra,

I am writing on behalf of the Innovative Lending Platform Association ("ILPA"), a leading trade organization representing a diverse group of online lending and servicing companies that provide financial products and services to small businesses, to share our concerns and request further clarification of the modified proposed regulations for the California Consumer Privacy Act of 2018 ("CCPA"), issued on February 10, 2020.

Our members exclusively serve small businesses and are committed to expanding access to capital for small businesses across the country, particularly in areas underserved by traditional financial institutions. Between 2015 and 2017, five major online lenders, including several of our member companies, funded more than $14 billion in loans to U.S. small businesses. In California, our member companies have provided over $1.8 billion in capital to more than 25,000 small businesses.

Access to credit is critical for small businesses to grow. According to the annual 2019 small business credit survey conducted by 12 U.S. Federal Reserve Banks[1], over half (53%) of small business credit applicants experienced a financing shortfall during the prior year. ILPA members fill this critical gap by leveraging technology, data and analytics to reduce transaction costs and power lending to small businesses.

We strongly believe in protecting our customers' data and treat the personal information of our customers carefully. We are highly supportive of the principles behind CCPA but have concerns about certain provisions of the proposed regulations that may have unintended impacts on our ability to provide much-needed capital to California small businesses. Our concerns and recommendations are set forth below:

- **§ 999.305. Notice at Collection of Personal Information:** The draft regulations do not provide any clarity on how prominent the notice at collection must be on every page beyond the introductory page. We request more detailed rules around this requirement, keeping in mind that a prominent declaration on every web page might not improve the user experience or their understanding that their information is being collected. W261-1

- **§ 999.312(b). Methods for Submitting Requests to Know and Requests to Delete:** The draft regulations state, "A business shall provide two or more designated methods for submitting requests to delete. Acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a link or form available online through a business's website, a designated email address, a form submitted in person, and a form submitted through the mail." However, it does not provide any guidance on how to respond to these differing methods of notification. Mail notifications are unique in their time to reach a business; for interactive forms are there certain fields that we must make available for the consumer to fill out? We request some additional clarity and detail regarding how to deal with these various designated methods for submitting requests. W261-2

  Also, we request further guidance on how to contact a small business borrower through any of these methods without maintaining some information about them. For example, we must maintain a mailing address in order

[1] Federal Reserve Bank, 2019 Report on Employer Firms, Small Business Credit Survey. https://www.fedsmallbusiness.org/medialibrary/fedsmallbusiness/files/2019/sbcs-employer-firms-report.pdf

to send a confirmation of deletion, but that runs contrary to the law. ILPA members would like further guidance on how to handle this specific situation. W261-2 (cont.)

- **Consumer Requests Submitted to Third Parties:** The draft regulations make it clear what a business must do in regards to notifying third parties that it has shared or sold a consumer's data, but it is not clear on what a business should do if it is contacted by one of those third parties with a request to delete consumer information. We request creating clear rules for this circumstance. W261-3

We thank you for the opportunity to present our concerns with the proposed regulations for CCPA on behalf of our members and we would be happy to meet with you at your convenience to discuss these issues as you work towards clarifying guidance.

Sincerely,

Scott Stewart, CEO
Innovative Lending Platform Association

From: Alisa Reinhardt
To: Privacy Regulations
Subject: CNCDA comments re: modifications to CCPA proposed regulations
Date: Tuesday, February 25, 2020 2:00:22 PM
Attachments: CNCDA letter to AG re CCPA Feb 2020.pdf

Good afternoon,

Please find, attached, comments on the recent modifications to the California Consumer Privacy Act proposed regulations.

Thank you,

Alisa Reinhardt
Director of Regulatory Affairs
California New Car Dealers Association
1517 L Street
Sacramento, CA 95814
[redacted] | fax (916) 441-5612
[redacted]

Serving California's Franchised New Car Dealers Since 1924

California New Car Dealers Association

February 25, 2020

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

RE: Modifications to California Consumer Privacy Act Proposed Regulations

Attorney General CCPA Regulations Team:

The California New Car Dealers Association (CNCDA) is a statewide trade association that represents the interests of 1,200 franchised new car and truck dealer members. CNCDA members are primarily engaged in the retail sale and lease of new and used motor vehicles, but also provide customers with parts, service, and automotive repair. CNCDA focuses primarily on (1) protecting and promoting the interests of franchised new car dealers before all state government and regulatory agencies and (2) providing compliance advice to best support our dealer members so that they can provide the best products and services to consumers and maintain high employment rates. We are providing comments and suggestions on these modified proposed regulations today on behalf of our dealer members.

California's new car dealers will endeavor to comply with all new requirements imposed on businesses pursuant to the California Consumer Privacy Act ("CCPA"). However, we think the modified proposed regulations should be further clarified to assist dealers in their compliance efforts.

Pursuant to California Government Code § 11349, adopted regulations must meet all the following standards:

(1) Necessity.
(2) Authority.
(3) Clarity.
(4) Consistency.
(5) Reference.
(6) Nonduplication.

In addition, one of the stated goals of Civil Code Section 1798.185(a)(7) is to minimize the burden on businesses. That is an important goal and should not be ignored in the implementation phase.

Despite a host of concerns with the CCPA statute generally regarding definitions, scope, and aggressive implementation timelines, the majority of our comments are provided under the specific lens of (1) Government Code § 11349 and (2) the overall high burden placed on dealers by various sections of the regulations.

I. Definitions: § 999.301(n) contains a grammatical error.

Section 999.301(n) states the following:

> *"Notice of financial incentive" means the notice given by a business explaining each financial incentive or price or service difference as required by Civil Code section 1798.125, subdivision (b), as required by that section and specified in these regulations.*

W262-1

In the above subsection, "as required by" is used twice in the same sentence and the subsection should be modified.

II. Notice at Collection of Personal Information: § 999.305(a)(2) is unclear, burdensome, and lacks authority.

Section 999.305(a)(2) states the following:

> *The notice at collection shall be designed and presented in a way that is easy to read and understandable to consumers.*

W262-2

Deleting the word "average" in front of "consumer" is unclear, burdensome, and lacks authority. Requiring businesses to tailor notices at collection of personal information to "consumers" denotes that businesses must take an individualized approach here and present notices at collection in whatever way facilitates ease of use by particular consumers, one by one. Having to take into account the individual "ease of use" for each consumer would be incredibly burdensome and unworkable. Any future interpretation of the meaning of this section of the regulations will likely look at the drafting history, and the decision to delete the word "average" is notable.

III. Notice at Collection of Personal Information: § 999.305(a)(3)(c) contains a grammatical error.

Section 999.305(a)(3)(c) states the following:

> *When a business collects consumers' personal information offline, it may 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 where the notice can be found online.*

W262-3

In the above subsection, the word "the" should be deleted in line 3.

IV. Notice at Collection of Personal Information: § 999.305(a)(5) is burdensome, lacks authority, and contains a grammatical error.

Section 999.305(a)(5) states the following:

> *A business shall not use a consumer's personal information for purpose materially different than those disclosed in the notice at collection. If the business seeks to use a consumer's previously collected personal information for a purpose materially different than what was previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.*

W262-4

Requiring businesses to obtain explicit consent from a consumer to use the consumer's personal information for any purpose other than that disclosed in the notice at collection lacks authority.

Civil Code Section 1798.100(b) provides:

> *…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.*

W262-4 (cont.)

As evidenced above, the CCPA statute mandates that businesses must provide *notice* to consumers when they wish to use the consumer's personal information for any purpose other than that disclosed in the notice at collection, but does not provide authority to mandate businesses to obtain *explicit consent* from consumers before using their personal information in this way.

Creating this extra mandate, not authorized by the statute, is overly burdensome on businesses who may decide to institute new business practices or programs. After a business provides consumers with notice about plans to use their information in new and/or different ways, a consumer at that point would have the ability to opt out of that new and/or different use if they object to that new and/or different use.

In addition, the letter "s" should be added to "purpose" in line 1 of Section 999.305(a)(5) above to make the sentence grammatically correct. W262-5

V. Notice of Right to Opt-Out of Sale of Personal Information: § 999.306(a)(2) unclear, burdensome, and lacks authority.

Section 999.306(a)(2) states the following:

> *The notice of right to opt-out shall be designed and presented in a way that is easy to read and understandable to consumers.*

W262-6

As discussed above, deleting the word "average" in front of "consumer" is unclear, burdensome, and lacks authority. Requiring businesses to tailor opt-out notices to "consumers" denotes that businesses must take an individualized approach here and present opt-out notices in whatever way facilitates ease of use by particular consumers, one by one. Having to take into account the individual "ease of use" for each consumer would be incredibly burdensome and unworkable. Any future interpretation of the meaning of this section of the regulations will likely look at the drafting history, and the decision to delete the word "average" is notable.

VI. Notice of Right to Opt-Out of Sale of Personal Information: § 999.306(b)(2) lacks authority.

Section 999.306(b)(2) states the following:

> *A business that substantially interacts with consumers offline shall also provide notice to the consumer by an offline method that facilitates consumer awareness of their right to opt-out. Such methods include, but are not limited to, printing the notice on paper forms that collect personal information, providing the consumer with a paper version of the notice, and posting signage directing consumers to where the notice can be found online.*

W262-7

Directing businesses that substantially interact with consumers offline to also provide notice to the consumer by an offline method lacks authority.

Civil Code Section 1798.130(a)(1) provides:

> *(a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:*
> *(1) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.*

W262-7 (cont.)

Because the CCPA statute does not provide for this third offline method, Section 999.306(b)(2) should simply mirror the privacy policy language in Section 999.308(b), which states that:

> *…A business that does not operate a website shall make the privacy policy conspicuously available to consumers.*

Dealers are already mandated under a bevy of state and federal laws to provide scores of consumer forms and signs. That being said, we do appreciate the modification to Section 999.312(c) giving businesses the ability to direct a consumer's in-person request to a computer terminal so the consumer can utilize the interactive webform already mandated by statute.

VII. Notice of Financial Incentive: § 999.307(a)(2) unclear, burdensome, and lacks authority.

Section 999.307(a)(2) states the following:

> *The notice of financial incentive shall be designed and presented in a way that is easy to read and understandable to consumers.*

As discussed above, deleting the word "average" in front of "consumer" is unclear, burdensome, and lacks authority. Requiring businesses to tailor financial incentive notices to "consumers" denotes that businesses must take an individualized approach here and present financial incentive notices in whatever way facilitates ease of use by particular consumers, one by one. Having to take into account the individual "ease of use" for each consumer would be incredibly burdensome and unworkable. Any future interpretation of the meaning of this section of the regulations will likely look at the drafting history, and the decision to delete the word "average" is notable.

W262-2 (cont.)

VIII. Notice of Financial Incentive: § 999.307(b)(2) is burdensome and unclear.

Section 999.307(b)(2) states the following:

> *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 and the value of the consumer's data…*

W262-8

Adding the requirement for businesses to include a description of the value of the consumer's data in any notice of financial incentive offered seems to require notices of financial incentive to be individualized for each consumer. This requirement would be extremely burdensome and is unclear in how it would be executed.

IX. Notice of Financial Incentive: § 999.307(b)(5)(a) & (b) are burdensome, unnecessary, and unclear.

Section 999.307(b)(5)(a) & (b) state the following:

> *(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 and the value of the consumer's data;*
> *(3) How the consumer can opt-in to the financial incentive or price or service difference;*
> *(4) A statement 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 how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, 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.*

Requiring businesses to calculate the value of a consumer's data, tell consumers how they calculated the value of the consumer's data, and provide a good-faith estimate of the value of a consumer's data is burdensome, unnecessary, and unclear. W262-9

The proposed requirement regarding calculation of value is vague. Requiring businesses to both provide a good-faith estimate of the value of a consumer's data *and* require businesses to describe the methodology they used to calculate the value of the consumer's data seem to be in conflict. A good-faith estimate connotes a certain level of vagueness, while a calculation connotes a certain level of mathematical certainty. A calculation is more onerous in nature than a good-faith estimate.

In addition, the methodology by which a business could undertake this calculation is burdensome and unclear. How do you attach a theoretical dollar amount to a potential vehicle sale transaction or a potential vehicle service event due to consumer information that is maintained for marketing purposes? Plus, this calculation could be different for each person: have they bought a car from the dealer before? Did they buy a high-value vehicle? Do they have family members who may also have vehicle-related needs? The list of possibilities here seems endless, especially for businesses that serve thousands of consumers every year. We understand the need to put some value quotient on consumer data in accordance with the CCPA statute, but Implementation of the CCPA as a whole is already going to be incredibly burdensome for businesses, and the way this section is drafted adds an unnecessary level of administrative headache on top of existing issues.

X. Privacy Policy: § 999.308(a)(2) is unclear, burdensome, and lacks authority.

Section 999.308(a)(2) states the following:

> *The privacy policy shall be designed and presented in a way that is easy to read and understandable to consumers.*

As discussed above, deleting the word "average" in front of "consumer" is unclear, burdensome, and lacks authority. Requiring businesses to tailor privacy notices to "consumers" denotes that businesses must take an individualized approach here and present privacy notices in whatever way facilitates ease of use by particular consumers, one by one. Having to take into account the individual "ease of use" for each consumer would be incredibly burdensome and unworkable. Any future interpretation of the meaning of this section of the regulations will likely look at the drafting history, and the decision to delete the word "average" is notable.

W262-2 (cont.)

XI. Privacy Policy: Request regarding § 999.308(c)(3)(b).

Section 999.308(c)(3)(b) states the following:

> *State whether or not the business sells personal information. If the business sells personal information, include either the contents of the notice of right to opt-out or a link to it in accordance with section 999.306.*

During the initial rollout of business's CCPA compliance efforts throughout the past few months, many dealerships have found that the question of "sale" of a consumer's personal information has raised the most questions and consternation among consumers. This is because the average consumer is unaware of the broad definition of the word "sale" contained in the CCPA statute.

Although the vast majority of dealerships do not "sell" consumer information in the traditional sense of the word (pre-CCPA), they are having to inform consumers that they do in fact "sell" personal information. Many consumers have angrily approached dealership staff asking questions such as, "how much do you get for selling my personal information?" This is a frustrating and confusing question for dealership staff members, because the dealership does not receive any monetary value for the sharing of consumer personal information with any of their vendors or vehicle manufacturers, and consumers think the truth is being obfuscated when they are informed of this fact – e.g., "If you don't get any money for selling my personal information, then why does this form you just gave me say that you do? You must be lying to me."

W262-10

Our request here is the ability to state in a privacy policy whether the business sells ***or shares/discloses*** personal information. If businesses are allowed the ability to affirmatively state that they ***share*** or ***disclose*** personal information, instead of being forced to use the word "sell" when it causes unnecessary anger and confusion for consumers, would be extremely helpful for individual business's compliance efforts and consumers' full understanding of a business's sharing practices.

XII. Methods for Submitting Requests to Know and Requests to Delete: § 999.312(a) is unclear.

Section 999.312(a) states the following:

> *A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to know. All other businesses shall provide two or more designated methods for submitting*

W262-11

requests to know, including, 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.

W262-11 (cont.)

This section was modified to delete the requirement for businesses that operate a website to provide an interactive webform for consumers to use when submitting requests to know. We support this modification, but since the option to provide an interactive webform is not specifically provided for in the listing of other acceptable methods, we would like to request clarification that an interactive webform is still one of the acceptable methods.

XIII. Methods for Submitting Requests to Know and Requests to Delete: § 999.312(e)(1) & (2) are burdensome, unclear, and lack authority.

Section 999.312(e)(1) & (2) state the following:

(e) If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either:
(1) Treat the request as if it had been submitted in accordance with the business's designated manner, or
(2) Provide the consumer with information on how to submit the request or remedy any deficiencies with the request, if applicable.

W262-12

Requiring businesses to (1) treat deficient consumer requests as if they had been submitted correctly or (2) respond to deficient consumer requests and give information on how to remedy deficiencies with the request is burdensome, unclear, and lacks authority.

There are many ways in which a consumer request could be deficient. This could involve lack of identifying information, lack of clarity about what is being requested, and submitting a request in a manner not contemplated by the CCPA statute. Despite the modification to this section, expecting busy business owners and employees to be able to read a consumer's mind and divine what they are asking, when that request is patently unclear, is overly burdensome and constitutes an unfair requirement.

XIV. Responding to Requests to Know and Requests to Delete: § 999.313(c)(1) lacks authority.

Section 999.313(c)(1) states the following:

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 requestor 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).

W262-13

Requiring businesses to evaluate a denied request for specific pieces of information and instead treat the request as if the consumer is seeking the disclosure of categories of personal information is not provided for by the CCPA statute and lacks authority. Instead, the request should simply be granted or denied. The modifications to

Section 999.313(d)(1) (deleting the requirement to treat deficient deletion requests as requests to opt out of sale) should be mirrored here. W262-13 (cont.)

XV. Responding to Requests to Know and Requests to Delete: § 999.313(c)(5) contains a grammatical error.

Section 999.313(c)(5) states the following:

> *If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial, unless prohibited from doings so by law. If the request is denied only in part, the business shall disclose the other information sought by the consumer.*

W262-14

In the above subsection, the letter "s" should be deleted from the word "doings" in line 4.

XVI. Responding to Requests to Know and Requests to Delete: § 999.313(d)(1) is unnecessary, unclear, and lacks authority.

Section 999.313(d)(1) states the following:

> *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. If the business sells personal information and the consumer has not already made a request to opt out, the business shall ask the consumer if they would like to opt out of the sale of their personal information and shall include either the contents of, or a link to, the notice of right to opt-out in accordance with section 999.306.*

W262-15

Requiring businesses to ask consumers who they have not been able to verify whether they would like to opt-out of the sale of their information is not provided for under the CCPA statute and lacks authority. If a deletion request is unverifiable, the process should stop once the business notifies the consumer that the request was unverifiable. It is acceptable for businesses to share the opt-out *notice* with unverifiable consumers who have submitted deletion requests, but businesses should not have to *affirmatively ask* unverifiable consumers "if they would like to opt out," without any other means of verification provided, especially since the consumer's request may be fraudulent in nature.

In addition, requiring businesses to look through opt-out requests just to ascertain whether an unverifiable consumer submitting a deletion request has already made an opt-out request is overly burdensome.

XVII. Responding to Requests to Know and Requests to Delete: § 999.313(d)(2)(c) is unclear.

Section 999.313(d)(2)(c) states the following:

> *(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. Deidentifying the personal information; or*
> *c. Aggregating the consumer information.*

W262-16

"Personal information" is a term defined by the CCPA statute, but "consumer information" is not. The purpose behind this modification to the regulations, and how businesses can comply with the CCPA in accordance with the modification, is unclear. W262-16 (cont.)

XVIII. Responding to Requests to Know and Requests to Delete: § 999.313(d)(5) is unnecessary and lacks authority.

Section 999.313(d)(5) states the following:

> *If the business complies with the consumer's request, the business shall inform the consumer that it will maintain a record of the request as allowed by Civil Code section 1798.105, subdivision (d). A business may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from the business's records.*

W262-17

Requiring a business to disclose that it will maintain a record of a deletion request "as allowed by" Civil Code Section 1798.105(d) is unnecessary and lacks authority. Although Civil Code Section 1798.105(d) is referenced, this section does not include a mandate to maintain records of requests or disclose to consumers that they maintain records of requests. In fact, retention of these requests is not referenced at all. In addition, it is unclear how these requests are supposed to be maintained, especially if consumer data is deleted and so the request cannot be linked to a consumer record.

XIX. Requests to Opt-Out: § 999.315(a) & (b) lack authority.

Section 999.315(a) & (b) state the following:

> *(a) A business shall provide two or more designated methods for submitting requests to opt-out, including an interactive form 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 global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information.*
>
> *(b) A business shall consider the methods by which it interacts with consumers when determining which methods consumers may use to submit requests to opt-out, the manner in which the business sells personal information to third parties, available technology, and ease of use by the consumer. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer.*

W262-18

Requiring a business to provide two or more designated methods for submitting requests to opt-out lacks authority. Civil Code Section 1798.135 mandates businesses to provide an opt-out link on Internet homepages, but does not provide for additional opt-out methods as described in Section 999.315(b).

XX. Requests to Opt-Out: § 999.315(b) is unclear, burdensome, and lacks authority.

Section 999.315(b) states the following:

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

W262-2 (cont.)

As discussed above, deleting the word "average" in front of "consumer" on line 4 of the above subsection is unclear, burdensome, and lacks authority. Requiring businesses to tailor opt-out methods to "the consumer" denotes that businesses must take an individualized approach here and present opt-out methods in whatever way facilitates ease of use by particular consumers, one by one. Having to take into account the individual "ease of use" for each consumer would be incredibly burdensome and unworkable. Any future interpretation of the meaning of this section of the regulations will likely look at the drafting history, and the decision to delete the word "average" is notable.

XXI. Requests to Opt-Out: § 999.315(c) is unclear, burdensome, and lacks authority.

Section 999.315(c) states the following:

> *A business's methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out. A business shall not utilize a method that is designed with the purpose or substantial effect of subverting or impairing a consumer's decision to opt-out.*

W262-19

Requiring a business to provide methods for submitting requests to opt-out that are "easy" is incredibly subjective. What if a business offers a toll-free telephone number and an in-person form but a particular consumer does not have "easy" access to a telephone or a car? This subsection should be removed due to being burdensome and unclear.

XXII. Requests to Opt-Out: § 999.315(d) is burdensome and lacks authority.

Section 999.315(d) states the following:

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

W262-20

Requiring a business that collects personal information from consumers online to treat user-enabled general browser privacy controls as valid requests to opt out submitted pursuant to Civil Code Section 1798.120 is burdensome and lacks authority.

If the regulations are attempting to cover tech companies that regularly track consumers' browsing data, they need to be narrowly tailored as such. As written, this section does not give consumers meaningful choice and covers *all* businesses. This change in the law is not authorized under the CCPA statute. W262-20 (cont.)

In addition, this section assumes that all computer systems and tracking mechanisms are compatible, which may not be the case.

XXIII. Requests to Opt-Out: § 999.315(d)(1) contains a grammatical error.

Section 999.315(d)(1) states the following:

> *Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to the opt-out of the sale of personal information. The privacy control shall require that the consumer affirmatively select their choice to opt-out and shall not be designed with any pre-selected settings.*

W262-21

The word "the" should be deleted from line 2, above (highlighted).

XXIV. Requests to Opt-In After Opting Out of the Sale of Personal Information: § 999.316(a) is burdensome and lacks authority.

Section 999.316(a) states the following:

> *Requests to opt-in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.*

W262-22

Requiring businesses to implement a two-step opt-in process after a consumer has opted out of the sale of personal information is not mandated by the CCPA statute and lacks authority. This requirement is excessive and will be hard for businesses to manage.

XXV. Training; Record-Keeping: § 999.317(b) and (c) are unnecessary and lack authority.

Section 999.317(b) & (c) state the following:

> *(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. The business shall implement and maintain reasonable security procedures and practices in maintaining these records.*
>
> *(c) The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.*

W262-23

Requiring businesses to maintain detailed records of consumer requests made pursuant to the CCPA and how the business responded to those requests for 24 months is unnecessary and lacks authority under the CCPA statute.

XXVI. Requests to Access or Delete Household Information: § 999.318(a) contains a grammatical error.

Section 999.318(a) states the following:

> *Where a household does not have a password-protected account with a business, a business shall not comply with a request to know specific pieces of personal information about the household or a request to deleted household personal information unless all of the following conditions are satisfied:*

W262-24

The letter "d" should be deleted from the word "deleted" (highlighted above).

XXVII. Requests to Access or Delete Household Information: § 999.318(a)(3) is unclear and burdensome.

Section 999.318(a)(3) states the following:

> *(a) Where a household does not have a password-protected account with a business, a business shall not comply with a request to know specific pieces of personal information about the household or a request to deleted household personal information unless all of the following conditions are satisfied:*
> *(1) All consumers of the household jointly request access to specific pieces of information for the household or the deletion of household personal information;*
> *(2) The business individually verifies all the members of the household subject to the verification requirements set forth in section 999.325; and*
> *(3) The business verifies that each member making the request is currently a member of the household.*

W262-25

Requiring businesses to verify that each member of a household making a request is *currently* a member of a household at the time of the request is overly burdensome and unclear in how it would be executed. Compliance with this subsection would be incredibly difficult.

XXII. General Requests.

1) Provide guidance on a business' right to cure and how that process will work. W262-26
2) Provide model forms and notices businesses can use to help with compliance efforts. W262-27
3) Streamline required notices as much as possible so that consumers are not over-informed at every turn and business compliance is made more manageable. W262-28
4) Provide more time for businesses to implement these drastic changes to their day-to-day practices. W262-29
5) In cost estimates, account for the need for an attorney or compliance officer to decipher the law's requirements and implement them at a business. W262-30
6) Consider classifying vehicle geolocation data as sensitive information that should not be disclosed. W262-31
7) If consumer information needs to be shared between businesses for reasonable safety and security purposes (such as vehicle history, safety, & performance), this information should not be subject to opt-out requests. W262-32

California's new car dealers understand the state's goals to provide consumers with greater control over how their data is used by businesses. However, the CCPA's overall impact on businesses cannot be overstated. There are over 1,300 franchised new car dealers in the state of California alone, and almost every single one of them will be heavily impacted by the new law. Because of this enormous impact, we appreciate the opportunity provided to provide our comments and feedback on the implementing regulations. While we appreciate some of the

modifications that have been made to date, we believe more modifications should be made to increase clarity regarding compliance obligations.

We welcome the opportunity to discuss this series of suggestions further. Please don't hesitate to contact me at [redacted] or [redacted]

Sincerely,

Alisa Reinhardt
Director of Regulatory Affairs, California New Car Dealers Association

From:	Porter, Erica
To:	Privacy Regulations
Cc:	Kurpiewski, Christian
Subject:	Senator Jackson"s Comments on the Proposed CCPA Regulations
Date:	Tuesday, February 25, 2020 1:52:39 PM
Attachments:	Sen Jackon Comments on CCPA Regulations.pdf

Good afternoon,

Attached is a letter from Senator Hannah-Beth Jackson, Chair of the Senate Judiciary Committee, regarding the California Attorney General's recent proposed regulations around the CCPA.

Thank you.

Erica Porter
She/Her/Hers
Committee Assistant
Senate Judiciary Committee
State Capitol, Room 2187
[redacted]

California Legislature

Senate Committee on Judiciary

HANNAH-BETH JACKSON
CHAIR

STATE CAPITOL
ROOM 2187
SACRAMENTO, CA 95814
TEL (916) 651-4113
FAX (916) 403-7394

February 25, 2020

Attorney General Xavier Becerra
c/o Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Dear Attorney General Becerra,

Once again, thank you and your staff for your tireless work executing your regulatory obligations pursuant to the California Consumer Privacy Act (CCPA). I know it must be a thankless task and that the Attorney General's office is being bombarded on all sides. As you know, I did not weigh in on your initial proposed regulations. Although I hoped for slightly more privacy-protective language in some provisions, your office did an amazing job and deserve a medal for your efforts. However, I have read through the recently released, modified regulations and feel that I must express deep concern regarding one of them in particular.

Since the moment the CCPA became law in 2018, there has been a constant onslaught of proposals, bills, and other efforts to undermine the protections of the CCPA and diminish its scope. I have worked tirelessly to fend off these attacks and to ensure that only those bills truly seeking to clarify and simplify the law are enacted. One specific area that I find sacrosanct is what is considered "personal information" for purposes of the CCPA and therefore afforded its protections. Relatedly, I have pushed back on efforts to inappropriately expand carve outs from the definition, such as efforts seeking to expand the definition of "deidentified information." Although I believe I have been successful in defending these core definitions of the CCPA, I believe that Section 999.302 of your modified proposed regulations weakens the very definition we have been fervently protecting. W263-1

The section provides that IP addresses are not personal information so long as the business "does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household." Such a regulation directly contradicts the CCPA's definition of "personal information," which includes the following in its non-exhaustive list of information considered personal information: "Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar

identifiers." (Civ. Code § 1798.140(o)(1)(A).) This definition appreciates that IP addresses are sensitive enough to not only be covered by the CCPA but to be associated with other similar identifiers such as name and social security number. In fact, IP addresses are also explicitly included in the definition of "unique personal identifier":

> "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; **an Internet Protocol address**; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device.

W263-1 (cont.)

(Civ. Code § 1798.140(x), emphasis added.) The intent of this language is to make clear that IP addresses can identify particular consumers and devices and, when tracked systematically and surreptitiously, create serious privacy concerns.

Section 999.302 would only consider an IP address personal information if the business collecting it did not, and could not reasonably, *link* it with a particular consumer or household. While the ability to *link* such information to a particular consumer or household is one of the bases under which information would fall into the definition of "personal information," it is not the only one. Personal information also includes any "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." (Civ. Code § 1798.140(o)(1).) The definition is drafted much broader than the regulation would render it, and legislative attempts to narrow what is considered personal information in such a manner, such as in AB 873 (2019), were rejected by the Legislature. The regulation would allow the widespread collection and sale of this sensitive piece of personal information without any requirements to notify consumers or provide them with the right to opt out of the sale of the information.

I understand this proposed regulation is likely intended to clarify the law and simplify compliance, but I believe the regulation significantly changes it. The CCPA already makes clear that certain obligations imposed by the law do not require businesses to collect, retain, or otherwise reidentify or link information if the information is maintained in a manner that would not be considered personal information. (Civ. Code §§ 1798.100(e), 1798.110(d), 1798.145(k).) But this wholesale exemption from the protections of the CCPA goes well beyond that. It is for these reasons that I urge you to delete Section 999.302 from your final regulations.

Sincerely,

Senator Hannah-Beth Jackson

From: Tengel, Brian R.
To: Privacy Regulations
Subject: Experian Comments to the California Attorney General on CCPA Revised Proposed Regulations
Date: Tuesday, February 25, 2020 1:51:01 PM
Attachments: Experian Comments to the California Attorney General on CCPA Revised Proposed Regulations.pdf

---

Attorney General Becerra:

On behalf of Experian, please find attached comments on the revised proposed CCPA regulations.

Thank you,

Brian Tengel

Brian R. Tengel, Esq. | Venable LLP
t [redacted] | f 202.344.8300 | m [redacted]
600 Massachusetts Avenue, NW, Washington, DC 20001

[redacted] | www.Venable.com

February 25, 2020

Via electronic filing

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

Re: The California Consumer Privacy Act Revised Proposed Regulations

Attorney General Becerra:

I am pleased to offer the enclosed comments on behalf of Experian regarding the revised proposed regulations to implement the California Consumer Privacy Act of 2018 ("CCPA") dated February 10, 2020.[1]

As we noted in our previous comments dated March 8, 2019, and December 6, 2019, Experian is comprised of a family of companies that are tied together by two simple objectives: (1) helping organizations protect, manage, and understand their data; and (2) helping consumers make informed choices and live smarter lives. Experian's products and services facilitate consumers' access to credit, protect families from identity theft, provide consumers expert education on credit management, and provide numerous anti-fraud tools to businesses.

Consumer privacy is central to Experian's corporate values, and we applaud the California legislature's goal of increasing consumer privacy and transparency, as well as the Attorney General's continued efforts to engage with stakeholders as part of furthering the CCPA's purposes through the subject regulations. While the revised proposed regulations strengthen and improve the original proposed regulations[2] in several respects, below we highlight three important issues that we believe the final regulations should address. First, the Attorney General should promulgate a new regulation clarifying that the CCPA's reference to "professional or employment-related information" excludes business-related information in commercial credit reports. Second, the Attorney General should promulgate a new regulation clarifying that the CCPA exempts data processing for anti-fraud purposes and protects the ability to create legitimate fraud prevention tools. As noted in our previous comments, both of these new regulations would further the purposes of the CCPA and would ensure that businesses like Experian have the information they

[1] The revised proposed regulations were released on February 7, 2020 but were subsequently modified on February 10, 2020. *See* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf.

[2] The original proposed regulations were released on October 10, 2019. *See* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf.

need to provide commercial credit reports and anti-fraud tools and services.[3] Finally, we request that the Attorney General revise Section 999.315 to clarify that businesses are not required to share opt-out requests with third parties.

1. *Promulgate a New Regulation Clarifying that the CCPA's Reference to "Professional or Employment-Related Information" Excludes Business-Related Information in Commercial Credit Reports*

The CCPA's definition of "personal information" includes "professional or employment-related information."[4] In the revised proposed regulations, the Attorney General defined the term "employment-related information" to mean "personal information that is collected by the business about a natural person for the reasons identified in Civil Code section 1798.145, subdivision (h)(1)."[5] That subdivision generally covers personal information collected about a natural person in the employment context. W264-1

Experian understands that "professional or employment-related information" was included in the CCPA's definition of personal information to capture scenarios where an individual's profession helps define that person when marketers, retailers, or others offering consumer products or services are seeking to segment the consumer market. For example, certain generalizations made about blue-collar workers versus white-collar workers may be used for consumer marketing purposes. The revised proposed regulations, however, now define the term "employment-related information" in a manner that broadly sweeps business or employment-related data into the definition of personal information, regardless of whether the individual to whom the data is linked is acting in a consumer capacity or professional capacity.[6]

If this proposed definition were to become final, the CCPA would give individuals the right to delete or prevent the sharing of all business or employment-related information about them, which could include information about businesses (including financial information, business records, and other non-consumer information) to the extent that it is associated with a particular

[3] Promulgating these regulations would also be consistent with the recent actions of the California legislature, which likewise recognized and sought to address certain unintended CCPA consequences for businesses when it amended the law last fall to exclude personal data collected in the employment context and in a business-to-business context, until January 1, 2021. *See* Cal. Civ. Code § 1798.145(h)(1)(A)–(C), (n)(1).

[4] "Personal information" means "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," including "[p]rofessional or employment-related information." Cal. Civ. Code § 1798.140(o)(1)(I).

[5] Cal. Code Regs. tit. 11, § 999.301(i) (proposed Feb. 10, 2020). The regulation further provides that "[t]he collection of employment-related information, including for the purpose of administering employment benefits, shall be considered a business purpose." *Id.*

[6] Although a temporary exclusion currently exists in the CCPA for personal information collected in the employment context, *see supra* note 3, this exclusion is set to expire at the end of this year and thus does not provide a permanent solution to the problem.

individual. Business or employment-related information serves as the foundation of the commercial credit reports that Experian and other companies have provided to the market for decades and that enable businesses to make prudent lending decisions.[7] If all business or employment-related information in these reports continues to qualify as personal information under the CCPA, the deletion and opt-out rights afforded by the law would jeopardize the accuracy and reliability of such reports.[8]

As detailed in our previous comments, many serious unintended consequences could result if the CCPA were interpreted to cover the business-related information in commercial credit reports. These consequences include that federal and state government agencies—as well as private actors—may be unable to conduct proper due diligence before making important business decisions, and that furnishers of business credit information may stop providing data.

W264-1 (cont.)

For these reasons, we request that the Attorney General modify the term "[p]rofessional or employment-related information" (including the newly defined term "employment-related information") to expressly exclude information about individuals like business representatives and sole proprietors acting in their business capacities, *i.e.*, personal and related business information used in commercial credit reports.[9]

2. *Promulgate a New Regulation Clarifying that the CCPA Exempts Data Processing for Anti-Fraud Purposes and Protects the Ability to Create Legitimate Fraud Prevention Tools*

The CCPA's exemptions do not fully exempt data processing for anti-fraud purposes. First, although the fraud exemption in the CCPA's data deletion requirement clearly covers users of fraud tools (who "maintain the consumer's personal information in order to . . . protect against . . . fraudulent . . . activity"),[10] arguably, the exemption does not cover Experian's data suppliers that provide information necessary to create those fraud tools because those data suppliers do not necessarily maintain the information in order to protect against fraudulent activity. The exemption also may not enable Experian's use of data to create and enhance anti-fraud tools because Experian does not just use these tools to protect Experian from fraud, but sells these tools in the marketplace to enable businesses to protect themselves from fraud. Second, even though the CCPA clearly exempts data processing for anti-fraud purposes from the scope of the deletion right, the law is far

W264-2

[7] This information includes data elements such as an individual's name, address, birthdate, and tax ID number, as well as any judgments instituted against the individual, d/b/a information, and information from various Secretaries of State on commercial licenses the individual may hold, among other data points.

[8] Although personal information contained in *consumer* credit reports is expressly exempted from the ambit of the CCPA, no such exception is made for data in *commercial* credit reports. Cal. Civ. Code § 1798.145(d).

[9] As previously noted, the Attorney General has specific authority to adopt rules to "updat[e] as needed additional categories of personal information." Cal. Civ. Code § 1798.185(a)(1). The Attorney General also has general authority to adopt rules to "further the purposes of this title." *Id.* §§ 1798.185(a), (b)(2).

[10] Cal. Civ. Code § 1798.105(d)(2).

less clear regarding an analogous exemption to the opt-out right for such anti-fraud data processing.

As a result of this imprecise drafting in the CCPA, the law could inadvertently restrict the ability to gather the information needed to create, provide, enhance, or deliver anti-fraud tools and services, impacting the government and private sector actors that rely on these tools and potentially exposing consumers to an increased risk of fraud. For this reason, and for the reasons explained in our previous comments, we request that the Attorney General promulgate a new regulation to clarify (1) the scope of the fraud exemption to the deletion right and (2) that such an exemption also exists for the opt-out right in the CCPA. In particular, we request that the Attorney General clarify that the CCPA fraud exemption to the consumer deletion right covers the collection, use, and sharing of personal information to create and distribute fraud prevention and detection tools. We also ask the Attorney General to clarify that a parallel exemption exists for the opt-out right so consumers may not opt out of a business's sharing of personal information for fraud prevention purposes.

W264-2 (cont.)

3. *Businesses Should Not Be Required to Share Opt-Out Requests with Third Parties*

Section 999.315(f) of the revised proposed regulations provides that, if a business sells a consumer's personal information to any third parties after the consumer submits their opt-out request but before the business complies with that request, the business must notify those third parties that the consumer has exercised their opt-out right and must direct those third parties not to sell that consumer's information.[11]

Although Experian appreciates the Attorney General's revisions to this proposed regulation, we respectfully submit that the regulation's requirement for businesses to share opt-out requests with third parties—even given the narrowed scope of the revised regulation—would prove unduly burdensome by imposing new tracking and disclosure obligations on businesses. Requiring businesses to share opt-out requests with third parties would necessarily involve expending considerable resources to develop and implement new systems, processes, and delivery mechanisms to communicate the opt-out requests to third parties and to manage and track those requests. The burdens imposed by this regulation are inconsistent with the California legislature's intent to appropriately balance the costs to businesses and benefits for consumers.

In sum, we request that the Attorney General revise Section 999.315 to clarify that businesses are not required to share consumers' opt-out requests with third parties.

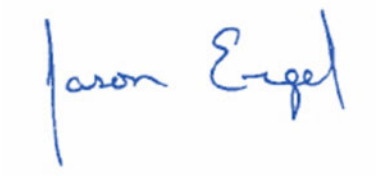
W264-3

[11] Cal. Code Regs. tit. 11, § 999.315(f).

* * * *

Thank you for this opportunity to provide input on the California Consumer Privacy Act rulemaking. Please feel free to contact me with any questions or requests for additional information. We look forward to continuing to work with your office on these important matters.

Regards,



Jason Engel
Senior Vice President and General Counsel
Experian North America

From: Anya Stewart
To: Privacy Regulations
Cc: Seren Taylor
Subject: Submission of PIFC CCPA Regulatory Comments
Date: Tuesday, February 25, 2020 1:44:36 PM
Attachments: image001.png
image002.png
PIFC CCPA Regulatory Comments - Final.pdf

To Whom it May Concern:

Attached, please find comments regarding Department of Justice (Attorney General) February 10, 2020 modified proposal to adopt § 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).

Please let me know if there are any questions.

Best,
Anya

Anya Stewart
Legislative and Communications Manager
Personal Insurance Federation of CA

T: [redacted]
F: (916) 446-9548
W: www.pifc.org
E: [redacted]
1201 K Street, Suite 950
Sacramento, CA 95814

PIFC

Date February 25, 2020

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

SUBJECT: Comments regarding Department of Justice (Attorney General) February 10, 2020 modified proposal to adopt § 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,

The Personal Insurance Federation of California (PIFC) respectfully submits the following comments and concerns regarding the modifications to the proposed CCPA regulations first published on October 11, 2019.

The modifications to the proposed regulations resulted in some notable improvements, which we appreciate. However, the changes failed to address the vast majority of our concerns and some of the revisions exacerbate the many problematic aspects of the CCPA. Therefore, we remain very concerned that these regulations include significant new requirements that are causing insurers to alter their current compliance framework and communications protocol under an already tight implementation timeframe.

Given the complexity of the regulations, and the fact that certain provisions of the proposed regulations exceed the substantive and procedural scope of the statute, *we reiterate our request that the effective date of the regulations be at least 18 months from final issuance of the regulation.* Companies must have reasonable time to come into compliance with these comprehensive rules, and the CCPA grants the Attorney General discretion to delay enforcement of the regulations.

We provided extensive comments regarding the original draft regulations on December 4, 2019. Thus, the comments below will focus on the most recent changes.

Proposed § 999.302. Guidance Regarding the Interpretation of CCPA Definitions

(a): The newly proposed guidance regarding the definition of "personal information" (PI) is an improvement relative to the prior draft regulations. However, we have significant concerns about the lack of clarity regarding the language "*...or could be reasonably linked....*" W265-1

Government Code section 11349(c) defines "clarity" as meaning "...written or displayed so that the meaning of regulations will be easily understood by those persons directly affected by them."

Personal Insurance Federation of California
1201 K Street Suite 950 Sacramento California 95814
T (916) 442 6646 F (916) 446 9548 E www.pifc.org

The clarity standard is further defined in section 16 of title 1 of the California Code of Regulations (CCR), which provides, among other things, that a regulation shall be presumed not to comply with the "clarity" standard if the regulation can, on its face, be reasonably and logically interpreted to have more than one meaning.

Since it is unknown what that phraseology means in practice, and it could be interpreted many different ways, we request that the words "*or could be reasonably linked*" be deleted. Further, there is no purpose to having such language if the information is not, in fact, ever linked to any consumer or household.

W265-1 (cont.)

Proposed §999.305 Notice at Collection of Personal Information

(a)(3)(d): The regulation provides that *"When a business collects personal information over the telephone or in person, it may provide the notice orally."*

This could be interpreted to mean reading the entire notice over the phone, which may be impractical for both the business and the consumer. Therefore, we request that an option to orally ***direct the consumer to where the notice can be found online*** be added to the regulation.

W265-2

(4): The proposed regulation requires that *"When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection."*

We are concerned that determining the consumer's "reasonable" expectations is subject to great interpretation, and the screen size and character limits may make just-in-time notices impractical. Therefore, we request that the regulations be amended to simply require a link to the full terms, which is a better approach for all parties.

W265-3

Proposed § 999.314. Service Providers

The regulations restrict service provider retention, use or disclosure of personal information except for enumerated purposes that are much narrower than what is permitted under CCPA (Civil Code Section 1798.140(v)). Among other things, in the definition of a service provider, the CCPA permits the provider to retain, use or disclose the PI "*as otherwise permitted by this title.*"

We request that the draft regulations be amended better align with the statute, and not be unnecessarily restrictive or go beyond that envisioned by the CCPA as enacted.

W265-4

Proposed § 999.315. Requests to Opt-Out

(c): The regulation provides that "*A business's methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out.*"

The terms "easy" and "minimal" are subjective standards that lack clarity because they can be reasonably and logically interpreted to have more than one meaning. We request that this requirement be removed from the regulation.

W265-5

(a)(d)(e)(g): The notion of using global privacy controls is inconsistent with CCPA law. The CCPA envisioned express opt-outs, but the proposed regulations impose a broad opt-out election that could remove the opt-out choice as it would apply to specific industries, uses, and companies, and

W265-6

would instead imply that a consumer wants it to apply universally. Insurers should not be lumped into publisher side digital advertising.

In addition to this inconsistency, it is unworkable. The proposed regulation seeks to impose a requirement, which from a technology standpoint, may not be feasible. The technology to track and honor such signals simply is not available. The proposal considers browser enabled privacy controls or plugins/cookies as do-not-sell requests coming from the consumer. The problem is that website operators generally do not know who the consumer is when browsing the site and may not be able to tie the opt-out request to a specific consumer. Recognition of the lack of readily available technology is one of the main reasons that a federal law was never passed mandating consumer choice relative to online behavioral advertising. Therefore, we request that the requirement be removed from the regulations. W265-6 (cont.)

Proposed § 999.317. Training; Record-Keeping

(2): The proposed modification sets an annual, July 1 deadline for updating response metrics in the privacy policy. Our previous comments raised serious concerns about the unnecessary and costly burden being imposed by the requirement to gather and post these metrics. The CCPA did not include any such requirement.

Adding a calendar deadline seems arbitrary and unnecessary so long as the company posts the metrics annually. To be clear, we continue to request that the record-keeping requirement be removed from the regulations, but at a minimum the calendar date should be deleted. W265-7

Proposed § 999.318. Requests to Access or Delete Household Information

This regulation prohibits complying with a request to know specific pieces of personal information about a household, unless all consumers of the household jointly request access, and the business individually verifies all members and their current status as a household member.

We are concerned that, for example, cookies or online tags used for tracking purposes may be associated with a household and there would be no harm to delete the information - in fact, this may be exactly what the consumer wants.

This provision would prohibit honoring the deletion request without verifying the identity of all household members, which may, as a practical matter, be impossible. Rather than making this an absolute prohibition, we request that the regulation be amended to allow it to be within the discretion of the business. In making this choice, the regulations could direct the business to give due consideration to the sensitivity of the personal information and risk of disclosure to unauthorized parties. W265-8

Proposed § 999.323. General Rules Regarding Verification

(d): This proposed regulation provides that "*A business shall not require the consumer to pay a fee for the verification of their request to know or request to delete.*" The example provided indicates that a business may not require a consumer to provide a notarized affidavit to verify their identity unless the business compensates the consumer for the cost of notarization.

This change is inconsistent with the CCPA because that law was not intended to ***decrease*** a business' ability to prevent of identity theft and fraud, yet the modified proposed regulation could W265-9

minimize use of an important tool – notarized affidavits – for a business to confirm an individual's identity before providing certain information could be meaningfully restricted. In fact, for the benefit and protection of consumers this practice should be explicitly permitted; therefore, we request the following amendment:

(d) A business shall not require the consumer to pay a fee for the verification of their request to know or request to delete. ~~For example~~ However, a business may ~~not~~ require a consumer to provide a notarized affidavit to verify their identity ~~unless the business compensates the consumer for the cost of notarization~~.

W265-9 (cont.)

Financial services including insurers, based on the information, may be more sensitive to validating before releasing information than other industries. Therefore, the need to notarize a form may arise more often. In some cases, such as when the individual does not have an account or has insufficient information on hand, securing a notarized document may be the only realistic way to verify an identity of the requestor. Requiring reimbursement/compensation, may negatively impact the feasibility of this option and create tremendous operational challenges. Given the importance of notarization as a verification tool, it is important that the regulation not be overly burdensome and restrictive with regard to ability to use it.

Proposed § 999.336. Discriminatory Practices

(g): The regulation provides that "*A price or service difference that is the direct result of compliance with federal law shall not be considered discriminatory.*"

Consistent with the intent of this section, it would make sense to include state laws. Therefore, we request the proposed regulation be amended as follows:

W265-10

*"A price or service difference that is the direct result of compliance with federal **or state** law shall not be considered discriminatory."*

Conclusion

As noted in our previous letter, per the "Notice of Proposed Rulemaking Action", Government Code section 11346.5, subdivision (a)(3)(D) requires the Attorney General to evaluate whether the proposed regulations are inconsistent or incompatible with existing state regulations. After conducting a review for any regulations that would relate to or affect this area, the Attorney General concluded that these are the only regulations that concern the CCPA. "The Attorney General has determined these proposed regulations are not inconsistent or incompatible with any existing state regulations, because there are no existing regulations that address the specific subject matter of the proposed regulations."

W265-11

We believe this assertion is factually inaccurate. For insurers, the California Department of Insurance (CDI) is charged with protecting insurance consumers and currently and fully regulates the insurance business, specifically including the implementation and enforcement of the Insurance Information and Privacy Act [CA Insurance Code Section 791] and the market conduct practices of insurers doing business in California.

The challenge with multiple regulators promulgating regulations, examining conduct and taking enforcement action is significant. A more effective and efficient solution is to charge regulators that already oversee industries with the enforcement of the rules relating to that industry, in this case the CDI over the insurance industry. The CDI has staff expertise in insurance and privacy, and

procedures for examining insurer conduct and handling consumer complaints in place. Therefore, we strongly recommend that the Attorney General defer to the CDI regarding investigation (market conduct) and/or enforcement of the CCPA.

W265-11 (cont.)

We appreciate the Attorney General's willingness to work with stakeholders, but it is clear that much more work needs to be done to develop fair regulations that can be implemented in a manner that best serves Californians. We look forward to continued work on these important regulations.

Sincerely,

Seren Taylor
Senior Legislative Advocate

From:	Rachel Nemeth
To:	Privacy Regulations
Subject:	CTA comments on Revised CCPA Proposed Regulations
Date:	Tuesday, February 25, 2020 1:44:31 PM
Attachments:	CTA Letter on Revised CCPA Proposed Regulations 2.25.2020.pdf

Good afternoon,

See attached for comments from Consumer Technology Association (CTA).

Thank you,
Rachel

Rachel Sanford Nemeth
Director, Regulatory Affairs
Consumer Technology Association, producer of CES®
d: [redacted]
m: [redacted]
CTA.tech | CES.tech

Consumer Technology Association™

1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

February 25, 2020

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

Dear Ms. Kim:

Consumer Technology Association® ("CTA")®[1] submits this letter commenting on the proposed California Consumer Privacy Act ("CCPA")[2] regulations, as revised by the California Department of Justice ("Department") earlier this month.[3] As CTA explained in prior comments to the Department, since the CCPA was signed into law, companies of all sizes have raced to establish processes, policies, and systems to come into compliance.[4] For many companies, building CCPA-compliant programs already has been a significant, challenging, and expensive initiative. To that end, CTA appreciates that the Department incorporated stakeholder feedback in a number of provisions. These changes reduce some of the confusion regarding businesses' regulatory requirements.

In particular, CTA supports the clarification in section 999.302 that whether or not information is "personal information" depends on if the business maintains it in a manner that "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." This modification, including its example of IP addresses, is particularly helpful for companies that have been confused about their obligations when they collect only limited information through their websites. In addition, CTA appreciates the clarification in section 999.314(c) that service providers can use personal information obtained from a business to improve the quality of their services and products without triggering a "sale."[5] W266-1 W266-2

CTA believes, however, that additional changes still are needed. These include the following:

- ***Section 999.307(b) – Notice of Financial Incentive.*** CTA explained in initial comments that companies have no practical way to estimate the value of an individual consumer's data, regardless of whether they provide a financial incentive that relates to the use of W266-3

[1] As North America's largest technology trade association, CTA® *is* the tech sector. Our members are the world's leading innovators – from startups to global brands – helping support more than 18 million American jobs. CTA owns and produces CES® – the largest, most influential tech event on the planet.
[2] Cal Civ. Code § 1798.100 *et. seq.*
[3] *See* California Department of Justice, Updated Notice of Modifications to Text of Proposed Regulations and Addition of Documents and Information to Rulemaking File, OAL File No. 2019-1001-05 (Feb. 10, 2020).
[4] *See* Comments of Consumer Technology Association on Proposed Adoption of California Consumer Privacy Act Regulations (filed Dec. 6, 2019) ("CTA Comments").
[5] However, as described below, CTA believes at least one additional change is needed to section 999.314(c).

such data.[6] Indeed, financial incentive programs can be based on complex calculations of costs to the business and market comparisons, rather than any sort of direct correlation to value acquired by the business in the exchange of data.[7] CTA accordingly continues to believe the Department should strike the requirement in subsection (b)(5) to include a good-faith estimate of the value of the consumer's data, in addition to the new requirement in subsection (b)(2) to include as a material term "the value of the consumer's data."[8]

W266-3 (cont.)

- ***Section 999.308(c)(1)(e)(2) – Disclosures in Privacy Policies About Categories of Data Disclosed to Third Parties.*** As revised, the regulations would require that businesses disclose in their privacy policies "[f]or each category of personal information identified," the categories of third parties to whom the information was disclosed or sold. For businesses with complex data flows to third parties, this requirement will be overly burdensome and will lead to more complicated and less consumer-friendly privacy policies.[9]

W266-4

- ***Section 999.313(d)(6) – Response to Denied Deletion Request and Treatment of Retained Personal Information***. In initial comments, CTA explained that section 999.313(d)(6) presents unnecessary operational challenges.[10] While CTA appreciates the intent behind the changes in section 999.313(d)(6)(a), the requirement still does not work in practice: A business that does not provide a specific basis for a denial because of a legal restriction would effectively be revealing to the consumer that such a restriction exists. Moreover, individualized responses significantly slow down the speed with which businesses can process and respond to consumers' deletion requests. The better approach is to allow businesses to be more general in their explanations about the reason a request may have been denied.

W266-5

CTA also is concerned about section 999.313(d)(6)(c), which prohibits the use of personal information that is retained under a deletion exception "for any other purpose than provided for by that exception."[11] The restrictive nature of this requirement appears to conflict with the much more permissive approach in several of the CCPA's deletion exceptions.[12] To eliminate any confusion, the regulations should instead make

W266-6

[6] CTA Comments at 5-6. CTA noted further that such "good faith" estimates would only confuse consumers rather than provide them with any additional helpful information. *Id.* at 6.

[7] Moreover, the value of the data to the business typically is derived by the business aggregating the data – there is little value to the business based on data of any single individual or household.

[8] For the same reasons, CTA believes the Department should strike in its entirety section 999.337 regarding calculating the value of consumer data.

[9] *See* CTA Comments at 3.

[10] *Id.* at 7-8.

[11] As an initial matter, more than one deletion exception may apply, which does not appear to be contemplated in the proposed regulations.

[12] Cal. Civ. Code § 1798.105(d)(7) ("To enable solely internal uses that are *reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business*.") (emphasis added); *id.* § 1798.105(d)(9) ("Otherwise use the consumer's personal information, internally, *in a lawful manner that is compatible with the context in which the consumer provided the information*.") (emphasis added).

clear that retained personal information can continue to be used for purposes that are consistent with any applicable exceptions. W266-6 (cont.)

- ***Section 999.314(c)(3) – Service Provider Use of Personal Information to Build or Improve Its Services.*** As noted above, CTA in general appreciates the clarification in section 999.314(c)(3) that service providers can use personal information obtained from a business to improve the quality of their services and products without triggering a "sale." The draft regulation, however, would prohibit service providers from doing so if they are "cleaning or augmenting data acquired from another source." The terms "cleaning" and "augmenting" never appear in the CCPA, nor do they have a common understanding in the industry. This clause is likely to generate significant confusion and lead to inconsistent application, and therefore should be removed. W266-7

- ***Section 999.315(d) – Requests to Opt Out through User-Enabled Privacy Controls***. CTA remains concerned that the regulations would require businesses to respond to global opt-out mechanisms and signals that do not currently exist, let alone in any standardized or uniform way.[13] Without consistency, a legal requirement to respond to such "global privacy controls" creates an unworkable situation for implementers to operationalize. The requirement also could distort the marketplace. W266-8

- ***Section 999.317(b) – Records of Consumer Requests.*** CTA continues to believe that a requirement to maintain records of consumer requests for 24 months is unnecessarily long and inconsistent with the CCPA's typical 12-month timeframe for many of its requirements.[14] The change in section 999.317(b) adding a reasonable security requirement for such records underscores the problem with the timeframe – businesses may be forced to keep this information longer than they otherwise would under their data minimization and security policies. W266-9

- ***Section 999.317(g) – Requirement to Publicly Disclose Statistics on Consumer Requests.*** Although CTA appreciates that the Department raised the threshold for this requirement, it is still far from clear that the statistics would yield any useful information. Indeed, the data could be misleading.[15] Accordingly, this requirement, which has no basis in the CCPA itself, is unnecessary at best and counterproductive at worst. It should be eliminated. W266-10

- ***Section 999.323(b)(3) – Factors to Consider in Determining the Method by Which a Business Will Verify a Consumer's Identify***. As drafted, the requirement indicates that verification mechanisms must be customized for each consumer based on the type, sensitivity, and value of the personal information collected and maintained about that particular consumer. As CTA explained in initial comments, it is impractical for many companies to customize their verification mechanisms on a consumer-by-consumer and W266-11

[13] CTA Comments at 11. One only needs to look at the failed experience with Do Not Track to understand the challenges in developing such mechanisms.
[14] *Id.* at 14-15 (citing Cal. Civ. Code § 1798.130(2) as one example).
[15] *Id. at* 15-16.

request-by-request basis.[16] Instead, the regulations should simply require that businesses employ a reasonable, risk-based verification method. W266-11 (cont.)

- ***Section 999.330(a) – Parental Consent.*** CTA supports the change clarifying that the requirement to obtain "affirmative authorization," separate and in addition to any verifiable parental consent required under the Children's Online Privacy Protection Act ("COPPA"), only applies where a business knows it is selling, rather than merely collecting and maintaining, children's personal information. CTA, however, still believes that the regulations should allow any mechanism that satisfies COPPA's verifiable parental consent requirement to also satisfy the CCPA's "affirmative authorization" requirement, avoiding a California-specific double opt-in.[17] W266-12

* * *

CTA appreciates that the Department has seriously considered stakeholder feedback. Its willingness to make changes to the regulations, thus far, show a genuine willingness to work with stakeholders. CTA believes, however, that the additional changes described above remain necessary to ensure that businesses, especially startups and other small businesses, can reasonably implement processes and procedures to comply with the CCPA and the regulations as ultimately adopted.

Sincerely,

/s/ Michael Petricone
Michael Petricone
Sr. VP, Government and Regulatory Affairs

/s/ Rachel Nemeth
Rachel Nemeth
Director, Regulatory Affairs

[16] *Id.* at 12-13.
[17] *Id.* at 13-14.

From:	Shanahan, Richard
To:	Privacy Regulations
Cc:	Mizoguchi, Kenichiro
Subject:	OAL File No. 2019-1001-05: CCPA Modifications
Date:	Tuesday, February 25, 2020 1:39:31 PM
Attachments:	image001.png 02242020_CCPA AG Comments.pdf

Ms. Kim,

Please find attached comments from Hitachi Group Companies regarding modifications to the daft regulations to implement the California Consumer Privacy Act. We appreciate the Attorney General's Office continuing to work with industry to create meaningful and appropriate implementation regulations for this law.

Best regards,

Richard Shanahan
Manager | Government & External Relations
Hitachi, Ltd. | Washington, DC Corporate Office
t. [redacted] | m. [redacted]

Follow Us
www.hitachi.us/gov-relations

HITACHI
Inspire the Next

HITACHI
Inspire the Next

February 25, 2020

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

RE: ***Notice of Proposed Rulemaking Action Concerning California Consumer Privacy Act (CCPA)***

Dear Attorney General Becerra:

The following comments are submitted by Hitachi Group companies ("Hitachi") doing business in the United States in connection with the Notice of Proposed Rulemaking Action (NOPA) *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).*

Hitachi appreciates the modified regulations published by the California Department of Justice and commends the Attorney General ("AG") for continuing to gather information to increase clarity around the compliance and enforcement of CCPA. Privacy standards should be fair, equitable, and protect the public while also fostering innovation in the State of California and across the country.

Responses to Modified Regulations

New Section 999.302: Guidance Regarding the Interpretation of CCPA Definitions
Hitachi appreciates this new section and its attempts to address businesses' use of cookies to assess web traffic to their websites. As noted in our December 2019 comments, global companies frequently have corporate websites that gather incidental information on those visiting and do not sell the data collected. The scope of information in this new section does appear to try and alleviate some concerns global companies may have in this area, creating the exemption if the business cannot reasonably link an individual IP address to a particular consumer or household. W267-1

To make this section even stronger, the AG's office should issue guidance on the "reasonable" standard in this section. Establishing what is "reasonable" is key to helping businesses understand and comply with the standard. It would be wise for the AG's office to create objective criteria applicable to any company doing business in California. When an objective standard is created, it also provides clarity to consumers and can enhance individual privacy protections. When the regulations are clear, consumers have a better understanding of how their data is being used or not used, which empowers them to make better informed decisions about what they want shared or protected.

Business Threshold Requirements (Civil Code Section 1798.140, subdivision (c))
Our previous comments noted that there needs to be clarification on the business threshold requirements. It is unclear if the AG's office is using a $25M gross revenues standard from just California sales, from California consumers, or worldwide. The modified regulations fail to address this major regulatory issue and the AG's office should ensure this is crystal clear. W267-2

The new regulations do clarify the minimum of 10,000,000 consumers in 999.317(g) by providing a timeframe of the previous calendar year. That is an example of creating certainty for businesses.

Treatment of Households (Civil Code section 1798.140, subdivision (o))

Our December 2019 comments also requested more clarification around the "household" definition. We note that 999.301(k) seeks to provide more information on how the CCPA views a household by clarifying "household" to mean people residing at the same address, sharing common devices or same services, and identified by a shared group account or unique identifier. By noting the business shall not comply with requests to know specific pieces of personal information about the household, or requests to delete information, the definition gives businesses some guidance and allows the business to protect the privacy of household members. It further helps a business understand that no one person necessarily holds all the rights of the household or can act on behalf of a household.

While that is helpful, there are still questions as to how a business applies this definition when applying the various rights CCPA confers on consumers. In 999.318(a), the AG's office provides a series of conditions that must be satisfied in order to delete household data. While this is helpful, it could lead to unsatisfactory results for the consumer. It is possible the business does not have enough information to individually verify all members of the household and may have no way to verify that each person is currently a member of the household. This would result in denial of the request to delete household information. Section 999.318(b) recognition of password-protected account access is useful for those circumstances. W267-3

The regulations still do not offer enough clarity on who is assigned personal data rights to shared devices. Is the modification intending to tell businesses that the data is collectively owned? If that is the case, when a business determines the value of data, does it do so for the household, or is it determining the value for each individual in the household, and how does a business that does not have an on-going relationship with the household know how many people are in that household to determine the value of the data collected?

The modifications are an improvement, but the final regulations should continue to clarify the ambiguity around "household."

Verification of Requests

Article 4 lays out various considerations businesses can take into account when verifying a request to "Know, Delete, Opt-Out, and Opt-In After Opting-Out." The regulations' section 999.313(c)(3) now create a listing of conditions that must be met before a business is required to conduct a search for the information. That is a helpful improvement to the previous version of the regulations and is appreciated. W267-4

Missing from the modified regulations, however, is clarity around the use of "reasonable method" standards. As noted in our previous comments, the AG's office needs to specifically recognize safe harbors for businesses who use risk-based verification methods that generally conform to the standards outlined in Article 4. We continue to be worried that small businesses will be particularly harmed by the lack of safe harbor provisions when they apply a standard that is reasonable for their resources, but are not given assurance that their definition of "reasonable method" conforms with the State's definition. The AG's office would be wise to recognize a business's resources and capabilities when determining if the business has created a reasonable standard for verification. W267-7

We continue to recommend the creation of a guidance document that favors a risk-based verification process that also takes into account the sensitivity of the data that is being processed. The regulations could then cite adherence to the guidance document as part of a test to create a safe harbor provision for businesses under this verification title. This would allow some flexibility as technology and security advances and would give businesses certainty to liability under the title.

Service Provider

We appreciate the updates to the service providers section, specifically 999.314(c). The revision appropriately recognizes the benefits service providers can create for consumers and their customers when data is used for internal improvements of quality and services. We appreciate that recognition and the further guidance provided in 999.314(c)(3). W267-5

Business Outside of CA

We noted in our original comments that California Civil Code 1798.145(a)(6) states that the statue will not restrict a business' ability to "collect or sell a consumers personal information if every aspect of that commercial conduct takes place wholly outside of California" and the clarifying language stating "commercial conduct takes place wholly outside California if the business collected that information while the consumer was outside California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold." The modified regulations, however, do not address the complexity as to exactly when a potential consumer was physically in the state. We noted that provisions such as this could create a chilling effect on innovation in California if businesses determine it is better to conduct research outside the state to avoid CCPA regulations and/or if a business determines it is better to deny citizens of the state access to new innovations due to regulatory compliance. Final regulations must address this issue. W267-6

Conclusion

Hitachi lauds the AG's efforts and looks forward to continuing to work with the State of California as CCPA takes effect.

Sincerely,

Toshiaki Tokunaga

Toshiaki Tokunaga
Chairman of the Board
Hitachi Vantara LLC

Background on Hitachi

Founded in 1910 and headquartered in Tokyo, Japan, Hitachi, Ltd. is a global technology conglomerate answering society's most pressing challenges through cutting-edge operational technology (OT), information technology (IT), and products/systems. A Social Innovation leader, Hitachi delivers advanced technology solutions in the mobility, human life, industry, energy, and IT sectors. The company's consolidated revenues for FY2018 (ended March 31, 2019) totaled $86.2 billion, and its 803 companies employ 295,000+ employees worldwide.

Since establishing a regional subsidiary in the United States in 1959, Hitachi has been a committed American partner. For over thirty years, it has invested heavily in research and development (R&D) in the U.S., and this continued reinvestment has resulted in 11 major R&D centers that support high-skilled jobs in manufacturing and technology. Dedicated to delivering the technologies of tomorrow, Hitachi recently opened a Center for Innovation in Santa Clara, California to explore applications in machine learning, artificial intelligence, Internet of Things (IoT) devices, data analytics, and autonomous vehicles among other advanced technologies. Hitachi is also proud of its human capital investment, supporting 21,000 employees across 88 companies in North America. At 13% of total revenue, North America is Hitachi, Ltd.'s second largest market, generating $10.9 billion in revenue in FY2018.

From: Matt Kownacki
To: Privacy Regulations
Subject: AFSA comments on revised CCPA regs
Date: Tuesday, February 25, 2020 1:37:05 PM
Attachments: AFSA comment letter - CCPA revised regs .pdf

Ms. Kim,

Attached are comments from the American Financial Services Association regarding the most recent revision of the proposed CCPA regulations.

Please let me know if you have any questions.

Thank you,
Matt Kownacki

Matt Kownacki
Director, State Research and Policy
American Financial Services Association
[redacted]

February 25, 2020

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

Re: CCPA revised proposed regulations

Dear Ms. Kim:

On behalf of the American Financial Services Association ("AFSA"),[1] thank you for the opportunity to provide comments on the Office of the Attorney General's ("OAG") revised regulations to implement the California Consumer Privacy Act ("CCPA"). We also appreciate your consideration of our comments regarding the previous version of the proposed regulation and the significant changes reflected in the revised proposal.

AFSA members share the state's goal of protecting the privacy of consumers, promoting understanding by consumers of the personal information about them that is collected, sold, and shared for a business purpose, and guarding personal information from unauthorized access. While the revised proposal does include positive changes that address concerns we raised in our previous comments, we believe the revisions did not go far enough and reiterate our previous concerns about vague terms, requirements that lack basis in the underlying statute, and the substantial burdens these regulations place on covered entities.

§ 999.317. Training; Record-keeping

Section 999.317(e) stipulates that information maintained for record-keeping generally may not be used for any purpose except as necessary for compliance with the CCPA and that it may not be shared with any third party. As there are situations in which it may be necessary to share such information to comply with legal obligations other than just those in the CCPA, we suggest revising 999.317(e). to read:

W268-1

> 999.317(e) Information maintained for record-keeping purposes shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and these regulations. Information maintained for record-keeping purposes shall not be shared with any third party except to comply with a legal obligation.

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

We believe this change would be consistent with the statute, specifically Section 1798.105(d)(8) of the CCPA. W268-1 (cont.)

Enforcement Delay

Although the effective date and issues of enforcement are not addressed directly in the revised regulations, we continue to believe that clarity in this area is warranted. The CCPA was largely effective on September 23, 2018, and operative on January 1, 2020, and it will be enforceable by the OAG on July 1, 2020. We appreciate the OAG's clear commitment to draft comprehensive regulations that reflect the significant volume of feedback received throughout the process. Recognizing that such a process takes time, it is not clear that final regulations could be made effective and enforceable by July 1, 2020. Accordingly, we request a delayed enforcement date, which would give affected businesses the opportunity to evaluate the specific requirements set forth in the regulations and implement the new systems and processes needed to be fully in compliance with the law. W268-2

In addition, we request that the OAG include in the final regulations a statement to the effect that any enforcement actions will be based on conduct that takes place after the statutory enforcement date of July 1, 2020, or such later date as the regulations may become enforceable. In making this request, we note that the proposed regulations address all the major aspects of the CCPA: how to provide notices, content of the privacy policy, the process for handling submitted requests, verification, and calculating the value of consumer data. While businesses continue to take steps to meet regulatory requirements, without having final regulations in place to govern compliance, businesses lack clarity that the solutions they are readying will, in fact, meet the final regulatory requirements. We request that businesses have all the applicable rules and requirements, in final form, with a reasonable timeframe to achieve compliance, before their actions can be determined to be unlawful. When drafting the CCPA, the legislature recognized the need for delayed enforcement to ensure businesses have to adequate time to comply with regulations, and we believe that the outlined enforcement delay would be consistent with the legislature's intent. W268-3

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

Sincerely,

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

From: Chris Pedigo
To: Privacy Regulations
Subject: CCPA Comments from DCN
Date: Tuesday, February 25, 2020 1:33:51 PM
Attachments: DCN Comments re CA AG Revised CCPA Regulations - 2020-02-24 Final.pdf

---

To Whom It May Concern –

Please find the attached comments from Digital Content Next regarding the proposed regulations for the California Consumer Privacy Act. Please let me know if you have any questions about these comments or would like the comments delivered in a different format.

Sincerely,

--
Chris Pedigo
SVP, Government Affairs
Digital Content Next
[redacted]

Follow us on Twitter: @DCNorg
Sign up for our weekly newsletter, InContext, for insights in digital media.

February 24, 2019

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

RE: California Consumer Privacy Act Regulations

Dear Attorney General,

We appreciate the opportunity to comment on the regulations proposed by your office to implement the California Consumer Privacy Act (CCPA). Founded in 2001 as the Online Publishers Association, Digital Content Next (DCN) is the only trade organization in the U.S. dedicated to serving the unique and diverse needs of high-quality digital content companies which enjoy trusted, direct relationships with consumers and marketers. DCN's [1]members are some of the most trusted and well-respected media brands that, together, have an audience of 256,277,000 unique visitors or 100 percent reach of the U.S. online population[2]. In layman's terms, every person in the U.S. who goes online will visit one of our member companies' websites at least one time each month.

Personal Information

We support the clarifying language that information is not considered personal information for purposes of the CCPA as long as it cannot be linked or reasonably linked to a consumer. However, while the indication that IP addresses, for example, can be out of scope if they are used in a sufficiently limited fashion is a step in the right direction, we are concerned that the current language could be misinterpreted by ad tech groups to support broader profiling and data sale activities in connection with behaviorally-targeted advertising than intended under the CCPA. For example, an ad tech company might argue that none of the information it holds is personal information under the CCPA as it cannot identify the name of the consumer. We suggest that this section be clarified to indicate that any use of such information to identify, even if pseudonymously, a consumer ensures that it is still personal information. W269-1

[1] https://digitalcontentnext.org/wp-content/uploads/2019/11/DCN-letter-to-CA-AG-2019-11-07.pdf

[2] *comScore Media Metrix Multi-Platform (Desktop P2+ and Mobile P18+) Audience Duplication Report*, December 2018, U.S.

Methods for Requests to Know

We support the clarifying language which allows for "exclusively online" businesses to only offer an email address for the submission of requests to know. In many cases, mandating a second method would be awkward for consumers and would necessitate the collection of additional personal information. W269-2

Verification of Consumer Identity

We support the addition of language that a business may deny a consumer request if the business cannot verify the identity of the consumer. Verification requires reasonable action by the consumer to confirm or provide additional information. Some consumers may start the process but never finish it for a myriad of reasons. However, we are concerned that the 45-day timeframe starts when the consumer submits the initial request. It would be unreasonable to require that a business comply with a request if the consumer verified their identity on day 44. We suggest providing reasonable flexibility for businesses by starting the 45-day clock after the consumer's identity has been verified. W269-3

Responding to Requests to Know

We have concerns about the modified requirements for responding to requests to know. The new provisions replaced the restriction barring businesses from providing 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. As this provision protects consumers, we would like to ask to reinsert it.

With regard to the new provisions in Section 999.313 (c)(3), there is a new four-part test whereby a business is not required to search for personal information if all the following conditions are met: W269-4

a. The business does not maintain the personal information in a searchable or reasonably accessible format:
b. The business maintains the personal information solely for legal or compliance purposes;
c. The business does not sell the personal information and does not use it for any commercial purpose; and
d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions states above.

Our primary concern is that these conditions do not include a scenario where a business does not store data in a manner that is linkable to a specific individual. Under this four-part test, it appears that a business, which would otherwise store data in aggregate, would need to start storing data in ways that link to an individual. We are also concerned that the four-part test might be an impossible hurdle to clear. A and B appear to contradict each other. For example, a business that maintains information for "legal or compliance purposes" (test b) would likely maintain that information in what could be considered a "reasonably accessible format (test a)."

Global Privacy Settings

We appreciate the additional clarity in Section 999.315 (d) (1) with regard to the development and communication of global privacy settings. We are concerned, however, about the requirements of Section 999.315 (d) (2) which seems to imply that a consumer's global privacy setting would override any express, affirmative consent that a consumer gave to a business. We suggest allowing for a business-specific setting to override a global setting if the business setting is not for tracking or use across the web or outside of the business' relationship with the consumer. In addition, under this provision, a business would need to notify the consumer if the global setting conflicts with an "existing business-specific privacy setting" *every time the consumer visits the site or app.* Notifying the consumer of this conflict every time they visit the site or app is likely to frustrate the consumer who expects a business to remember their preferences. We suggest adding flexibility for businesses to maintain a consumer's privacy settings especially if a business has gained express, affirmative consent or already confirmed the consumer's "existing business-specific privacy setting." W269-5

In addition, we are concerned that while the regulations provide for flexibility, they create uncertainty with respect to which signals a business will be required to respond to. For example, certain privacy controls by design do not store information in the consumer's browser, which means businesses would not be able to read or receive a signal regarding the consumer's choice. It is not clear whether the current standards exclude such mechanisms, which are technically impossible to respond to. As such, it would be helpful to provide additional clarity by requiring that any such privacy control utilizes a standard signal to broadcast a Do Not Sell choice from consumers. We have appreciated the examples included in the regulations and it would be helpful to include some additional examples to indicate which existing mechanisms meet the standards articulated in the regulations (or the ones that do not). Guidance on the following existing mechanisms would be appreciated: browsers' "Do Not Track" setting, iOS's "Limit Ad Tracking", and Android's "Opt out of Ads Personalization".

Requirement for a Landing Page

We are concerned that regulations require that a business must direct a consumer who want to activate their Do Not Sell right to a landing page with additional information. Upon clicking the "Do Not Sell My Personal Information", it is possible to opt the user out immediately, with no further ado. Instead, the draft regulations require that the user be shown an additional notice when clicking on the Do Not Sell link. Users who wish to read notices can find them in the footer of pages or in the privacy policy. Users who wish to opt out of the sale of their personal information may often want to do so and then go about their business. Forcing a notice upon them at that point deteriorates the user experience and renders the exercise of their rights more administrative and less straightforward. We therefore recommend that the draft regulations be amended such that, if the user is opted out simply upon clicking the link, there is no need to show the notice of opt-out at that point (though of course the notice would remain accessible through other means). W269-6

Just-in-Time Notices

A new requirement was included in the most recent version of the regulations such that when a business collects information from a consumer's mobile device for a purpose that "the consumer would not reasonably expect," it shall provide a just-in-time notice containing a W269-7

summary of the categories of personal information being collected and a link to the full Notice at Collection. The example of a just-in-time notice they use are pop-up windows. This is a significant change to an app's user experience that will require substantive time and resources to develop. If such a requirement remains, a delay should be provided in order to implement it properly. Also, we are concerned about the number of notices presented to consumers. A "just-in-time" notice would be the third notice during a single visit to the app, all being summary of the previous notices. W269-7 (cont.)

Service Providers

Section 999.314 (c) (3) appears to be more restrictive than the original definition of a Service Provider (which allows processing for all listed "business purpose[s]"). This new construct will therefore impact already agreed upon contracts with CCPA language. We ask that you allow businesses additional time to conform contracts to comply with this new section. W269-8

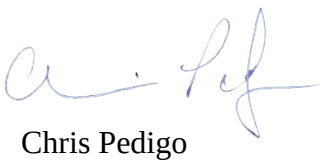
Also, we note that the definition of "service provider" in section 1798.140 (v) contradicts with subsection (2) of the definition of "third party." This contradiction is causing extensive negotiation with vendors who want to limit themselves to the definition of "service provider" and reject any addition contained in subsection (2) of the definition of "third party." It would be helpful if you could clarify in regulations how organizations can differentiate between service providers and third parties. W269-9

Conclusion

Thank you for the opportunity to comment on the proposed regulations regarding the CCPA. We applaud your thoughtful approach to the practical questions for implementing this important law. Please do not hesitate to reach out directly to us with any questions or comments.

Sincerely,

Jason Kint
CEO
Digital Content Next



Chris Pedigo
SVP, Government Affairs
Digital Content Next

From:	Kammerer, Susan
To:	Privacy Regulations
Cc:	Merz, Jeremy; Gleason, Angela
Subject:	APCIA Comments on CCPA
Date:	Tuesday, February 25, 2020 1:24:50 PM
Attachments:	20-2-25 CA CCPA Revised Regulations - APCIA Comments - Final.pdf

To Whom it May Concern:

Thank you for the opportunity to provide comments on the CCPA rulemaking process. Please see APCIA's attached comment letter.

Thank you,

Susan Kammerer
APCIA Western Region
1415 L Street, Suite 670
Sacramento, CA 95814
[redacted]

February 25, 2020

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

VIA Electronic Mail: PrivacyRegulations@doj.ca.gov

To Whom It May Concern:

The American Property Casualty Insurance Association (APCIA)[1] appreciates the opportunity to provide feedback on the revised California Consumer Privacy Act Regulations (revised regulations). The revised regulations contain improvements that will benefit consumers and businesses alike. For instance, the regulations take a more nuanced approach to some of the challenges presented by IP addresses, mobile applications, and verification procedures. There is also helpful training guidance. Consumer expectations are more accurately represented with regards to consent for material changes as well.

Nevertheless, significant challenges remain. This is particularly true for regulated industries, like insurance, where multiple versions of a single right may apply based on existing privacy obligations. Further, the revised regulations fail to address certain complexities and needlessly prescriptive requirements that will enhance consumer confusion and prohibit businesses from having the flexibility to make meaningful changes to practices and procedures based on evolving consumer perceptions and technologies.

The following comments are limited to concerns with the proposed revisions.

999.305 Notice at Collection of Personal Information

General Observations
The Attorney General's office should further reduce the number of situations in which notice is required at the point of collection. Multiple notices and policies can add to consumer confusion, redundancy, and

W270-1

[1] APCIA is the preeminent national insurance industry trade association, representing property and casualty insurers doing business locally, nationally, and globally. Representing nearly 60 percent of the U.S. property casualty insurance market, APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers. APCIA represents the broadest cross-section of home, auto, and business insurers of all sizes, structures, and regions of any national trade association.

notice fatigue rather than promoting meaningful consumer choice and transparency. Many aspects of the notice at collection could be included in the privacy notice, if they are not already. To this end, the regulations should make clear that a separate notice at collection is not required if a business chooses to provide or link to its full privacy policy as described in Section 999.308.

W270-1 (cont.)

Website Links

The clarifications in section 999.305(a)(3) would benefit from additional detail to add certainty that including a conspicuous link to the notice at collection on every webpage where personal information is collected is not mandatory. The only reference in the California Consumer Privacy Act (CCPA) to a conspicuous posting is in relation to the posting of a "Do Not Sell My Personal Information" link at Cal. Civ. Code 1798.135. Likewise, the CCPA only requires a broadly defined homepage posting for the "Do Not Sell My Personal Information" link. For all other disclosure obligations businesses have flexibility to determine its best placement taking into consideration the totality of information that must be presented to the consumer.

To be certain, clarity and consumer transparency are important, but this must be carefully balanced with all privacy and non-privacy related notification requirements. "Conspicuous" infers a mandatory prioritization and placing a "conspicuous" link on every page that collects personal information is extremely burdensome and will take up valuable space that should otherwise be utilized to include additional important and/or required service/product information. Busy webpages can also be discouraging and confusing to consumers misdirecting their focus from important details. APCIA believes the introductory webpage posting should be sufficient in many cases for the notice at collection and if every webpage where personal information is collected is necessary the business should be given the flexibility to decide the appropriate placement of that link.

W270-2

Recommendation:

999.305(a)(3)(a) - APCIA respectfully urges the Attorney General to eliminate the new addition of "conspicuous" to Section 999.305(a). Additionally, recognizing this is an illustrative example, we suggest including the options in this section as a list of alternatives to reinforce flexibility for businesses.

(3) The notice at collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information. Illustrative examples follow:

a. When a business collects consumers' personal information online it may post a ~~conspicuous~~ link to the notice on: (i) the introductory page of the business's website; (ii) all webpages where personal information is collected; ~~and~~ or (iii) the introductory page of the business's website and all webpages where personal information is collected.

Accessibility for Consumers with Disabilities

The regulation should not prioritize, and potentially mandate, utilization of specific standards, rather the owner of the website should be able to determine how to make its website reasonably accessible to those with disabilities. Identifying specific standards also prevents a company from leveraging new

W270-3

technologies. Importantly, given the broad scope of industries subject to the CCPA, it is difficult to identify a standard that will work for every industry, regardless of the standard developer's intent.

Recommendation:
999.305(a)(2)(d) - "Be reasonably accessible to consumers with disabilities~~. For notices provided~~ online. ~~, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Consortium, incorporated herein by reference.~~ In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format."

W270-3 (cont.)

Mobile Applications
Section 999.305(a)(3)(b) has been revised to clarify that an application's setting menu is "within the application." This is helpful and appreciated. However, for the reasons identified above, posting a link on the mobile application's download page and within the application should be separate examples rather than contingent requirements.

W270-4

Recommendation:
999.305(a)(3)(b). When a business collects personal information through a mobile application, it may provide a link to the notice on the mobile application's download page ~~and~~ or within the application, such as through the application's settings menu.

Telephonic Interactions
APCIA appreciates the inclusion of an example for telephonic interactions in Section 999.305(a)(3)(d). Unfortunately, we have significant concerns that the illustrative example places an unnecessary burden on consumers. Providing an oral version of a privacy policy would require consumers to listen to a complex legal notice. Whether they would absorb such an oral notice is doubtful. We anticipate frustration with no perceptible consumer benefit. In addition, there are scenarios where it is not only impractical, but impossible, to provide the consumer with the notice at collection orally, for example when the consumer leaves a voicemail message that includes personal information. APCIA recommends that a business should be permitted to refer individuals to the privacy policy.

W270-5

Recommendation:
999.305(a)(3)(d). When a business collects personal information over the telephone or in person, it may ~~provide the notice orally~~ direct the consumer to to the business's privacy policy.

Just-in-Time notice
In Section 999.305(a)(4), the revised regulations propose a new "just-in-time notice" for the collection of personal information from a consumer's mobile device for a purpose the consumer would not reasonably expect. As proposed, this revision raises several concerns. First, it imposes an obligation that is not contemplated by the statute. Cal. Civ. Code §1798.110 gives the consumer "**the right to request** information, it does not require automatic notification of the categories of personal information, which is required by this new regulatory section. Second, APCIA has significant concern with the complex and

W270-6

numerous notices that the regulation and statute require. This new section simply piles on to an already complex framework. Third, as a practical matter, meeting the disclosure obligations could be difficult to achieve given the screen size and character limits available. Finally, the subjective requirement to determine a consumer's expectations may not be as obvious as the flashlight example provided in the regulation and may be difficult or impossible to determine. This could result in stifling innovation that would be beneficial to the consumer. For example, usage-based insurance applications, in addition to tracking driving behavior for insurance rating purposes, add safety features such as crash detection, lock out assistance, or theft recovery services. The consumer may or may not "reasonably expect" these services but would not object to them. W270-6 (cont.)

For these reasons, APCIA recommends that this section should be eliminated, however, if it remains, it should be amended such that a link to the generally available privacy notice is sufficient.

Businesses that Do Not Collect Information Directly

The changes proposed to section 999.305(d) are a positive movement to reduce multiple and redundant consumer notices in a meaningful way. The revisions recognize that when multiple parties have access to consumer information, the party that does not collect the information directly from the consumer should not have to provide a notice at collection. Unfortunately, the revisions limit the scope of this change to data brokers registered with the Attorney General. APCIA urges the Attorney General to expand this exemption beyond data brokers, so long as the business includes instructions in the privacy policy on how to submit a request to opt-out. W270-7

Employee Notification

The regulation should reflect disclosure obligations that are current law and not memorialize language that may or may not be law in the future. Sections 999.305(e) and (f) should be deleted and revisited should the employee-related exemptions sunset on January 1, 2021. W270-8

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

Section 999.306(f) identifies an example of an opt-out button that businesses may use. The format may be confusing for consumers. Is the intent to slide the circle over the "x" to express a desire to opt-out? This would seem in-line with some smart phone operations, but it is unclear in the regulation. Additional language identifying this opt-out button as an "illustrative example" and clearly indicating it is not the only option or format of an opt-out button is welcome. W270-9

Responding to Requests to Know and Requests to Delete

The Attorney General's addition of "business days" as opposed to "calendar days" is welcome and appreciated. Nonetheless, consistent with our overarching concern with multiple notices, APCIA respectfully recommends deleting the need for a confirmation receipt. The CCPA and this regulation require detailed notice requirements in multiple forms and in multiple points along the consumer interaction process, adding this additional notice 10 days into a request when the consumer already knows the process that is going to take place after their request (see the detailed CCPA privacy statement) seems overly burdensome to businesses trying to comply in what is already a short 45 days. Additionally, this provides no value to the consumer other than additional interaction with a business that they likely do not want. W270-10

Responding to Requests to Delete

The new obligation in revised section 999.313(d)(1) to give an unverified requestor the right to opt out of the sale of their personal information is as problematic as the automatic opt-out this new language is intended to replace. If an unverified consumer opts out, the business must either honor the request even though it cannot verify the request or deny the request. Pursuant to Section 999.315(h) a denial would require a good-faith, reasonable, and documented belief that the request to opt-out is fraudulent. On the spot, the business representative may not have enough information on which to form an opinion.

The interest of consumers is poorly served by this provision. For instance, if an ex-spouse tries to request deletion of a current consumer's data, but his/her request cannot be verified, then, in practice, you are still giving the ex-spouse the authority to opt the current consumer out of everything. This remains contrary to the individual control rights that the CCPA advocates for. W270-11

APCIA recommends that the new sentence at the end of 999.313(d)(1) should be deleted as follows:

> "For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulation 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. ~~if the business sells personal information and the consumer has not already made a request to opt out, the business shall ask the consumer if they would like to opt out of the sale of their personal information and shall include either the contents of, or a link to, the notice of right to opt out in accordance with Section 999.306~~."

APCIA is unclear as to the intent of changing "personal information" to "consumer information" in Section 999.313(d)(2)(c). This change is inconsistent with the language used throughout the regulation. In fact, the only other place that the term "consumer information" is used is in Section 999.323 where the context makes it clear that consumer information is deidentified personal information. Deidentified data in this context does not make sense. W270-12

Additionally, the revisions to Section 999.313(d)(3) indicate that a business can delay compliance with a request to delete data stored on the archived or back-up system until the data is restored to an active system or next accessed or used for sale, disclosure, or commercial purpose. This section would benefit from additional clarification to provide a reasonable expectation within which the request would have to be fulfilled after the data is restored. Instantaneous compliance would be very difficult, if not impossible, to achieve, therefore, we recommend the following: ". . . may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is ~~restored to an active system or~~ next accessed or used for a sale, disclosure, or commercial purpose or within a reasonable period of time, not to exceed 1 year, that data is restored to an active system." W270-13

Service Providers

The revised regulations make some improvements to the service provider obligations. However, of concern, the revised regulations restrict service provider retention, use or disclosure of personal information except for a list of enumerated purposes identified in the regulation. This restriction seems W270-14

narrower than the CCPA section 1798.140 definition which permits the service provider to retain, use or disclose personal information "as otherwise permitted by this title." This revised section should align with the statutory requirements. W270-14 (cont.)

Additionally, the change from "person or entity" to "second business" perpetuates confusion rather than clarity because "business" within the statute and regulation means an entity that is subject to the CCPA. Is the regulation now implying that an entity must be a "business" (i.e. subject to the CCPA) in order to be a service provider? W270-15

Requests to Opt-Out

Subsection (c) of Section 999.315 requires that the method for submitting a request to opt-out should be "easy" and "require minimal steps." These are subjective standards and will create opportunities for consumers to frivolously challenge a business's opt-out practices. W270-16

Training and Record-Keeping

Prohibition on Sharing Record Keeping Information with Third Parties

As drafted the revised regulations prohibit sharing information maintained for record-keeping purposes with third parties. This new language is unnecessarily restrictive and does not recognize the need to share information with third parties, such as for an outsourced data center, or as part of a legal obligation. We recommend deletion of the last sentence in section 999.317(e). Alternatively, this sentence should be amended as follows: "Information maintained for record-keeping purposes shall not be shared with any third party, except as required or permitted by law or to comply with legal obligations or investigations." W270-17

Metrics (Section 999.317(g)

APCIA continues to have concerns with and questions the need to post metrics related to the number of requests received and complied with in whole or in part, and denied. This information will only add length and complexity to privacy notices while providing consumers no discernable benefit. Moreover, the notices will lead to unfair assessments of businesses based on incomplete details. This is particularly true for regulated industries, such as insurance, where GLBA-regulated data is exempt from most CCPA requirements for good reason. W270-18

Also, the revised regulations now establish an arbitrary annual compliance deadline of July 1. There is no need for a set timeframe for posting the metrics, so long as the company posts them annually. For this reason, if the reporting requirements are retained, we respectfully recommend "by July 1 of each calendar year" be deleted. W270-19

Requests to Access or Delete Household Information

Section 999.318 prohibits businesses from complying with a request to know specific pieces of personal information about a household, unless all consumers of the household jointly request access, and the business individually verifies all members and their current status as a household member. APCIA has concerns that cookies or online tags used for tracking purposes may be associated with a household (i.e. a smart TV, tablet and mobile phone) and there would be no harm to delete the information, which may be exactly what the consumer wants. Ultimately, the revised regulation sets up a verification requirement that may be impossible to meet. As such, rather than making this an absolute prohibition, the regulations W270-20

should leave this determination to the discretion of the business. The regulations could achieve this by including language that "a business may choose not to comply" and direct businesses to give due consideration to the sensitivity of the personal information and risk of disclosure to unauthorized parties. W270-20 (cont.)

General Rules Regarding Verification

The revised regulations contain an express prohibition against "requiring" a consumer to pay a fee for verification of their request to know or delete. Such a strict prohibition could be misused by the consumer. For example, Section 999.326(c) allows a business to require proof of authorization from the authorized agent. If the authorized agent charges a fee to the consumer to submit proof to the business, the consumer can contend that this fee violates Section 999.323(d) and must be paid for by the business or the business forego proof. This establishes third-party billing hazards, in which any expense by the consumer can be an expense to the business. In addition, existing California law, the Insurance Information and Privacy Protection Act (Ins. Code Sec. 791.08(d)) allows an insurance institution to charge a reasonable fee to cover the costs incurred in providing a copy of recorded personal information to individuals. While insurance information is exempt under CCPA, the dual standard (for companies that charge a fee) will not be well received by consumers. W270-21

The regulations still do not provide any information related to the process for verifying authorized agents. The burden to validate authorized agents is that of the Secretary of State. Yet, there is no clarity as to how a business is to verify this validation. Will the Secretary of State post a list on their website and if so, when can businesses expect to see that information? W270-22

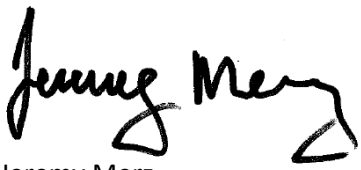
Technical Errors

Section 999.315(d)(1) should be amended to read "intends to ~~the~~ opt-out of the sale…" APCIA also noticed there were discrepancies between the red-line and clean versions of the revised regulation that the Attorney General may want to reconcile. W270-23

***

APCIA appreciates the opportunity to provide feedback. Please, let us know if you have any questions or would like additional information.

Respectfully submitted,



Jeremy Merz
Vice President State Affairs, Western Region
American Property Casualty Insurance Association
1415 L Street, Suite 670, Sacramento, CA 95814
P: [redacted] | [redacted]

From: Steve Denis
To: Privacy Regulations
Subject: File No.: Second Invitation for Comments on California Consumer Privacy Act Regulations Proposed Text of Regulations ("Invitation")
Date: Tuesday, February 25, 2020 1:20:15 PM
Attachments: CCPA AG Comment Letter SBFA - SecondInvitation.docx

Submitted by Electronic mail to: PrivacyRegulations@doj.ca.gov

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

Re: File No.: Second Invitation for Comments on California Consumer Privacy Act Regulations Proposed Text of Regulations ("Invitation")

Dear Attorney General Xavier Becerra,

The Small Business Finance Association ("SBFA") would like to thank the Office of the Attorney General ("AG") for one again reaching out to stakeholders and inviting them to provide input on the above referenced edits to the proposed regulations.

We appreciate the AG taking into consideration stakeholder comments in order to make edits to the proposed Regulations for the California Consumer Privacy Act ("CCPA"). While the SBFA understands the importance of protecting customer data and wants to insure that its customer data is protected and appreciate some changes that were made, we would appreciate additional changes, clarity and guidance in order to insure that SBFA member companies are able to comply with CCPA as well as continue to operate their business in an effective manner. The below comments are in response to the most recently proposed edits to the Regulations; however, we would still request that our previous comments be considered.

I. INTRODUCTION

The Small Business Finance Association (SBFA) is a non-profit advocacy organization dedicated to ensuring Main Street small businesses have access to the capital they need to grow and strengthen the economy. SBFA's mission is to educate policymakers and regulators about the technology-driven platforms emerging in the small business lending market and how our member companies bridge the small business capital gap using innovative financing solutions. SBFA is supported by companies committed to promoting small business owners' access to fair and responsible capital.

II. COLLECTION OF PERSONAL INFORMATION

A. Notice Of Privacy Policy At The Time Of Collection of Personal Data

W271-1

While we do appreciate the AG adding language that allows a company to provide the privacy disclosure verbally, there is still ambiguity as to how that would work from a practical standpoint. Is the company required to read, word for word, the entirety of its privacy policy that it has on its website? If so, the recitation of the privacy disclosure could take up to fifteen minutes depending on the length of the privacy policy (which may vary from company to company). This would provide for a horrible customer experience. As our members' clients are small businesses, this additional time may detract from the small businesses daily operations. W271-1 (cont.)

We would recommend some guidance as to how companies can comply with providing the privacy policy verbally. We would suggest allowing companies to inform a customer that the company has a privacy policy that the company obtains certain personal information that the customer provides to the company and the customer can review the privacy policy on the company's website or the company can provide the client the privacy policy via email.

B. Notice Provided To Customer When Information Collected

The proposed Regulations state that "a business that collects personal information from a consumer shall provide notice at collection…" Does this mean that only the company who directly collects the personal information must provide the disclosure or could this also include any company that is in receipt of the personal information from another company must also disclose to the customer that it is collecting the customer's personal information? W271-2

We would request clarity as to whether or not any secondary company that receives personal information from a primary company that collected the personal information, would also have to disclose the notice at the time that it received the customer information from the first company. We would recommend that only the company that directly requests the personal information from the customer should provide the privacy policy and any secondary company that receives the personal information from the primary company need not provide the privacy disclosure, unless that secondary company obtains additional personal information from the customer.

C. Categories Of Personal Information

Section 999.313(10)(f) states the business shall provide the "categories of personal information that the business disclosed for a business purpose in the preceding 12 months, and for reach category identified, the categories of third parties…" It is unclear if this solely refers to personal information disclosed to a third party (as defined in the CCPA) or just disclosed in general to another party (whom does not meet the definition of a third party under CCPA). As it is currently drafted a business might have to disclose categories of personal information that was disclosed to a party that is not a third party W271-3

under CCPA. We would request clarity as to whether this solely refers to personal information disclosed to the CCPA definition of a third party to and party.

W271-3 (cont.)

III. DELETION OF DATA

A. Deletion Of Data

Some of the items that have not been addressed surround the deletion of data. Besides attempting to fight fraud, the actual deletion of data is still unclear. As we mentioned in our previous comment, in the event of a deletion request, would a company have to delete the actual email (all emails have personal information as they all have the customers email address). Also, would a company have to delete all contracts with customers even if those contracts are basically saved in an electronic file where the data in the contracts is not scrubbed and "collected" for analytical reasons? Moreover, if a customer has requested to be removed from any marketing material (*e.g.* email or direct mailers), in order for the company to comply with the customer's request, the company must maintain the email address, name and address to make sure that the customer is suppressed from any future marketing campaigns. It is impossible for member companies to comply with both the customer's request to delete and request to stop receiving marketing material. Or if a customer states that his/her information was stolen, SBFS companies want to make sure they have a record of that so that if the personal who fraudulently applied tries to apply again, our member companies can stop that from happening. We request that the proposed Regulations be revised to include an exemption from the deletion requirement for these types of situations. This ties in to our concern that that while there are exceptions for deletion of data based on Section 1798.145(a)(2)(3)(4), we still have concerns regarding deletion of data and our members efforts to fight fraud. SBFA member companies have a wealth of information to fight fraud and assist in investigations into fraud rings or identity theft; however, if the company is required to delete the information, it will not be of any assistance to itself or others in fighting future fraud.

W271-4

By requiring the deletion of data, there are unintended consequences. Bad actors, knowing that if they request their information to be deleted, can perpetuate any fraud because a company may not have any internal fraud detection due to the bad actors request to delete information. It is imperative that the AG allow for retention of certain data in order to reduce fraud.

IV. CONCLUSION

We appreciate the AG's effort to draft meaningful proposed Regulations. Although we appreciate the AG's continued efforts, there are still issues with the Regulations and additional

work needs to be done in order to provide clarity and a frame in which companies can comply and are not subject to litigation.

Thank you for considering our comments and our previous comments. We remain committed to working with you to implement regulations that provide value to small businesses. We hope you appreciate our letter and recognize that it exhibits our commitment to working with you to make sure the final regulations work and provide value. We would be happy to discuss these matters in person or by telephone. You may reach me at [redacted].

Respectfully,

Steve Denis
Executive Director

From: Rachel Michelin
To: Privacy Regulations
Cc: Steve McCarthy
Subject: 2020.2.25 CRA California AG Proposed Regs Comments
Date: Tuesday, February 25, 2020 1:17:06 PM
Attachments: Outlook-vgutruih.png
Cal Retailers 2.25.20 CCPA reg comments.pdf

Hello,

On behalf of the California Retailers Association, attached please find Comments on the proposed CCPA Regulations revisions released on February 10, 2020.

Thank you.

Rachel Michelin
President & CEO
1121 L Street, #607
Sacramento, CA 95814
[redacted]
[redacted]
@CRAgovtaffairs

February 25, 2020

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

Dear Attorney General Becerra:

Thank you for the opportunity to comment on the revised California Consumer Privacy Act regulations that were released on February 10, 2020.

As you are aware, the retail industry is a driving force for California's economy. One in four jobs in California are in the retail industry. In California alone, over 3.2 million people are employed by retailers, eight times the number of employees in the entertainment industry. The retail industry accounts for $330 billion in California's gross domestic product each year.

California retailers value their relationship with consumers and have no higher priority than earning and maintaining the trust and confidence of our customers. Retailers embrace careful stewardship of customer data not only because maintaining customer trust is a core business imperative, but because it is the right thing to do. That is why the California Retail Association (the "Association") has worked closely with policymakers to try and build a workable and transparent regulatory structure for consumer data that meets the expectations of California consumers and aligns the ability of retailers and other businesses to offer Californians the goods and services they desire – both on-line and at any of California's 400,000 retail establishments.

In reviewing the second draft of the proposed CCPA regulations, we want to thank you for your willingness to address some of our concerns as outlined in our December 6, 2019, letter. While we appreciate your attention to our comments, we believe a few strategic changes in the proposed regulations would help this law realize its full potential to protect California consumers, enhance our state's technology economy, and promote uniform and fair enforcement.

IMPLEMENTATION PERIOD

- **The Regulations Should Not Be Effective Until at Least January 1, 2021, or beyond.**

W272-1

The CCPA is the country's first comprehensive privacy and data security law. Many businesses, consumer groups, and individual consumers alike are working diligently to understand and comply with the new regulatory structure that, clearly, remains to be finalized. There are many new obligations that require both internal and external resources not previously contemplated (e.g., designing and building the necessary infrastructure), and while retailers are committed to a substantial, good-faith effort to comply, our members continue to believe all stakeholders would benefit from additional time to understand and prepare for the application of the Regulations.

For these reasons, the Association asks the Attorney General to confirm a compliance grace period for the Regulations, up to and including January 1, 2021, or beyond.

§ 999.305 – Notice at Collection

- **Every collection and use of data must be described in a posted privacy policy at the time of collection and personal information may not be collected if a notice is not provided at or before the point of collection.**

W272-2 The regulation language is not clear in relation to what the disclosures should include or the locations (if in a physical environment) where the notices must be posted. If notices are required at every location where personal information may be collected, the effect may be consumer notice fatigue, thus losing the effectiveness of posting the notice. We recommend the regulations make it clear that a business that collects consumers' personal information offline may, as authorized for the online notice, post prominent signage directing consumers to where the notice can be found online. That notice need not contain more information than the fact that the business collections personal information and where the required notice can be found online.

- **In a business's Privacy Policy, the description of the categories of personal information collected must correlate with the categories of the third parties to whom the information is disclosed.**

W272-3 Many retailers, like most businesses, are required to function in an environment requiring multiple and complex third-party relationships. A consumer should not be required to read through difficult and complicated charts of information, nor should retailers be required to complete the extensive mapping required to correlate categories of third parties with types of personal information. We suggest this requirement be omitted in the privacy policy.

- **Access to different privacy notices (privacy policy, notice of collection of personal information, notice of opt-out of sale, and notice of financial incentives) must be available in-store and possibly at contact centers. Opt-out notices must be reasonably accessible to consumers with disabilities (e.g. comply with WCAG standards for online notices)**

W272-4 Retailers should have the discretion to provide notices in a way that makes sense for how customers interact with the store in the physical environment.

§ 999.305(a)(4) – Just-in-time Notice

- **Just-in-time notice required on mobile devices when collection of personal information would not be reasonably expected by the customer.**

W272-5 This potentially could cause consumer notice fatigue. In order to be effective, retailers request guidance on what a consumer could reasonably expect. For example, some app developers use data acquired from users to develop new features that will be released subsequently. Would using data for internal research and development without additional notice be permissible? Also, this requirement may incentivize long, complex initial notices to preemptively cover possible unanticipated uses for data. Additionally, there are some passive collections of data in the physical environment that would prove difficult to capture affirmative consent for, such as driver's license scans for age verification or CCTV. Finally, we respectfully request further clarity as to whether a user-enabled setting on a mobile device or app would trigger the "just-in-time" notice requirement.

§ 999.307 – Notice of Financial Incentive

- **The AG should clarify that a financial incentive or price or service difference is "related to the disclosure, deletion, or sale of personal information" only when the incentive or price or service difference is provided in exchange for the customer's exercise of a right conferred by the CCPA or the AG regulations and not otherwise.**

W272-6 This interpretation is consistent with the text and examples offered in 999.336. In example 2, the retailer is not providing the benefit in exchange for the customer's decision not to delete the information. To the contrary, the retailer is doing what the consumer requested. The coupon (opportunity for a price difference) is not provided because the consumer did or did not exercise a right conferred by the CCPA or these regulations. The coupon is provided to encourage the consumer to spend more money with the retailer. In Examples 1 and 4, on the other hand, the consumer's exercise of the right conferred by the CCPA apparently is the reason for the business's subsequent action with respect to the financial incentive or price or service difference. We request that the AG confirm that the retailer's loyalty program in example 2 is not offering a financial incentive or price or service difference for which a notice of financial incentive is required.

- **The requirement to include a business's estimated value of the consumer's data in the business's financial incentive notice would effectively require the business to publicly disclose confidential information that offers little benefit to the consumer.**

W272-7

The specific calculation combined with a description of how that calculation was made provides specific insight into a retailer's accounting calculations. Also, the estimated value of consumer's data, when based on calculations involving hundreds of thousands, and in some cases millions, of individual's data will not be particularly informative or relevant to a single individual reading the calculation in the notice. An alternative to the current requirement would be to require a retailer to maintain its estimated value of the consumer's data analysis internally and provide it to the Attorney General upon request, and marking it as "business confidential" to protect it from a state public records request. A similar approach is currently taken for business confidential information disclosed to the HHS Office for Civil Rights in the context of HIPAA enforcement.

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

- **The revised regulations specify two standards for requests for access and requests for deletion:**
  - **Access –** *exclusively online companies that have direct relationships with consumers "shall only be required to provide an email address for submitting requests to know." Also specifies other companies (e.g., bricks-and-mortar or bricks-and-clicks) must at a minimum have a toll-free number and one other method, but states as examples a designated email address, an in-person form, or a form submitted via mail.*
  - **Delete –** *specifies two different methods that must be used but doesn't require a toll-free number as one of the methods; specifies as examples for delete requests methods like toll-free phone number, link or form available online, designated email address, in-person form, form submitted via mail.*

W272-8

The Association continues to have concerns related to this requirement as it places additional burdens and compliance obligations on retailers with physical store locations. The requirement poses greater security risks for consumers when dealing with personal information on paper forms and could increase the risk of paper forms being lost in the submission process or in the mail. The Association prefers a requirement that businesses with physical locations have prominent signage pointing consumers to online web sites and/or a toll-free number to submit requests. This seems more reasonable to keep the submission process as consistent as possible which will also help keep consumer's Personal Information secure.

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

- **The revised regulations require different levels of verification for different types of data.**

W272-9

For mixed sets of data, we suggest retailers have the discretion to require the most stringent verification criteria to apply for the entire request.

- **If consumer access request is denied for identity verification failure, businesses must evaluate whether the customer was seeking disclosure of categories of personal information about the customer.**

W272-10

The Association asks for clarity on whether this needs to be customized to the individual making the request.

- **If consumer access request is denied because of conflict with federal or state law, or an exception to CCPA, businesses must inform the requestor and explain the basis for the denial (unless prohibited by law).**

W272-11

The Association asks for clarity on the levels of specificity they must provide for denying the request (e.g., explanation of which law or just a general statement).

- **Companies that collect more than 10 million Californians' personal information must post metrics on the volume of CCPA requests and metrics on response times annually.**

W272-12

The Association requests clarification on how this information would be useful to the consumer.

- **If a deletion request is denied due to statutory exception, the revised regulations require businesses to explain specific reasons to consumers and place restrictions on the processing of the consumer's information.**

W272-13

Requiring businesses to explain this for each unique circumstance complicates and slows down the process.

- **User-enabled global privacy controls (e.g., browser plug-in or privacy settings) that communicates customer choice to opt-out is treated as opt-out of sale requests.**

W272-14

The Association is asking for additional guidance on how to implement this regulation.

- **The revised regulations clarify all sections of the access disclosure report must be personalized to the individual consumer.**

W272-15

This should only be required if the benefit to the consumer outweighs the burden and expense it places on the retailer.

- **The revised regulations stipulate that requests for consumer information must include signed instruction form requesting customer from an authorized agent.**

W272-16

As signatures could be forged, a notarization process should be required.

- **For households that have password-protected accounts, businesses may process access and delete requests as usual, but if there is a member of the household who is younger than 13, businesses must obtain verifiable parental consent prior to complying with requests for the household.**

W272-17

This requirement needs to ensure parental consent is part of the request process. Otherwise, retailers face conflicting priorities of honoring the access request and protecting children's information.

- **A business that cannot verify an individual within 45 days of the request being made must notify the consumer the request is being closed due to the inability to verify.**

W272-18

Retailers need clarity on whether they must wait the entire 45 days to notify consumers or notify consumers as soon as the inability to verify is determined.

§ 999.315(d) – Global Privacy Controls

- **Requiring businesses to recognize and act upon "global privacy controls," as described in this requirement, remains a very complicated and challenging prospect with many technological hurdles.**

W272-19

In (d)(1), it is unclear if the "privacy control" reference applies only to privacy controls established by the retailer, or "global privacy controls" not established by the retailer (e.g. controls created by developers or manufacturers of browsers, devices, or other mechanisms). Clarity on this point would be particularly helpful for retailers to understand what "global privacy controls" it must recognize and act upon to comply.

§ 999.323(d) – No Fee for Verification

- **A business shall not require the consumer to pay a fee for verification, such as asking the consumer to provide a notarized affidavit to verify their identity.**

W272-20

This regulation forces retailers to take too much risk in balancing providing access to the consumer while protecting consumer data. Some consumers may be harder to verify, so retailers should be able to use verification methods deemed reasonable by other industries/sectors.

§ 999.325(e)(2) – Verification illustrative example

- **This illustrative example may guide the public expectation in the wrong direction by stating a business may verify identity by asking for the recent item purchased and the cost. If one gets an abandoned receipt of someone else, that person holds the key to the customer's Personal Information maintained by that business.**

W272-21

This is confusing and is too fact-specific to aid retailers in determining how to comply with the regulations' verification requirements and raises more questions about how a business should interpret the verification requirements in this section. Retailers would benefit from an example more clearly addressing what is expected of a retailer to verify an actual person that is associated with personal information when that personal information is maintained in a manner that is not associated with an actual person.

W272-22 The revised regulations also create two types of "request to know" with respective ID verification standards (e.g. request to know specific pieces of information and request to know categories of personal information) - this is inconsistent with the CCPA. Requiring less degree of the authentication standard for categories of information increases security risks (e.g. hackers now know the types information there is to retrieve, and it may expose information that one has transacted with that business).

§ 999.326 – Authorized Agent

- **Requires a business to accept of the power of attorney per the Probate Code.**

W272-23 If Power of Attorney is provided, the retailer can't verify requestor's identity per 999.326(a). A Power of Attorney is effective if notarized or bears two witnesses' signatures. It is a very low standard and easy to forge – the law should not dictate what the retailer must accept when authenticating a document. As signatures could be forged, a notarization process should be required.

The California Retailers Association represents all segments of the retail industry, including general merchandise, department stores, mass merchandisers, online markets, restaurants, convenience stores, supermarkets and grocery stores, chain drug stores, and specialty retail such as auto, vision, jewelry, hardware and home stores. The Association respectfully submits our comments to the Attorney General with the specific intent to improve the proposed Regulations so that consumers have more transparency and control over their personal information, while continuing to benefit from the retail experience they enjoy today.

The Association thanks the Attorney General's Office for its hard work and dedication to the development of the CCPA Regulations and look forward to the opportunity to continue to work with Attorney General on privacy issues.

Sincerely,

Rachel Michelin
President & CEO
California Retailers Association

From: Melanie Tiano
To: Privacy Regulations
Subject: CTIA Comments in Response to Modified Regulations
Date: Tuesday, February 25, 2020 12:51:35 PM
Attachments: image003.png
CTIA Comment on CCPA Modified Regulations 02.25.20.pdf

To Whom It May Concern:

Attached please find CTIA's comments in response to the modified proposed regulations.

Please let me know if you have any questions.

Thank you,

Melanie

Melanie K. Tiano
Director, Cybersecurity and Privacy
1400 16th Street, NW
Washington, DC 20036
[redacted] (office)
[redacted] (mobile)

Before the
STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
ATTORNEY GENERAL'S OFFICE
Los Angeles, CA 90013

In the Matter of California Consumer Privacy Act Rulemaking Process	)))))))	Public Forums on the California Consumer Privacy Act

COMMENTS OF CTIA

Gerard Keegan
Vice President, State Legislative Affairs

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th St. NW, Suite 600
Washington, DC 20036

(202) 736-3200
www.ctia.org

February 25, 2020

TABLE OF CONTENTS

Before the
STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
ATTORNEY GENERAL'S OFFICE
Los Angeles, CA 90013

In the Matter of	)	
	)	
California Consumer Privacy Act Rulemaking Process	)	Public Forums on the California Consumer Privacy Act
	)	
	)	

INTRODUCTION

CTIA welcomes the opportunity to provide comments on the California Attorney General's modified proposed regulations ("modified regulations") to implement the California Consumer Protection Act of 2018 ("CCPA" or "Act").[1] These comments supplement CTIA's previous comments filed on December 6, 2019.[2] CTIA understands the demanding statutory deadlines governing this process and commends the Attorney General's efforts to address some key concerns and implementation challenges raised by the initial proposed regulations.

Nevertheless, CTIA remains concerned that many of the provisions included in the initial proposed regulations that were either: (1) outside the CCPA's grant of rulemaking authority; (2) inconsistent or in conflict with the CCPA; (3) unnecessarily or unduly burdensome; or (4) so vague as to functionally prohibit uniform compliance, have not been adequately addressed in the modified regulations. To the extent those issues remain unaddressed, CTIA renews the concerns raised in its December 6 comments.

[1] *See generally* Cal. Civ. Code § 1798.100 *et seq.*
[2] *See* Comments of CTIA, *In the Matter of California Consumer Privacy Act Regulations,* California Office of the Attorney General, Request for Comments, December 6, 2019 ("CTIA's Dec. 6 Comments").

CTIA understands that in enacting the CCPA, it was the Legislature's intent to protect consumers' privacy. Above all else, this understanding serves as the guiding principle for these comments. If adopted in their current form, CTIA is concerned that several of the modified regulations would have the opposite effect, requiring businesses to jeopardize consumers' privacy in order to satisfy vague or unnecessary compliance obligations.

CTIA's most urgent concerns pertain to the following sections of the modified regulations:

- § 999.306 – Notice of Right to Opt-Out of Sale of Personal Information
- § 999.307 – Notice of Financial Incentives and § 999.337 – Calculating the Value of Consumer Data
- § 999.313 – Responding to Requests to Know and Request to Delete.
- § 999.314 – Service Providers
- § 999.315 – Requests to Opt-Out
- § 999.316 – Requests to Opt-In After Opting Out of the Sale of Personal Information
- § 999.326 – Authorized Agent

Where appropriate, CTIA provides proposed regulatory language to address the issues identified.

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

a. The Proposed Opt-Out Button is Needlessly Misleading and Beyond the Scope of the CCPA's Authority

CTIA recommends the Attorney General modify the opt-out button established by subdivision § 999.306(f) (pictured below).

W273-1

CTIA recognizes the difficulty in developing such a button and appreciates the Attorney General's efforts in designing the current iteration. However, to the extent a business wants to use the optional button, the current design would needlessly mislead consumers into thinking that the

button itself provides an immediate interactive opt-out control, rather than a link to a page with more information about how consumers may exercise opt-out requests, as was contemplated by the Legislature.

The button proposed in the modified regulations is a toggle or radio button, which will mislead consumers into believing that by sliding the toggle, they might immediately and fully exercise their CCPA opt-out rights. However, as is evident from these modified regulations, the opt-out button was not intended to be a switch.[3] Moreover, even if that was the intent, it would be a significant and unauthorized departure from the grant of rulemaking authority established by the CCPA. Specifically, Cal. Civ. Code §1798.185(a)(4)(C) requires the Attorney General to establish rules and procedures for the development and use of a logo or button that "promote[s] consumer awareness of the opportunity to opt-out of the sale of personal information." The statute does not authorize the Attorney General to mandate a specific and additional mechanism through which businesses might be compelled to offer further opt-out functionality.

W273-1 (cont.)

Accordingly, CTIA recommends that the Attorney General redesign the opt-out button to better reflect the Legislature's intent and to avoid unnecessary consumer confusion.

II. § 999.307 Notice of Financial Incentives and § 999.337 – Calculating the Value of Consumer Data

The Financial Incentives Framework Remains Impractical and Misleading to Consumers

W273-2

CTIA appreciates the Attorney General's modifications to subdivisions §§ 999.307 and 999.337 relating to financial incentives, which would provide more flexibility in how businesses

[3] *See* § 999.306(f)(3) (stating that the button "shall link to a webpage or online location containing the information specified in section 999.306(c).").

value consumer data. Nevertheless, CTIA reiterates its concern that the requirements of these proposed subdivisions exceed the Attorney General's rulemaking authority and would require businesses to disclose information that could be detrimental to both consumers and businesses. As the Initial Statement of Reasons ("ISOR") acknowledges, methods for calculating the value of personal information vary widely, and consumers tend to value their information in subjective, context-specific ways.[4] Still, the Attorney General proposes to require companies to disclose specific monetary valuations of personal information to put consumers "in a position to make informed decisions on whether to opt-in to the offered financial incentives."[5]

W273-2 (cont.)

Based on CTIA members' experience, this information will likely both under- and overestimate the value of data depending on who the consumer is, and thus confuse a significant number of consumers. At worst, it will mislead consumers by creating a false sense of certainty about the value of their personal information. Moreover, the implication that a business could quantify the value of the data of one or more consumers with a dollar amount is inaccurate and misleading. In CTIA members' experience, financial incentive programs are based on a complex calculation of costs to the business and market comparisons, and they are designed to reward loyal customers rather than to serve as a value exchange. Thus, a single customer's business or data holds little independent "value." Instead, data gains value when it is aggregated and that value is dependent upon changing business circumstances and priorities.

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

a. The Removal of the Security Risk Exception in § 999.313(c)(3) Poses a Threat to Consumers

W273-3

[4] *See Initial Statement of Reasons ("ISOR") for Proposed Adoption of California Consumer Privacy Act Regulations* 38 (2019).
[5] *ISOR* at 12.

CTIA requests the Attorney General reinstate former subdivision § 999.313(c)(3) which prohibited businesses from responding to requests for the specific pieces of personal information when doing so created unreasonable risks. While a stringent standard to meet, this provision would act as a final stopgap to protect consumers' privacy and generally limit unforeseen consequences of the new CCPA framework.

Indeed, while due to the lack of precedent of comprehensive privacy legislation like the CCPA, it remains unclear to what extent threat actors will attempt to manipulate CCPA access requests for their own malicious purposes, including identity theft, harassment, or cybersecurity attacks, it seems likely to occur. In its previous iteration, subdivision § 999.313(c)(3) utilized a flexible standard that addressed this concern by requiring businesses to adjust their procedures in response to perceived risk. Thus, businesses were empowered to proactively respond to changes in technology and criminal tactics, even when such changes are, as of now, not foreseeable. W273-3 (cont.)

For these reasons, CTIA asks the Attorney General to reinstate the following language in addition to (and not in lieu of) subdivision § 999.313(c)(3) of the modified proposed regulations:

> ***§ 999.313(c)(3).*** *"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 the personal information, the consumer's account with the business, or the security of the business's systems or networks."*

b. **The "Legal or Compliance Purposes" Requirement in § 999.313(c)(3) is Overly Burdensome**

The Attorney General has included a new provision in subdivision § 999.313(c)(3) that clarifies that a business is not required to search for personal information in response to requests to know if each of four enumerated conditions are met.[6] While CTIA appreciates the Attorney W273-4

[6] Modified regulation § 999.313(c)(4) (stating that a business shall not be required to search for personal information when, "a. the business does not maintain the personal information in a searchable or reasonably accessible format; b. the business maintains the personal information solely for legal or compliance purposes; c. the business does not sell the personal information and does not use it for any commercial purpose; and d. the business describes to the consumer

General's attempt to reduce burdens on businesses, one of the conditions – that the personal information at issue be maintained solely for legal or compliance purposes – creates a standard that renders this provision largely unusable.

Under this standard, if a business maintains personal information for any purpose other than legal or compliance, that business would be required to search for personal information even when the information is stored in archival, backup, or some other inaccessible format, regardless of the costs or time associated with conducting such a search. For example, businesses would be required to search for information in unstructured databases, such as log files maintained solely for network protection and cybersecurity purposes, even when this information is not searchable or reasonably accessible. Under the modified regulation, a business would be required to search for this information whenever the purposes for storage fall outside of the requirement that the information be maintained "solely for legal and compliance purposes." Moreover, this requirement to search could require businesses to further process personal information to determine whether the information is maintained solely for "legal or compliance purposes." The result is additional, needless processing beyond what a business would normally engage in.

W273-4 (cont.)

Accordingly, CTIA requests that the Attorney General modify this subdivision as follows:

> **§ 999.313(c)(4).** "*In responding to a request to know, a business is not required to search for personal information if all the following conditions are met:*
>
> - *a. The business does not maintain the personal information in a searchable or reasonably accessible format;*
> - ~~*b. The business maintains the personal information solely for legal or compliance purposes;*~~
> - *c. The business does not sell the personal information and does not use it for any commercial purpose; and*

the categories of records that may contain personal information that it did not search because it meets the conditions stated above.").

- *d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above."*

W273-4 (cont.)

IV. § 999.314 – Service Providers

a. The Restriction on Cleaning or Augmenting Data from Other Sources Effectively Nullifies 314(c)(3)

Subdivision § 999.314(c) permits service providers to retain, use, and disclose personal information "for internal use [] to build or improve the quality of its services." However, this provision creates uncertainty as to the extent that service providers may do so when improving the quality of its services involves "cleaning or augmenting data acquired from another source." Given the lack of a legal definition or common understanding of the meaning of "cleaning" data, this limitation creates substantial ambiguity. Furthermore, the restriction is likely to impede service providers – particularly small and medium enterprises – from doing the very thing that subdivision § 999.314(c)(3) purports to allow – build and improve the quality of their services. This requirement is likely to have an adverse impact on data-dependent industries throughout California.

W273-5

i. The Restriction on Cleaning or Augmenting Data from Other Sources Creates Confusion and Encourages Inconsistent Implementation

The act of "cleaning" is neither defined under California law, nor does it appear to be a term that has a common meaning in industry standards and practice. Consequently, introducing this term into the modified regulations is likely to create confusion and inconsistent application among businesses subject to the CCPA. Further confusion arises around the scope of this restriction: it is unclear whether a service provider may use its own data to "clean" or "augment" a business's data, or whether a service provider's own data would be considered "acquired from another source," given that at some point in time, it likely was. Further confusion arises around the scope of this restriction. Inclusion of this provision therefore undermines the aim of the modified regulations to

provide businesses with clear instructions as to how the CCPA should be interpreted and invites inconsistent implementation of the law.

ii. The Restriction on Cleaning or Augmenting Data from Other Sources Potentially Creates Inadvertent Competitive Advantages for Large Businesses at the Detriment of Smaller Businesses

Not all service providers have the internal resources to create quality data, and further, not all businesses can conduct quality data analytics on their own. Businesses that have the resources to collect new pools of data to support their own analytics operations likely will; but only large businesses with significant resources are positioned to do so.

W273-5 (cont.)

Thus, this limitation has the potential to establish disparate treatment for companies functionally engaged in the same activity. Large businesses with resources are empowered to collect data and improve their services without such activities being considered "sales" under the law. Small and mid-sized companies and startups—or any entity that lacks the resources to perform analytics in-house or to collect large pools of quality data—will be left with two less desirable options. They may either contract with a third party to perform analytics and be swept into the heightened "sale" provisions of the CCPA, or not perform analytics at all. Thus, as formulated, this subdivision could benefit large organizations and at the expense of small and mid-sized businesses.

Accordingly, CTIA requests that the Attorney General modify this subdivision as follows:

> **§ *999.314(c).*** *A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except: (1) To perform the services specified in the written contract with the business that provided the personal information; (2) To retain and employ another service provider as a subcontractor, where the subcontractor meets the requirements for a service provider under the CCPA and these regulations; (3) For internal use by the service provider to build or improve the quality of its services, including the cleaning or augmenting of data acquired from another source, provided that the use does not include building or modifying household or consumer profiles~~, or cleaning or augmenting data acquired from another source~~; (4) To detect data security*

incidents, or protect against fraudulent or illegal activity; or (5) For the purposes enumerated in Civil Code section 1798.145, subsections (a)(1) through (a)(4).

W273-5 (cont.)

V. § 999.315 – Requests to Opt Out.

a. The Inclusion of Browser Plug-In Opt-Outs is Not Authorized by the CCPA

CTIA reiterates the concerns it raised in its December 6 comments regarding expanding the consumer opt-out methods to include global privacy controls, such as browser plug-ins or privacy settings. This expansion is a significant and unauthorized departure from the grant of rulemaking authority established by the CCPA. As explained in our earlier comment, there is simply no support in the text of the CCPA for the Attorney General to create additional opt-out mechanisms. Despite this, subdivision § 999.315(c) would require businesses to treat user-enabled privacy controls, such as browser plug-ins, privacy settings, or other mechanisms, as valid requests to opt out. This mandate is inconsistent with the requirements of the Cal. Civ. Code § 1798.135(a)(1), which specifies the one and only method by which consumers can convey their requests to opt out – through the "Do Not Sell My Personal Information Link" – as well as the processes that businesses must follow in response to such requests.[7]

W273-6

Accordingly, CTIA requests that the Attorney General withdraw this proposal. Should the Attorney General decline CTIA's request, we ask that the three specific concerns described below be addressed.

b. Business Should Not Be Required to Comply with User Enabled Privacy Controls Until Reasonably Available Technology Exists

Subdivision § 999.315(d)(1) requires businesses treat user enabled privacy controls as opt-out requests only to the extent that such controls clearly communicate that a consumer intended to

W273-7

[7] Cal. Civ. Code 1798.135(a)(1) (Stating a business shall "Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information.").

opt out of the sale of their personal information. However, uncertainty surrounding privacy control technology will make subdivision § 999.315(d)(1) difficult to operationalize, leading to inconsistent approaches. For example, currently, there are different understandings of what constitutes a browser setting or plug-in and which mechanisms reflect genuine user intent. Similarly, not every browser can communicate clearly whether users are California consumers under the CCPA, which also potentially raises questions about extraterritorial reach. Thus, there is insufficient consistency and interoperability to make this regulation workable. CTIA asks that the Attorney General clarify that a business is obligated to comply with user enabled privacy control requests only if, and when, reasonably available technology and privacy standards exist.

W273-7 (cont.)

c. **The Limitation on Pre-selected Settings is Overbroad and Misleading**

CTIA also requests that the Attorney General clarify subdivision § 999.315(d)(1) of the modified regulations which requires that a consumer affirmatively select their choice to opt out of the sale of their personal information within the global privacy control's settings. This provision may cause confusion because it states broadly and without exception that the privacy control "shall not be designed with any pre-selected settings." This requirement appears in conflict with the Attorney General's intention that privacy controls should default to allowing the sale of personal information (since consumers must affirmatively opt out). By prohibiting "any pre-selected settings," however, subdivision § 999.315(d)(1) misleadingly suggests that no default setting is permissible, rather than prohibiting only those pre-selected settings which would automatically, and without consumers' consent, opt consumers out of the sale of their personal information.

Accordingly, CTIA recommends the Attorney General modify subdivision § 999.315(d)(1) as follows:

> ***§ 999.315(d)(1).*** *"Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to the opt-*

out of the sale of personal information. The privacy control shall require that the consumer affirmatively select their choice to opt-out and shall not be designed ~~with any pre-selected settings.~~ in a manner that would prevent the sale of personal information unless the customer affirmatively selects their choice to opt out."

W273-7 (cont.)

d. **Providing Fraudsters with the Reason for Denial of Opt-Out Requests Endangers Consumers**

Subdivision § 999.315(h) empowers businesses to combat fraud by providing businesses with the flexibility to deny opt-out requests when a business has a "good-faith, reasonable, and documented belief' that the request is fraudulent. This flexibility is necessary to address the uncertainty surrounding how threat actors might abuse such requests and any changing criminal tactics that may arise. However, subdivision § 999.315(h) also requires that in cases where a business denies an opt-out request because it suspects fraud, the business must provide the suspected fraudster with "an explanation why it believes the request is fraudulent."

W273-8

This provision effectively requires businesses to provide suspected fraudsters with a roadmap for how they might resubmit more effective fraudulent requests. Although the risks associated with fraudulent opt-out requests may be low, providing reasons for denial in this context may increase fraudsters' ability to successfully execute more damaging access and deletion requests.

Accordingly, CTIA asks the Attorney General to modify subdivision § 999.315(h) as follows:

> ***§ 999.315(h).*** *"A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request because ~~and shall provide an explanation why~~ it believes the request is fraudulent."*

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

W273-9

Clarify that Requests to Opt In Provisions Apply Notwithstanding Businesses' Obligations Under 1798.135(a)(5)

CTIA requests that the Attorney General clarify subdivision § 999.316(b), which addresses how businesses might respond to consumers who have opted out of the sale of their personal information and who later attempt to use a product or service that requires the sale of personal information.

The Attorney General should clarify that this provision is intended to apply notwithstanding a business' general obligation to respect consumers' opt-out decisions for at least twelve months.[8] Without this express clarification, subdivision § 999.316(b) could be read to be in conflict with this statutory requirement. Accordingly, CTIA asks the Attorney General to modify this subdivision as follows:

W273-9 (cont.)

> ***§ 999.316(b).*** *"Notwithstanding a business's requirement, pursuant to Cal. Civ. Code §1798.135(a)(5), to respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information, ~~I~~if a consumer who has opted-out of the sale of their personal information initiates a transaction or attempts to use a product or service that requires the sale of their personal information, a business may inform the consumer that the transaction, product, or service requires the sale of their personal information and provide instructions on how the consumer can opt in."*

The same issue arises in § 999.315(d)(2) when a consumer's global privacy control settings are in conflict with the consumer's existing business-specific privacy setting or their participation the business's financial incentives program. CTIA asks the Attorney General to provide similar clarification, modifying that subdivision to read:

> ***§ 999.315(d)(2).*** *"Notwithstanding a business's requirement, pursuant to Cal. Civ. Code §1798.135(a)(5), to respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information, ~~I~~if a global privacy control conflicts with a consumer's existing business-specific privacy setting or their participation in a business's financial incentive program, the business shall respect the global privacy control but may notify the consumer of the conflict and give the consumer the choice to*

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

confirm the business-specific privacy setting or participation in the financial incentive program.

W273-9 (cont.)

VII. § 999.326 – Authorized Agent

a. The Authorized Agent Framework Creates an Unreasonable Risk of Fraud

As formulated, the unauthorized agent framework creates an unreasonable risk of consumer fraud. CTIA requests that the Attorney General clarify this process and implement greater safeguards to protect consumers. For example, the Attorney General should require all natural persons or businesses acting as authorized agents under the CCPA to register on a publicly available registry. Businesses presented with requests to know or requests to delete from a person purporting to act as a consumer's authorized CCPA agent may then consult this registry for authentication purposes.

Additionally, under subdivision § 999.326, the few existing safeguards that are intended to protect consumers utilizing the authorized agent process may be disregarded if "the consumer has provided the authorized agent with power of attorney." CTIA is concerned that this creates incentives for fraudsters to create false power of attorney documents. Moreover, under the current framework, there is no clear provision which authorizes businesses to verify these alleged power of attorney documents for their authenticity.

W273-10

Accordingly, CTIA requests that subdivision § 999.326(b) be deleted in its entirety to prevent unintended security risks. In the alternative, CTIA requests a moratorium on the authorized agent process until such time as protocols are developed to better protect consumer welfare.

b. The Authorized Agent Framework is Operationally Flawed as it Prevents Businesses from Verifying Authorized Agent Requests

Under subdivision § 999.326(a), when a consumer uses an authorized agent, a business may require a consumer to (i) provide the authorized agent written and signed permission to submit the

W273-11

request on their behalf; (ii) verify their own identity directly with the business; or (iii) directly confirm with the business that they provided the authorized agent permission to submit the request. This process is vague and operationally flawed as these requirements must be fulfilled by a consumer even when the business may have only had contact only with the authorized agent. To facilitate this process, businesses should be permitted to make these requests to the consumer through the authorized agents. Moreover, business should be expressly empowered to deny requests from authorized agents when a consumer fails to meet these verification standards.

W273-11 (cont.)

Accordingly, if the Attorney General does not delete or otherwise impose a moratorium on the authorized agent provisions, CTIA requests that the Attorney General provide express language authorizing businesses to verify that the subject consumer has authorized the agent with the same degree of rigor that businesses could otherwise utilize for direct consumer requests. This language might make clear that when an authorized agent fails to verify the same number of data points that would be required for direct consumer verification, a business may deny the request.

CONCLUSION

CTIA appreciates the Attorney General's consideration of these comments and stands ready to provide any additional information that might help to inform the development of final regulations.

Respectfully submitted,

/s/ Gerard Keegan
Gerard Keegan
Vice President, State Legislative Affairs

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th St. NW, Suite 600
Washington, DC 20036
[redacted]

February 25, 2020

From: Thomas Bloodworth
To: Privacy Regulations
Cc: Scott Talbott; Thomas Bloodworth
Subject: ETA Comments RE: Strengthening Fraud Prevention Under the California Consumer Privacy Act ("CCPA")
Date: Tuesday, February 25, 2020 12:45:18 PM
Attachments: image002.png
image010.png
ETA Comments - Privacy - AG Second Proposed Regulations.pdf

Lisa B. Kim, Privacy Regulations Coordinator –

Thank you for the opportunity to participate in thoughtful rulemaking. ETA and our members appreciate efforts to strengthen privacy protections for all California citizens, particularly as it relates to our ability to defend consumers against fraud. You will find our comments to the Second Proposed Regulations attached.

If you have any questions, please do not hesitate to let us know.

Thank you,

Tom Bloodworth
State Government Affairs
Electronic Transactions Association

p: [redacted]
a: 1620 L Street NW, Suite 1020 Washington, DC 20036
e: [redacted]

ELECTRONIC TRANSACTIONS ASSOCIATION

1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

February 25, 2020

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

RE: Strengthening Fraud Prevention Under the California Consumer Privacy Act ("CCPA")

Dear Attorney General Becerra:

On behalf of the Electronic Transactions Association ("ETA"), we appreciate the opportunity to comment on the California Consumer Privacy Act of 2018 ("CCPA"). The payments industry makes dedicated efforts to use innovation to fight fraud and ensure that consumers have access to safe, convenient, and affordable payment services. ETA and its members strongly support privacy laws that allow companies to implement innovative tools to protect consumer privacy and data while fighting fraud. ETA supports efforts by policymakers to strengthen the fraud prevention components of the CCPA including through an express exception for use of personal information for purposes of fraud prevention.

ETA is the leading trade association for the payments industry, representing over 500 payments and financial technology ("FinTech") companies that offer electronic transaction processing products and services and commercial loans, primarily to small businesses. During 2018 in North America alone, ETA members processed over $7 trillion in consumer purchases. ETA members include financial institutions, payment processors, FinTech companies, and all other parts of the payments ecosystem.

Executive Summary

ETA and its members support U.S. and international efforts to strengthen privacy laws to not only help industry combat fraud and but also disclose to consumers how their data is being used. As lawmakers and regulators explore additional ways to protect consumers, it is critical that government coordinate with the payments industry so that companies can continue to combat fraud and cybercrime and ensure consumers have access to safe, convenient, and affordable payment options and other financial services.

There are numerous existing consumer protection laws in the U.S. and around the globe that address data security and privacy, and which align with the payments industry's fraud fighting efforts. In the U.S., for example, financial information data is governed by federal laws, including the Gramm-Leach-Bliley Act and related Federal Trade Commission's Safeguards Rule and Consumer Financial Protection Bureau's Privacy Rule, as well as robust self-regulatory programs like the Payment Card Industry Data Security Standard, which sets forth requirements designed to

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

ensure companies that process, store, or transmit credit card information maintain a secure environment for such data. All of these laws and self-regulatory efforts recognize the critical role played by industry in combatting fraud, and they include provisions that allow for the targeted use and sharing of information by financial institutions and payments companies to protect consumers and to prevent fraud from occurring in the first instance.

Moving forward, ETA encourages policymakers to consider ways that law enforcement and industry stakeholders can continue to work together to develop new ways to combat rapidly evolving and increasingly sophisticated fraud and cybercrime. Working together, lawmakers, regulators, and the payments industry have kept the rate of fraud on payment systems at remarkably low levels. By continuing to collaborate, government and industry can provide consumers with access to safe and reliable payment services. Additionally, as different states and the federal government consider this important issue, it is important for policymakers to work together across state-lines to provide a consistent privacy framework without creating a patchwork of conflicting regulations.

Specific Comments

Notice at Collection of Information - §999.305(a)

The proposed rule would add a new requirement that is above and beyond the statutory requirements laid out in the CCPA. Section 999.305(a)(5) of the proposed rule requires that if a company intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notices at collection, the business must directly notify the consumer of this new use and **obtain explicit consent from the consumer to use it for this new purpose.** W274-1

This requirement to obtain "explicit consent" for a new use goes well beyond the requirements of the CCPA which only requires, "A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section." *1798.100(b)*. In fact, this requirement could result in less specificity in privacy policies which goes against the purpose of the law.

Additionally, Section 999.305(a)(4) requires just-in-time notice of collection for a purpose "that the consumer would not reasonably expect" and provides a clear description of an extreme case: a consumer would not reasonably expect a flashlight app to collect geolocation information. It is not clear, however, which less-extreme situations would similarly trigger this requirement. For example, many fraud-prevention mechanisms employed by the financial services industry use device geolocation as one factor among many in assessing whether a particular requested transaction may be fraudulent. Although the fact of collecting geolocation would be disclosed appropriately in the notice at collection, an additional pop-up notification could prove difficult to implement and may subvert the purpose of the fraud-prevention mechanism in the first instance, by alerting fraudsters to the timing and structure of businesses' fraud prevention methodologies. Consumers reasonably expect financial services businesses to protect them in a variety of ways, but inclusion of this provision introduces ambiguity. W274-2

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

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

Section 999.306(e) of the proposed rule prohibits a business from selling the personal information it collected during the time the business did not have a notice of right to opt-out posted unless it obtains the affirmative authorization of the consumer.

This requirement means that if a business did not sell personal information, and then did not have a "Do Not Sell" button, if it then chooses to sell personal information and has a button, then personal information collected about consumers during the time the button was not shown will be automatically subject to the opt-out. Accordingly, businesses will then have the option to request that consumers authorize the sale pursuant to 1798.135. First, this is counter to the text of the CCPA, which allows for new uses of data pursuant to notice, whereas explicit consent is required under the proposed regulations. This is in contravention to the statute. In addition, there is lack of clarity as to when businesses will be able to seek authorization from these consumers who will have been "deemed" to have opted out. W274-3

Notice of Financial Incentive - §999.307(b)(5)

Section 999.307(b)(5) of the proposed rule requires an explication of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including: 1) An estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and 2) A description of the method the business used to calculate the value of the consumer's data. This requirement is well above and beyond the requirements of the CCPA. ETA believes these requirements should not be included in the final rule, however, if these requirements are to be retained, this regulation should specifically relieve companies from having to reveal any trade secrets or proprietary information. W274-4

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

The deletion of a critical security control in Section 999.313(c)(3) opens businesses to significant security risk and unnecessarily exposes consumer personal information to potential theft and misuse. As articulated in the original draft regulations, businesses that could demonstrate that the release of certain personal information would create, "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," were not compelled to enable the creation of those risks by disclosing the data in response to a data access request. W274-5

Now, by removing this important clause without proposing any alternative language to protect against these risks, the regulations weaken the security of personal information by facilitating the creation of new avenues for hackers and other fraudsters to leverage the CCPA to attack businesses and steal the personal information of consumers for their own purposes. The original draft text set out specific criteria for businesses to meet so as to ensure that businesses would not leverage the exemption as a larger loophole for compliance with the CCPA. Only when a risk can be shown to

be 1) substantial, 2) articulable, and 3) unreasonable could the exclusion be leveraged. We urge you to reinstate the original language and allow businesses to have the ability to protect both their networks and the personal information they hold. W274-5 (cont.)

In proposed regulations Section 999.313(c)(5), if a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial. If the request is denied only in part, the business shall disclose the other information sought by the consumer. Several exceptions relate to issues where disclosing the basis for the denial is not feasible: such as for law enforcement purposes, exercising or defending legal claims, regulatory investigation, or criminal inquiry. ETA asks that the regulations include clarification that if a company includes the CCPA exemptions in their privacy policy they can just point consumers to those exemptions on their privacy policy and note that they are not responding because of an exemption listed in the privacy policy per CCPA. W274-6

Proposed regulations Section 999.313(d)(6) and (d)(7) appear to require an individual-by-individual description of excluded data – even though for certain exceptions the entire data repository is excepted (e.g. the GLBA exception). If entire exception-covered data stores are excluded from the data access fulfillment mechanisms employed by the business, it will be excessively difficult to access and report with specificity whether any particular requester's data resides in those excepted data stores. This section should be clarified to account for the disparity in exception of entire data sets and specificity in responses to requests. W274-7

In proposed regulations Section 999.313(d)(6)(a), where a business denies a consumer's request to delete the business must inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including any statutory and regulatory exception therefor. A company is simply not required to comply with the law if an exemption applies and therefor it is not a "denial." This requirement should be clarified to allow for companies to direct consumers to their policies explaining possible exemptions. W274-8

Service Provider – Protecting Against Fraud - §999.314(c)

In proposed regulations Section 999.314(a), a person or entity that provides services to a person or organization is not a business so long as it would otherwise meet the requirements of a "service provider" under Civil Code section 1798.140(v), that person or entity shall be deemed a service provider for the purposes of CCPA. When a person or entity is providing services to an organization that is not a business under CCPA, it is illogical for any requirements to be imposed on such service providers. As such, ETA recommends the following language to replace Section 999.314(a): W274-9

To the extent that a person or entity provides services to a person or organization that is not a business, no obligations under CCPA shall apply to such person or entity.

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

Requests to Opt-Out – Protecting Against Fraud - §999.315

Proposed regulation Section 999.315(h) requires a business, when denying a request to opt-out for suspected fraud, to "…inform the [opt-out] requestor that it will not comply with the request and shall provide an explanation of why it believes the request is fraudulent."

Businesses are constantly combatting the onslaught of fraudsters seeking access to consumers' money and financial information. Provisions requiring the disclosure to suspected fraudsters of why their attempt at fraud has failed, while well-intentioned, may open vectors for fraudsters to gather information concerning businesses' identity theft and fraud prevention methods, and may conflict with other obligations. W274-10

ETA recommends removing any requirement that would mandate the disclosure of the specifics of fraud detection and prevention programs.

Training- Record-Keeping - §999.317(g)

In proposed regulations Section 999.317(g), a business that alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 10,000,000 or more consumers, must compile a number of metrics from the previous calendar year and disclose that information in their privacy policy. W274-11

This is a new, onerous requirement that is outside of the scope of the CCPA's statutory language and does not serve consumers' privacy interests, particularly because the metrics would be available to the Attorney General in an investigation or an enforcement action regardless of publication.

General Rules Regarding Verification - §999.323

The new requirement in Section 999.323(d) that businesses not charge consumers for proper identity verification could be more thoughtfully constructed and is overbroad. Paired with the example highlighted in the modified draft, this new language effectively discourages the use of notaries, which is a commonly accepted legal method for authenticating the identity of an individual. The Uniform Statutory Form Power of Attorney (Cal. Probate Code Section 4401) even references the attachment of a required notary certification[1]. W274-12

When read in tandem with Section 999.326(b), which explicitly references the Probate Code's requirements as a means for businesses to streamline the verification of Authorized Agents, the new text in Section 999.323(b) creates an unnecessary barrier to consumer choice and a direct conflict with Section 999.323(e)'s requirement that businesses "implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information."

[1] The form explicitly states, "Include certificate of acknowledgment of notary public in compliance with Section 1189 of the Civil Code or other applicable law." Cal. Probate Code Section 4401.

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

Businesses required to ensure the security of the personal information they are tasked with disclosing or deleting should not be penalized for employing a separately required method for authenticating legal affidavits signed by consumers.

We recommend that the regulations make clear that use of a notary to verify the identity of the consumer does not trigger a monetary penalty to businesses looking to secure personal information when a consumer chooses to exercise his or her rights under the CCPA.

W274-12 (cont.)

Verification for Non-Accountholders - §999.325

Proposed regulations Section 999.325(g) requires that "If the business has no reasonable method by which it can verify any consumer, the business shall explain why it has no reasonable verification method in its privacy policy."

Fraudsters are increasingly sophisticated, and often build their success on the ability to gather specific knowledge of a business's fraud prevention programs. Required disclosure of verification difficulties or vulnerabilities in fraud detection serves only to better-equip fraudsters to gain access to consumers' personal information.

W274-13

The Role of the Payments Industry in Fighting Fraud

The payments industry is committed to providing consumers and merchants with a safe, reliable, and modern payments system. Indeed, consumers continue to choose electronic payments over cash and checks because of the protections afforded by electronic payments. These protections include, for example, zero liability for fraudulent charges, making electronic payments the safest and most reliable way to pay.

When it comes to credit cards, for example, a consumer can submit a chargeback request to his or her card issuing bank disputing a particular transaction. This process protects consumers and ensures that the financial institution bears ultimate responsibility for fraudulent transactions, demonstrating the industry's strong interest in making sure fraudulent actors do not gain access to payment systems.

In addition, the payments industry has a long history of fighting fraud through robust underwriting and monitoring policies and procedures, and the use of advanced authentication technologies. With the benefit of decades of expertise, ETA members have developed effective due diligence programs to prevent fraudulent actors from accessing payment systems, monitor the use of those systems, and terminate access for network participants that engage in fraud. Working with its members and industry and government stakeholders, ETA has published various guidelines that provide underwriting and diligence best practices for merchant and risk underwriting, including the "Guidelines on Merchant and ISO Underwriting and Risk Monitoring" and "Payment Facilitator Guidelines," which provide information on anti-fraud tools, security, and related issues.

ETA members are constantly developing and deploying new technology and tools to detect, deter, and eliminate fraud. Just a few examples of these efforts include the following:

- **Data Encryption.** The payments industry has introduced point-to-point encryption (P2PE) and the tokenization of data to minimize or eliminate the exposure of unencrypted data in connection with a purchase.

- **Improved Authentication.** The use of new authentication methods to verify and authenticate transactions helps minimize potentially fraudulent transactions. These new tools include the use of the following types of advanced tools:
  - biometric authentication, including the use of thumbprints, facial, and voice recognition
  - geolocation that compares the merchant's location with the location of the consumers phone
  - behavioral biometrics (e.g., monitoring keystrokes)

- **Fraud Scoring / Suspicious Activity Monitoring.** The payments industry continues to refine tools for monitoring and analyzing payment data for suspicious activity. With improvements in machine learning and artificial intelligence, the payments industry gains additional tools for identifying suspicious patterns in transaction data.

- **Chip Cards and EMV**. The payments industry has worked to replace magnetic stripes for credit and debit cards with a computer chip card, also called EMV. Chip cards make our payments system stronger by protecting against theft, counterfeit cards, and unauthorized use of cards in stores.

These are just some of the tools that the payments industry has developed in recent years to fight fraud, protect consumers, and ensure the integrity of the payments ecosystem. These efforts have been remarkably successful in reducing fraud while ensuring that consumers have access to fast, reliable, and safe payment options.

ETA Supports a Regulatory Framework that Recognizes the Efforts of Industry to Fight Fraud and Protect Privacy

ETA and its members support U.S and international regulatory efforts that encourage and respect industry efforts to combat fraud and disclose to consumers how their personal information is being used. Working together, lawmakers, regulators, and the payments industry have had remarkable success in protecting consumers and providing them with access to safe and convenient payment systems. This is achievable because the existing legal framework for protecting consumer privacy recognizes the important role of industry efforts in preventing and fighting fraud.

In the U.S., for example, laws have been passed to protect health information (HIPAA) and financial information (Gramm-Leach-Bliley Act and Fair Credit Reporting Act), and marketing activities are regulated through federal and state competition laws, as well as industry and activity

specific laws, such as the Telephone Consumer Protection Act, Telemarketing Sales Rule, and CAN-SPAM regulations. These laws recognize the important role that industry plays in combatting fraud and provide provisions that allow for the targeted use and sharing of data to protect consumers and to prevent actual or potential fraud from occurring in the first instance.

Just a few of these U.S. laws include:

Consumer Protection Laws and Provisions Related to Industry Fighting Fraud
Gramm Leach Bliley Act ("GLBA"): The GLBA requires financial institutions to explain their information-sharing practices to customers and safeguard sensitive data. The GLBA has an exception to its information-sharing restrictions for information disclosed to "protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability."[2]
Bank Secrecy Act ("BSA"): The BSA establishes various requirements for covered financial institutions to assist the government in identifying and combatting money laundering and terrorist finance. The BSA includes numerous provisions governing the sharing of information between covered financial institutions and law enforcement, as well as sharing of information between financial institutions in order to identify and report activities that may involve terrorist activity or money laundering.
Health Insurance Portability and Accountability Act of 1996 ("HIPAA"): This law provides data privacy and security provisions for safeguarding medical information. Under the HIPAA Privacy Rule, a covered entity can disclose protected health information to detect fraud, abuse, or compliance violations.
California Financial Information Privacy Act ("CFIPA"): The CFIPA governs financial institutions in California handling nonpublic personal information of the State's residents, including provisions related to consumer notice and the sharing of this personal information. The CFIPA creates an exception to its restrictions to allow sharing of consumer information with nonaffiliated third parties "to protect against or prevent actual or potential fraud, identity theft, unauthorized transactions, claims, or other liability."[3]
Federal Trade Commission ("FTC") Act: Section 5 of the FTC Act prohibits unfair or deceptive business acts or practices, including those relating to privacy and data security. The FTC has recognized the need for industry to share information in order to fight fraud. In a 2012 privacy report, the FTC identified "fraud prevention" as a category "of data practices that companies can engage in without offering consumer choice" because they are "sufficiently accepted or necessary for public policy reasons."[4]

[2] 12 C.F.R. § 1016.15(a).

[3] Cal. Fin. Code § 4056. While the CCPA does not contain an express fraud prevention exception from the substantive rights and protections in the law as a whole, for purposes of the opt-out requirement for the sale of a consumer's personal information, there is an argument that a business's disclosure of personal information to prevent fraud affecting the consumer would not amount to the "sale" of such information because the information is not being disclosed "for monetary or other valuable consideration." As discussed further in this letter, such language should indeed be clarified in the CCPA to preserve this vital consumer protection.

[4] FTC, Protecting Consumer Privacy in an Era of Rapid Change, available at https://www ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change recommendations/120326privacyreport.pdf at 36 (2012); see also id. at 39 (reaffirming this preliminary conclusion following review of public comments).

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

Consumer Protection Laws and Provisions Related to Industry Fighting Fraud
The Fair Credit Reporting Act ("FCRA"): The FCRA establishes a framework for the use and sharing of consumer reports and requires covered entities to develop and implement an identity theft prevention program. While not an explicit exemption, it has traditionally been understood that consumer information disclosed for the purposes of fraud prevention is not "consumer report information" subject to the restrictions of the FCRA.[5]
Telephone Consumer Protection Act ("TCPA"): The TCPA was designed to safeguard consumer privacy by regulating telemarketing using voice calls, text messaging, and faxes. In 2015, the Federal Communications Commission exempted from the TCPA calls from financial institutions intended to prevent fraudulent transactions, identity theft, or data breaches.[6]

Likewise, the legal frameworks in Europe and Canada respect the need for industry to share personal information in order to protect consumers from fraud. In Europe, the recently enacted General Data Protection Regulation (GDPR) recognizes the important role that industry plays in fighting fraud and expressly permits (a) "processing of personal data strictly necessary for the purposes of preventing fraud,"[7] and (b) decision-making based on profiling that is used for fraud monitoring and prevention consistent with law. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) allows for the sharing of personal information without consent if it is "made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud. . . ."[8]

As lawmakers and regulators continue to explore new ways to protect consumers, ETA and its members encourage them to collaborate with industry to ensure that new laws and regulations are appropriately tailored to address specific needs – this ensures a balance between protecting consumers and allowing industry room to innovate and develop new and beneficial security practices and fraud detection and mitigation tools.

Conclusion

The payments industry never rests. We work tirelessly to fight fraud and protect consumers, including by developing new tools and solutions to prevent, identify and fight fraud by analyzing data. Privacy laws, such as the CCPA, should recognize these goals and the important role the payments industry plays in combatting fraud. By working together, lawmakers, regulators, and

[5] This view was supported by the court's decision in Kidd v. Thomson Reuters Corp., 299 F. Supp. 3d 400 (S.D.N.Y. 2017), which concluded that Thomson Reuters was not a "consumer reporting agency" by virtue of a service that disclosed information to customers for fraud prevention purposes.

[6] See In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 et al<https://www fcc.gov/document/tcpa-omnibus-declaratory-ruling-and-order>., CG Docket No. 02-278, July 10, 2015 at ¶ 129.

[7] European Union, GDPR, Recital 47.

[8] PIPEDA, Available at https://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/118084/sc-2000-c-5 html.

ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

industry can protect consumers while providing them with access to the safest and most convenient payments system in the world.

* * *

Thank you for the opportunity to participate in the discussion on this important issue. If you have any additional questions, you can contact me or ETA Senior Vice President, Scott Talbott at [redacted]

Sincerely,

Tom Bloodworth
State Government Affairs
Electronic Transactions Association
[redacted]

From:	Monticollo, Allaire
To:	Privacy Regulations
Cc:	Signorelli, Michael A.
Subject:	Advertising Trade Associations" Joint Submission of Comments on the Revised Proposed CCPA Regulations
Date:	Tuesday, February 25, 2020 11:44:04 AM
Attachments:	Joint Ad Trade Comments on Revised Proposed CCPA Regulations.pdf

Dear Privacy Regulations Coordinator:

Please find attached joint comments from the following advertising trade associations on the content of the revised proposed regulations implementing the California Consumer Privacy Act: the Association of National Advertisers, the American Association of Advertising Agencies, the Interactive Advertising Bureau, the American Advertising Federation, and the Network Advertising Initiative.

If you have any questions, please feel free to reach out to Mike Signorelli at [redacted] or by phone at [redacted].

Best Regards,
Allie Monticollo

Allaire Monticollo, Esq. | Venable LLP
t [redacted] | f 202.344.8300
600 Massachusetts Avenue, NW, Washington, DC 20001

[redacted] | www.Venable.com

February 25, 2020

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

RE: Revised Proposed Regulations Implementing the California Consumer Privacy Act

Dear Privacy Regulations Coordinator:

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies, from small businesses to household brands, across every segment of the advertising industry. We provide the following comments to the California Office of the Attorney General ("OAG") on the content of the February 10, 2020 release of revised proposed regulations implementing the California Consumer Privacy Act ("CCPA").[1] We appreciate the opportunity to continue to engage with the OAG on the important subject of consumer privacy and the implementing regulations that will help shape privacy protections in the state of California.[2]

We and our members strongly support protecting the privacy of Californians, and we believe consumer privacy deserves meaningful protection. We are encouraged by several updates the OAG made to the CCPA implementing regulations that will enhance consumer privacy and provide more clarity for businesses in their efforts to operationalize the law's terms. However, certain specific issues, which we address below in this letter, could be further clarified to help preserve consumers' ability to exercise meaningful choice in the marketplace and businesses' ability to provide products and services that consumers expect and value. We are also concerned that the quickly impending CCPA enforcement date of July 1, 2020 will leave little to no time for businesses to implement the changes the OAG has made to the draft regulations as well as any additional updates the OAG may make to the regulations before July of this year.

The undersigned organizations' combined membership includes more than 2,500 companies, is responsible for more than 85 percent of U.S. advertising spend, and drives more than 80 percent of our nation's digital advertising spend. Locally, our members are estimated to help generate some $767.7 billion dollars for the California economy and support more than 2 million jobs in the state.[3] Our members want to provide consumers with robust privacy protections while simultaneously maintaining their ability to do business in ways that benefit California's employment rate and its economy. We believe a regulatory scheme that enables strong individual privacy protections alongside continued economic development and advancement will best serve California consumers.

---

[1] *See* California Department of Justice, *Updated Notice of Modifications to Text of Proposed Regulations and Addition of Documents and Information to Rulemaking File* (Feb. 10, 2020), located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-mod-020720.pdf?.

[2] Our organizations submitted joint comments on the content of the OAG's original proposed rules implementing the CCPA. *See Joint Advertising Trade Association Comments on California Consumer Privacy Act Regulation*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/priavcy/ccpa-public-comments.pdf at CCPA 00000431 - 00000442.

[3] IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at http://www.ana net/getfile/23045.

The requests we pose in this submission represent targeted suggestions to improve the CCPA implementing regulations for consumers and businesses alike. These comments are supplementary to filings that may be submitted separately and individually by the undersigned trade associations.

I. Afford Businesses Time to Update Their Practices in Light of Regulatory Revisions

Although the CCPA went into effect on January 1, 2020, the final regulations have not yet been promulgated, leaving our members and thousands of other California businesses uncertain concerning their ultimate compliance obligations. Given the extraordinary complexity of the law and the potential for other open issues to be clarified in subsequent updates to the draft rules, there will not be sufficient time for businesses to effectively implement the final regulations prior to the anticipated enforcement date of July 1, 2020. We therefore ask you to delay enforcement of the CCPA until January 2021 in order to provide businesses a sufficient time period to implement the new regulations before being subject to enforcement.

a. It Is Appropriate to Provide Businesses a Reasonable Period of Time to Implement the Regulatory Updates

As soon as the California Legislature passed the CCPA, it was clear that the law's requirements would evolve through both the legislative and rulemaking process. It was not clear, however, that key CCPA provisions would be substantially amended so close to its effective date, and that the rules implementing its terms would not be finalized until after the law became operative. W275-1

While we recognize that the amendments in the California Legislature delayed the development and formal release of draft regulations implementing the CCPA until October 11, 2019,[4] these draft rules presented significant new and unprecedented requirements, such as entirely new recordkeeping obligations, notice requirements, and verification rules, among many other novel obligations.[5] Then, on February 10, 2020, the rules changed again, altering the requirements businesses had used to build systems, processes, and policies for the CCPA. Businesses are contending with the proposed regulations' new mandates from both the October 11, 2019 and February 10, 2020 release of draft rules, and they are working earnestly to adjust their systems and build new processes to facilitate compliance.

Unfortunately, it is presently unclear when the rules will be finalized and whether they will be further amended. Just mere months before enforcement is scheduled to begin, companies that are subject to the CCPA are faced with the possibility that the draft rules could substantially change again and impose other entirely new requirements and nuances on businesses. If the rules change again, the OAG must issue a new notice in the California Regulatory Notice Register and provide for another comment period of 15 to 45 days.[6] The rules will not be effective until they are submitted and reviewed by the Office of Administrative Law, further reducing the time available to businesses to implement the regulations. This timeline increases the likelihood that the draft rules will not be finalized before, or only a short period prior to the law's July 1, 2020 enforcement date.

We and our members strongly support the underlying goals of the CCPA. The limited and quickly shrinking time before the existing enforcement deadline, however, will place businesses in a nearly untenable position. Without final regulatory requirements, businesses will be unable to make operational changes to their systems, further delaying finalization of their compliance programs. Businesses should be

[4] *See* State of California Office of Administrative Law, *Notice Publication/Regulations Submission* (Oct. 11, 2019), located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-std400a.pdf.
[5] Cal. Code Regs. tit. 11, § 999.305-308, 317, 323-325 (proposed Feb. 10, 2020).
[6] *See* Office of the Attorney General, California Department of Justice, *California Consumer Privacy Act (CCPA): Background on Rulemaking Process* at 3, located at https://oal.ca.gov/rulemaking_participation.

afforded an appropriate time period to implement the new regulations once they become final and before being subject to enforcement.

b. Providing a Reasonable Period of Time for Implementing the New Regulations Benefits Consumers

While the law instructs the OAG not to bring any enforcement action prior to July 1, 2020, there is no restriction on you providing a reasonable period of additional time for California businesses to review and implement the final regulations before your office initiates any enforcement actions.[7] Thus, in order to avoid consumer and business confusion with respect to the new rules, we request that you delay enforcement of the law to begin in January 2021. This short deferral will give businesses the time they need to understand and effectively operationalize the rules helping ensure consumers have access to the rights afforded under the new law. W275-1 (cont.)

Business attempts to comply with an incomplete legal regime risk causing significant consumer frustration and the implementation of inadequate or duplicative compliance tools. While we understand that your office is working expeditiously to provide clear rules for businesses to operationalize the CCPA, the clock is working against well-intentioned businesses in their compliance efforts. We urge you to give California business the opportunity to understand what is required under the law before they are at risk for being penalized for violating its terms.

While our members support California's intent to provide consumers enhanced privacy protections, the evolving nature of the CCPA and the draft nature of the proposed rules make the current enforcement date of July 1, 2020 a difficult deadline for businesses and consumers alike. Consumer privacy is best served when businesses that leverage data do so in accordance with clear and concrete laws and regulations that present them with adequate time to adjust their practices to come into compliance with new requirements.

We urge you to provide a moratorium on enforcement until January 2021, thereby giving businesses throughout the United States that operate in California adequate time to prepare to adhere to the law's final form. Delaying the CCPA's enforcement in this manner will help ensure that businesses can effectively provide consumers with the new protections and rights that the law and its implementing regulations require.

II. Enable Consumer Choice By Removing the Requirement to Honor Browser Settings and Global Privacy Controls

The revised proposed rules require businesses that collect personal information from consumers online to treat user-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism that signals the consumer's choice to opt out of the sale of personal information, as a valid request submitted for that browser, device, or consumer.[8] In our prior submission to the OAG, we explained that this requirement robs consumers of the ability to exercise granular choice. This mandate would obstruct consumers' individualized, business-by-business decisions about entities that can and cannot engage in the sale of personal information. Moreover, this requirement represents an obligation that has no support in the text of the CCPA itself and extends far beyond the likely intent of the California Legislature in passing the law. For these reasons, we renew our request for the OAG to remove the requirement to respect user-enabled global privacy controls, or, at a minimum, to give businesses the W275-2

[7] Cal. Civ. Code § 1798.185(c).
[8] Cal Code Regs. tit. 11, § 999.315(d) (proposed Feb. 10, 2020).

option to honor user-enabled global privacy controls or decline to honor such settings if the business offers another, equally effective method for consumers to opt out of personal information sale.

The requirement to honor user-enabled global privacy controls is a substantive obligation that the California Legislature did not include in the text of the CCPA itself. Despite numerous amendments the legislature passed to refine the CCPA, none of them included a mandate to honor browser signals or global privacy controls. Additionally, the California Legislature considered a similar requirement in 2013 when it amended the California Online Privacy Protection Act, but it declined to impose a single, technical-based solution to address consumer choice and instead elected to offer consumers multiple ways to communicate their preferences to businesses.[9] The revised proposed rules' imposition of a requirement to honor user-enabled privacy controls would result in broadcasting a single signal to all businesses opting a consumer out from the entire data marketplace. This requirement would obstruct consumers' access to various products, services, and content that they enjoy and expect to receive.

Additionally, requiring businesses to honor global, single-signal privacy control opt out choices would effectively convert the CCPA's statutorily mandated opt out regime to an opt in regime. Because businesses would be required to respect a user-enabled global privacy control opt out setting under the draft rules, they would be forced to approach consumers on an individualized basis to ask them to opt in to personal information sale after receiving a user-enabled global privacy setting opt out through a browser. This outcome is certainly not the result the California Legislature intended in passing the CCPA, which clearly proposes an opt out approach to consumer data sales rather than an opt in approach.[10] W275-2 (cont.)

In the most recent iteration of the draft rules, the OAG added provisions to the requirement that allow a business to notify a consumer of a conflict between any business-specific privacy setting or financial incentive and a global privacy control.[11] According to the updated regulations, a business may give the consumer a choice to confirm the business-specific setting or the global privacy control.[12] However, the draft rules still require a business to "respect the global privacy control," thereby forcing businesses to act on global privacy settings before they can confirm whether the consumer actually wanted to make a choice to end beneficial transfers of data that occur via the Internet.[13] This option, therefore, does nothing to further a consumer's actual desired or expressed choices. The fact that the rules now allow for a business to confirm a consumer's intentions does little to save the consumer from unintentionally losing access to various products, services, and valuable content through the Internet. Additionally, this provision stands to advantage certain players in the market that have a direct relationship with consumers. Businesses that do not directly interact with consumers online, such as third-party entities, would not have the ability to confirm whether a consumer intended to apply a browser signal or privacy setting to the entire Internet or whether the consumer would rather abide by the choice the consumer made with respect to that particular business.

The revised proposed rules also note that a privacy control "shall require that the consumer affirmatively select their choice to opt-out and shall not be designed with any pre-selected settings."[14] Although this new provision reduces the potential for default settings to miscommunicate consumers' actual preferences, it does not address the fact that intermediaries in the online ecosystem stand between consumers and businesses and have the ability to interfere with the data-related selections consumers may make through technological choice tools. Obligating businesses to honor user-enabled privacy settings

[9] *See* AB 370 (Cal. 2013).
[10] Cal. Civ. Code § 1798.120.
[11] Cal. Code Regs. tit. 11, § 999.315(d)(2) (proposed Feb. 10, 2020).
[12] *Id*.
[13] *Id*.
[14] *Id*. at § 999.315(d)(2).

that are presented to consumers through an intermediary vests power in the hands of the intermediary and risks inhibiting consumers' ability to communicate preferences directly to particular businesses. It also makes intermediary meddling in consumers' expressed privacy choices harder to detect, especially if a consumer makes a choice directly with a business that conflicts with a global opt-out signal set by a browser.

To preserve consumers' ability to exercise granular choices in the marketplace, to keep the regulations' requirements in line with legislative intent in passing the CCPA, and to reduce entrenchment of intermediaries and browsers that have the ability to exercise control over user-enabled privacy settings, we ask the OAG to remove the requirement to honor user-enabled privacy controls. Alternatively, we ask the OAG to update the draft rules so a business may *either* honor user-enabled privacy controls or decline to honor such settings *if* the business provides another equally effective method for consumers to opt out of personal information sale, such as a "Do Not Sell My Personal Information" link.

W275-2 (cont.)

III. Clarify Financial Incentive Terms So Californians May Continue to Benefit from Consumer Loyalty Programs

The OAG did not take steps to materially clarify the draft rules' financial incentive requirements in its revisions to the proposed regulations. Without additional clarity on this issue, loyalty programs offered in California could be significantly undermined due to business confusion regarding how to implement the regulatory mandates. We respectfully ask the OAG to clarify or remove the rules' ambiguous terms requiring businesses to ensure that financial incentives are reasonably related to the value of a consumer's data. We also ask the OAG to clarify or remove the requirement to disclose an estimate of the value of the consumer's data as well as the method of calculating such value in a notice of financial incentive.

According to the revised proposed rules, "[i]f a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference."[15] Despite this mandate, the draft rules do not provide any helpful information regarding how a business may justify that a price or service difference is reasonably related to the value of a consumer's data. The revised proposed regulations also do not address how businesses may reasonably quantify nontangible value in terms of fostering consumer loyalty and goodwill.

W275-3

Californians greatly benefit from loyalty and rewards programs and the price differences and discounts they receive for participating in those programs. Loyalty programs exist due to consumers' widespread participation in such programs. Without consumer data, loyalty programs would not be possible. Consumer data increases businesses' access to useful information as well as their ability to generate revenue by marketing their products and services. Allowing consumers to continue to participate in loyalty programs without providing personal information to the business would defeat the purposes of the programs. Consumers who opt out or delete personal information from the loyalty program would essentially be permitted a "free ride" on the program, reaping all of its benefits due to data provided by other consumers. Additionally, it is not immediately apparent how any business can ensure that the program is "reasonably related to the value of the consumer's data." The lack of clarity on this issue and the "free rider" problem enabled by the draft regulations could cause many businesses to decline to continue offering loyalty programs to California residents.

Moreover, the requirement to disclose an estimate of the value of the consumer's data as well as the method of calculating such value in a notice of financial incentive represents a particularly onerous

W275-4

[15] *Id*. at § 999.336(b).

requirement that would engender consumer confusion and could have anticompetitive effects.[16] Businesses typically offer multiple discounts to consumers through loyalty programs at one time. Requiring businesses to disclose an estimate of the value of the consumer's data and the method of calculating such value would inundate and confuse consumers with multiple and potentially duplicative privacy notices and would provide no tangible consumer benefit. Additionally, disclosing such information in a privacy notice could reveal confidential information about a business and pose risks to the business's competitive position in the market. Forcing businesses to reveal internal and proprietary valuations of data could negatively impact competition and could impose significant risks to business proprietary information.

W275-4 (cont.)

For the foregoing reasons, we respectfully ask the CA AG to clarify or remove the unreasonably onerous financial incentive requirements inherent in the revised rules. In particular, we ask the OAG to clarify or remove the provisions requiring businesses to disclose a good faith estimate of the value of the consumer's data, disclose their methods of calculating such value, and ensure that financial incentives offered through loyalty programs are reasonably related to the value of the consumer's data. These requirements are particularly unclear and therefore could be impossible to operationalize. Without additional clarity, the draft rules' financial incentive terms could inhibit or drastically reduce the availability of loyalty programs offered in the state.

* * *

Thank you for the opportunity to submit input on the content of the revised proposed regulations implementing the CCPA. We look forward to continuing to engage with the OAG as it takes steps to finalize the draft rules. Please contact Mike Signorelli of Venable LLP at [redacted] with any questions you may have regarding these comments.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers

Alison Pepper
Senior Vice President
American Association of Advertising Agencies, 4A's

Christopher Oswald
SVP, Government Relations
Association of National Advertisers

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau

David LeDuc
Vice President, Public Policy
Network Advertising Initiative

Clark Rector
Executive VP-Government Affairs
American Advertising Federation

[16] *Id*. at § 999.307(b)(5).

From: Gibbons, Jennifer
To: Privacy Regulations
Cc: Desmond, Edward; Leigh Moyers; Sheila Millar, Esq.; Pasierb, Stephen
Subject: CCPA Revised Regulations -- Toy Association Comments February 2020
Date: Tuesday, February 25, 2020 11:03:25 AM
Attachments: image001.png
image004.png
image013.png
image015.png
image016.png
image017.png
image018.png
image003.png
image005.png
image006.png
TA Comments to CA AG on Revised CCPA Regulations_022520.pdf

Hello,

Attached, please find comments from the Toy Association, on behalf of its members, regarding the revised regulations related to the California Consumer Privacy Act (CCPA).

By way of background, The Toy Association represents more than 1,100 businesses – toy manufacturers, importers and retailers, as well as toy inventors, designers and testing labs – all involved in bringing safe, fun and educational toys and games for children to market. The Toy Association and its members work with government officials, consumer groups, and industry leaders on ongoing programs to ensure safe play, both online and offline.

The toy industry is deeply committed to privacy, security and product safety, and supports strong and effective standards to protect consumers. We support principles of transparency, notice, consumer choice, access, correction and deletion rights for consumers, and reasonable security, all part of the objectives of the CCPA.

Please feel free to contact us with any questions, or if additional information regarding our comments is needed.

Best,
Jennifer

the toy association™
Inspiring Generations of Play

Jennifer Gibbons
Vice President, State Government Affairs

1375 Broadway, Suite 1001 • New York, NY 10018
c. [redacted]
f. 202.459.0440
e. [redacted] • w. www.toyassociation.org

Follow us on:

1200 G Street NW • Suite 200 • Washington, DC 20005
t. 202.459.0354 • e. info@toyassociation.org

February 24, 2020

Via Electronic Submission: privacyregulations@doj.ca.gov

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

Re: Comments on Revised Proposed Regulations Under the CCPA

Dear Attorney General Xavier Becerra:

The Toy Association, Inc. (TTA), on behalf of its members is pleased to respond to the Attorney General's request for input from stakeholders on the updated Proposed Text of the Revised California Consumer Privacy Act Regulations (Proposed Regulations) implementing the California Consumer Privacy Act (CCPA) (Cal. Civ. Code §§ 1798.100–1798.199). TTA appreciates the changes made to these Proposed Regulations that address several of the concerns it expressed in its comments on the initial draft of the Proposed Regulations. As we indicated in our earlier comments, TTA represents more than 1,100 businesses – toy manufacturers, importers and retailers, as well as toy inventors, designers and testing labs – all involved in bringing safe, fun and educational toys and games for children to market. The U.S. toy industry contributes an annual positive economic impact of $109.2 billion to the U.S. economy. TTA and its members work with government officials, consumer groups, and industry leaders on ongoing programs to ensure safe play, both online and offline. We incorporate our prior comments herein by reference.

The revised Proposed Regulations respond to some, but not all, of the operational problems with implementing the CCPA and the conflicts between the CCPA and the Children's Online Privacy Protection Act (COPPA).These comments focus principally on how to further align the Proposed Regulations with COPPA and improve the ability of affected companies to operationalize the CCPA requirements.

- We are pleased that the Proposed Regulations provide for some exceptions for Service Providers' use of Personal Information for "support for internal operations." This is important for businesses engaging with children, teens and adults alike. The proposed revised rule could be further improved by mirroring language in the COPPA Rule and Preamble on activities that constitute support for internal operations. In developing that concept, with related rule and interpretive language, the FTC struck a careful balance between protecting children's privacy and allowing for important business activities, including improved products and services and innovation.

W276-1

- We encourage further revisions to the Proposed Regulations to account for potential new methods of verifying parental consent that might be recognized by the Federal Trade Commission (FTC) in accordance with COPPA. W276-2
- COPPA specifies that only parents may make requests to access, update and delete a child's personal information. Changes to the Proposed Regulations attempt to address this conflict, but we recommend further modification to explicitly limit requests to access or delete personal information of a child under the age of 13 to an individual who is reasonably determined to be the parent or guardian rather than any "authorized agent." W276-3
- We appreciate the modifications to the Proposed Regulations that seek to address the thorny issue of requests to access or delete household information that includes information supplied by a child under the age of 13. As a practical matter, however, requiring a business to verify each household member could impose undue burdens on parents in a manner inconsistent with COPPA. Provision should be made to assure that parents can readily access or delete household information regarding their children without obligating them to separately make a request for each child. W276-4
- The regulations should formally recognize that a participant in an approved COPPA Safe Harbor organization that adheres to the organization's guidance and requirements is entitled to safe harbor treatment under the CCPA as well as COPPA with regard to its handling of children's data. W276-5

I. TTA Welcomes Changes to the Proposed Regulations that Resolve Some Conflicts with COPPA

TTA's Comments on the initial draft of the Proposed Regulations pointed out several areas where the Proposed Regulations created conflicts with COPPA. TTA was pleased to see changes to the Proposed Regulations that address some of these conflicts, and thanks the Attorney General for its positive consideration of TTA's previous comments.

TTA had noted, for example, that the Proposed Regulations governing non-discrimination conflicted with COPPA. 16 C.F.R.§312.6(c). New language in § 999.336(g) clarifies that differences in price or service that are "the direct result of compliance with federal law shall not be considered discriminatory." W276-6

TTA also noted that the broad definitions of "sale" and "personal information" in the CCPA and Proposed Regulations created potential conflicts with COPPA. TTA was pleased to see the new language in § 999.302 establishing that "personal information" does not include, for example, IP addresses that a business collects from visitors to its website but cannot reasonably link to any particular consumer or household information. TTA understands this exception to include a business's use of an IP address or device identifier to provide customized experiences to repeat visitors to websites, where this is done without linking the IP address to any other personal or household information, as is permitted by COPPA. IP addresses or device identifiers can be used in this fashion, for example, when children publicly post an "alias" to track and compare game scores anonymously. Indeed, the FTC recognizes this to offer a privacy-safe experience to children that allows them to engage in social interactions without exchanging any "personal" information, and is widely used. W276-7

II. Exceptions for Use or Disclosure of Personal Information to Support Internal Operations of Services Providers

TTA welcomes the Attorney General's efforts to craft language that clarifies that service providers may use personal information for certain internal uses, like improving services, and that such use would not be considered a "sale" under CCPA. The proposed changes to § 999.314 allow service providers to use or disclose personal information for certain reasons, including "internal use" in some circumstances. We encourage the Attorney General, however, to align excluded activities with the approach to the "support for internal operations" exception adopted by the FTC when it updated the COPPA rule in 2013. Under 16 CFR §312.2, support for internal operations means those activities necessary to:

W276-1 (cont.)

(a) maintain or analyze the functioning of the website or online service;

(b) perform network communications;

(c) authenticate users of, or personalize the content on, the website or online service;

(d) serve contextual advertising on the website or online service or cap the frequency of advertising;

(e) protect the security or integrity of the user, website, or online service; [and]

(f) ensure legal or regulatory compliance.

When it updated the COPPA Rule in 2013, the FTC also specified that support for internal operations also includes activities such as intellectual property protection, payment and delivery functions, spam protection, optimization, statistical reporting, or de-bugging, expressly stating that it did not need to update Rule language for these activities to be covered. *See* 78 Fed. Reg. at 3,980 - 3,981. These activities are crucial to business operations. Because the FTC viewed these activities to be consistent with the above rule language, necessary to business operations, and not privacy-invasive, it concluded that there was no need to modify the Rule to explicitly include these additional examples.

Since the COPPA rule went into effect, companies have relied on this exclusion to conduct business-critical activities in a privacy-safe way. To ensure consistency with COPPA, TTA recommends that the Attorney General track the exceptions for internal use under the COPPA Rule and clarify that the essential business activities described in the 2013 COPPA Rule Preamble (78 Fed. Reg. 3,972 at 3,981 (Jan. 17, 2013)) are also covered.

III. Approved Methods to Verify Parental Consent are too Limited

The Proposed Rules require verifiable parental consent to the sale of the personal information of children under age 13. The methods outlined in 999.330(a)(2) include methods recognized under the COPPA Rule as reasonably designed to assure that the individual providing consent is the child's parent or guardian. The amendments to the Proposed Regulations open the door to alternative methods by specifying that the list is not exclusive. While this change is helpful, it does not fully remove regulatory uncertainty for businesses that utilize alternative methods that comply with COPPA. To help resolve this uncertainty, TTA recommends that the Proposed Regulations be modified to explicitly permit the automatic use of other methods for

W276-2 (cont.)

verifying parental consent recognized by the FTC or by authorized COPPA safe harbor organizations under the process outlined in the COPPA Rule at 16 C.F.R. § 312.5(b)(3).

W276-2 (cont.)

IV. Only Parents or Guardians May Request Access to or Deletion of Children's Personal Information

Under the CCPA and Proposed Regulations, a business must honor consumers' requests to access, delete, or opt-out of the "sale" of their personal information made through a properly designated "authorized agent." In contrast, requests to access and delete children's information under COPPA must be submitted by the parent, and the operator must take steps to verify that the requestor *is actually the parent*. The changes to the Proposed Regulations still do not resolve this direct conflict between COPPA and the CCPA.

W276-3 (cont.)

The Proposed Regulations now include a new § 999.330(c) which establishes approved methods for "determining whether a person submitting a request to know or a request to delete the personal information of a child under the age of 13 is the parent or guardian of the child," but does not *require* that the person submitting the request be a parent or guardian. To resolve this conflict with COPPA, we urge the Attorney General to amend §999.300(c) to explicitly state that only parents or guardians may make a request to access or delete the personal information of a child under the age of 13.

V. Procedures for Processing Requests Relating to Household Information Unduly Burden Parents

Changes to § 999.322 strengthen the protection of individual household members when a business receives a request to access or delete household information. Crucially, the Proposed Regulations now require verified parental consent when household information includes personal information of children under the age of 13, which addresses concerns raised by TTA in its previous comments, but only in part. TTA members often deal with parents who create a "Parent Account" to help them monitor children's activities, and to set permission levels for various activities. Unfortunately, these new procedures could unduly burden parents when a household includes a child under age 13, and especially when a household includes more than one such child. As written, the proposed procedures could require parents who ask a business to delete an account linked to multiple children to submit multiple requests or verifications, for themselves as members of the household as well as for each individual child under the age of 13. In keeping with COPPA's admonishment that operators avoid undue burdens to parents, TTA recommends that § 999.322 be modified to clarify that a single request from a verified parent or guardian is sufficient to verify and act on requests covering every child under 13 in the household.

W276-4 (cont.)

VI. The Rules Should Recognize COPPA Safe Harbor Organizations to Assist with CCPA Compliance efforts

Many members of TTA have developed relationships over time with what are called Safe Harbor organizations under COPPA. *See* 16 C.F.R. § 312.11. Administered pursuant to FTC rulemaking, Safe Harbor organizations advise participating COPPA-covered entities on the

W276-5 (cont.)

requirements of COPPA. Section 312.11(g) of the COPPA Rule specifies: "An operator will be deemed to be in compliance with the requirements of §§312.2 through 312.8, and 312.10 [of the COPPA Rule] if that operator complies with Commission-approved safe harbor program guidelines." The COPPA legislative framework not only encourages and rewards COPPA compliance, but is designed to aid in the FTC's enforcement effort. Safe Harbor organizations and their participants can develop innovative ideas for parental consent options and highlight for businesses and regulators new trends in both marketing and technology. Although there may be room for more generally under the CCPA regime to provide guidance for CCPA compliance, TTA suggests that the regulations formally acknowledge that companies participating in a recognized COPPA Safe Harbor organization also receive a safe harbor against sanctions for violation of the CCPA. It goes without saying that to receive safe harbor treatment, the participant must have followed guidance from its Safe Harbor organization in its handling of data from children under 13, including measures to respond to parental requests to access, correct or delete children's data.

W276-5
(cont.)

Conclusion

The toy industry supports strong national consumer privacy and safety frameworks. We hope this submittal will assist the Attorney General as it finalizes the regulations under the CCPA. Please contact Ed Desmond at [redacted] or Jennifer Gibbons at [redacted] if you would like additional information on our industry's perspective.

Sincerely,

Steve Pasierb
President & CEO

cc: Sheila A. Millar, Of Counsel

From: Dan Jaffe
To: Privacy Regulations
Subject: ANA Comments on Proposed CCPA Regulations
Date: Tuesday, February 25, 2020 11:01:03 AM
Attachments: ANA Comments on Revised Proposed CCPA Regulations.pdf

---

Attached are the Association of National Advertisers' comments in regard to the proposed regulations. If you have any questions, please feel free to contact me.

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
2020 K Street N.W. Suite 660
Washington DC 20006

[redacted] office
cell

Visit my Regulatory Rumblings Blog

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

COMMENTS

of the

ASSOCIATION OF NATIONAL ADVERTISERS

on the

California Consumer Privacy Act Revised Proposed Regulations

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
2020 K Street, NW
Suite 660
Washington, DC 20006
202.296.1883

Counsel:
Stu Ingis
Mike Signorelli
Tara Potashnik
Allaire Monticollo
Venable LLP
600 Massachusetts Ave., NW
Washington, DC 20001
202.344.4613

February 25, 2020

On behalf of the Association of National Advertisers ("ANA"), we offer the following comments in response to the California Office of the Attorney General's ("CA AG") February 10, 2020 request for public comment on the revised proposed regulations implementing the California Consumer Privacy Act (the "CCPA").[1] We appreciate the opportunity to continue to engage with the CA AG on the important subject of consumer privacy and the content of the rules that will help implement the CCPA.

ANA is the advertising industry's oldest and largest trade association. ANA's membership includes nearly 2,000 companies, marketing solutions providers, charities and nonprofits, with 25,000 brands that engage almost 150,000 industry professionals and collectively spend or support more than $400 billion in marketing and advertising annually. Nearly every advertisement you'll see in print, online, or on TV is connected in some way to ANA members' activities. A significant portion of our membership is either headquartered or does substantial business in California.

ANA has closely followed the development of the CCPA through the legislative and regulatory process and has thoughtfully considered the impact the regulatory scheme will have on consumers and businesses. ANA participated in the CA AG's preliminary CCPA rulemaking forums in San Marcos on January 14, 2019 and Sacramento on February 2, 2019, and ANA submitted comments to the CA AG during the pre-rulemaking stage.[2] ANA also testified at a February 20, 2019 informational hearing on the CCPA held by the California State Assembly Committee on Privacy and Consumer Protection. In addition, ANA participated in the CA AG's December 4, 2019 San Francisco public hearing to offer input on the initial draft of proposed regulations implementing the CCPA, and ANA submitted written comments to the CA AG in response to the October 11, 2019 request for comment.[3]

We and our members strongly support the responsible use of data and the underlying goal of enhancing consumer privacy that is inherent in the CCPA and its implementing regulations. We are encouraged that the updated rules provide a degree of enhanced clarity surrounding some ambiguous provisions in the law. Nevertheless, the regulations remain significantly unclear in several areas of vital importance to both consumers and businesses.

The CCPA is a novel, operationally complex, and, in many ways, confusing law. The impending enforcement date of July 1, 2020 and the lack of final requirements for entities to implement make matters even more complicated and burdensome for businesses that are earnestly trying to develop processes to facilitate compliance with the CCPA. It is essential that the CA AG continue to work to provide more clarity to help ensure that consumers are given effective privacy protections and that businesses are equipped to structure systems and practices to offer those protections to consumers.

---

[1] California Department of Justice, *Updated Notice of Modifications to Text of Proposed Regulations and Addition of Documents and Information to Rulemaking File* (Feb. 10, 2020), located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-mod-020720.pdf?.

[2] *See* ANA, *California Consumer Privacy Act Regulation*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf at CCPA00000432 – 00000442.

[3] *See Comments of the Association of National Advertisers on the California Consumer Privacy Act Proposed Regulations*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-comments-45day-pt2.pdf at CCPA_45DAY_00317 – 00342.

All of the topics we raise in the forthcoming comments represent issues that could have significant and detrimental impacts on consumers and businesses if they are not clarified by the CA AG. These issues, for example, could hinder consumers' ability to access programs, products, and services they enjoy and expect; thwart consumers' ability to make specific choices about entities' use of data in the marketplace; and impede the development of digestible and understandable privacy notices that appropriately inform consumers of business data practices. Moreover, the implementing regulations, as currently drafted, could impose significant costs on businesses and have a damaging impact on the California economy. We urge the CA AG to carefully consider the issues we address in these comments and to update the draft rules so they enhance consumer privacy and provide more clarity for businesses.

Our comments proceed by first addressing three issues of particular importance that we raised in prior submissions to the CA AG:

I. Provide Businesses a Reasonable Period of Time to Implement the New Regulations
II. Clarify Requirements Surrounding Loyalty Programs So Businesses May Continue to Offer Such Programs to Californians
III. Clarify that Businesses May Choose to Honor User-Enabled Global Privacy Controls *or* Provide Consumers Another, Equally Effective Method for Opting Out of Personal Information Sale

Next, we discuss other important issues that are created by certain provisions in the revised proposed regulations:

IV. Update the Household Definition to Better Reflect Appropriate Business Practices
V. Add a Provision Clarifying that Information Businesses Collect, Use, and Share for Fraud Prevention Purposes is Not Subject to Certain CCPA Rights
VI. Enable Flexibility for Providing the CCPA-Required Notice at Collection to Consumers Through the Telephone and in Person
VII. Remove New Duplicative and Unclear Transparency Requirements
VIII. Remove the Limitation on Service Providers' Internal Use of Personal Information

Finally, we reassert certain issues that we discussed in our initial comment submission to the CA AG on the content of the original proposed regulations. These issues remain unclear in the revised proposed rules and should be clarified by the CA AG issuing revisions to the proposed regulations:

IX. Clarify the Requirement to Obtain Parental Consent for Minors "in addition to" Verifiable Parental Consent Under the Children's Online Privacy Protection Act ("COPPA")
X. Remove the Requirement to "Permanently and Completely" Erase Personal Information
XI. Remove the Requirement to Provide a General Toll-Free Contact Number to Receive Consumer CCPA Requests

I. Provide Businesses a Reasonable Period of Time to Implement the New Regulations

Our members have taken significant steps to create policies, processes, and procedures to facilitate compliance with the CCPA. Although the law became effective on January 1, 2020, the lack of finalized regulations to implement the CCPA has left our members and thousands of other California businesses uncertain concerning their ultimate compliance obligations. Additionally, changes to the regulatory scheme so close to the law's enforcement date of July 1, 2020 could facilitate the creation of differing compliance processes and tools, which would confuse and frustrate consumers in their efforts to submit rights requests under the law. We therefore respectfully ask the CA AG to delay enforcement of the CCPA until January 2021 so entities that do business in California have enough time to implement the final rules' requirements to provide consumers with consistent and effective mechanisms for exercising their new rights under the law. W277-1

It is presently unclear when the draft rules will be finalized and whether they will be further amended. Just months before enforcement is scheduled to begin, companies that are subject to the CCPA are faced with the possibility that the draft rules could change from their present form for a second time and impose other entirely new requirements. If the rules are updated again, the ensuing public comment period of 15 or 45 days will further delay the finalization of the rules. Moreover, the rules will not be effective until they are submitted and reviewed by the California Office of Administrative Law, further reducing the time available to businesses to implement the final regulations. This timeline increases the likelihood that the draft rules will not be finalized before, or only a short period prior, to the law's July 1, 2020 enforcement date.

The CCPA is a novel and operationally complex legal regime that has already caused businesses across the country to incur significant costs to fulfill the consumer rights created by the law. Additionally, business attempts to comply with an incomplete legal regime risk causing significant consumer frustration and the implementation of inadequate or duplicative compliance tools. Furthermore, the most recent February 10, 2020 updates to the implementing regulations added additional content to the legal regime that businesses will need to consider and build into the processes they have already created for the CCPA.

While the statute itself instructs the CA AG to refrain from bringing an enforcement action before July 1, 2020, the office is not restricted from providing an additional reasonable period of time for California businesses to review and implement the final rules before enforcement begins. In order to avoid consumer frustration and business confusion with respect to the updated regulations, we request that you delay the enforcement of the law to begin in January 2021. This short forbearance will give businesses the time they need to comprehend and effectively implement the rules to help ensure consumers may appropriately benefit from the rights afforded under the CCPA.

II. Clarify Requirements Surrounding Loyalty Programs So Businesses May Continue to Offer Such Programs to Californians

The revised proposed regulations still contain significant and onerous requirements surrounding financial incentives that could threaten the viability of loyalty programs offered to California consumers. Specifically, the revised proposed regulations state that a business may offer a price or service difference to a consumer only if it is reasonably related to the value of the consumer's data.[4] According to the revised proposed rules, "[i]f a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference."[5] Additionally, businesses must disclose this good faith estimate of the value of the consumer's data and the method of computing such value in a notice of financial incentive.[6]

The draft rules do not provide any guidance regarding how a business may justify that a price or service difference offered through a loyalty program is reasonably related to the value of a consumer's data. The revised proposed regulations do not account for how businesses should quantify nontangible value in terms of fostering consumer loyalty and goodwill. In addition, the method by which a business values personal information associated with a consumer may vary situationally. For instance, it may depend on the discount being offered at a particular time or in a particular place. The actual value the business attributes to such data may, in many instances, be difficult or impossible to quantify. W277-2

From grocery rewards programs to beauty store points and drugstore cash back benefits to sandwich punch cards, consumers regularly and enthusiastically participate in vast and varied loyalty programs offered by brands and marketers. These programs enable consumers to receive more tailored offers and better prices for the goods and services they regularly receive. Businesses gain from the loyalty and brand trust they receive from consumers through their participation in these programs. Californians greatly benefit from loyalty and rewards programs and the price differences and discounts they receive for participating in those programs. Moreover, they expect to receive and participate in those programs alongside the rest of the American public. The revised regulations, as currently drafted, would significantly undermine loyalty programs in California and could very well force businesses to stop offering the programs in the state.

Making matters even more confusing is that businesses very regularly offer numerous price or service differences to consumers through loyalty and rewards programs at one time. For example, a coffee shop may offer participating loyalty program customers a punch card that gives the consumer a free coffee after the fifth punch on the card (representing a purchase of five coffees). The coffee shop may simultaneously offer 5% discounts on pastries purchased in the shop through the store's mobile application. If the "value of the consumer's data" does remain a constant number, it is unclear how the business may show that both incentives are reasonably related to the value of the consumer's data. The draft rules remain ambiguous on this point and

[4] Cal. Code Regs. tit. 11, § 999.336(b) (proposed Feb. 10, 2020).
[5] *Id.*
[6] *Id.* at § 999.307(d).

could therefore threaten to diminish loyalty programs in California due to business uncertainty in how to implement the proposed regulations' mandates.

The revised proposed rules still require businesses to disclose a good faith estimate of the value of the consumer's data and the method of calculating such value in a notice of financial incentive.[7] As ANA noted in its prior comment submission, requiring this information to be included in a consumer notice could reveal confidential information about a business that could jeopardize its competitive position in the market. Forcing businesses to reveal their proprietary, internal calculations and valuations in this fashion could have a negative impact on competition and pose significant risks to business proprietary information. Additionally, this valuation information and even the estimated value itself will be meaningless to consumers. A single business may offer several financial incentives to consumers through loyalty programs. Requiring businesses to make disclosures about their valuation methods and provide actual estimated values of consumer data for each financial incentive offered would overwhelm and inundate consumers with far too many notices without achieving the goal of providing meaningful information about business practices.

W277-2 (cont.)

We respectfully ask the CA AG to clarify or remove the unreasonably onerous financial incentive requirements inherent in the revised rules, particularly the provisions requiring businesses to disclose a good faith estimate of the value of the consumer's data, disclose their methods of calculating such value, and ensure that financial incentives offered through loyalty programs are reasonably related to the value of the consumer's data. These provisions are exceedingly burdensome if not impossible to operationalize, and, if left unchanged, could have a chilling effect on the availability of loyalty programs offered in the state.

III. Clarify that Businesses May Choose to Honor User-Enabled Global Privacy Controls *or* Provide Consumers Another, Equally Effective Method for Opting Out of Personal Information Sale

The revised proposed regulations would require a business that collects personal information from consumers online to "treat user-enabled global privacy controls, such as a browser plugin or privacy setting, device 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…."[8] The requirement to honor browser signals and user-enabled privacy controls is not present in the text of the CCPA itself and exceeds the scope of the law. Consequently, businesses have had no ability to anticipate or prepare for this new obligation. In addition, because global privacy controls cast a single opt out signal to every business across the entire Internet ecosystem, the draft rules threaten to hinder consumers' ability to make specific, business-by-business choices about which entities can and cannot sell personal information. We ask the CA AG to clarify that businesses have the choice to honor user-enabled global privacy controls *or* provide consumers with another, equally effective method of opting out of personal information sale.

W277-3

[7] *Id*. at § 999.307(b)(5).
[8] *Id*. at § 999.315(d).

In our prior comment submission, we explained that the unprecedented browser signal requirement certainly does not further the purposes of the law. In fact, the requirement to honor user-enabled privacy settings would thwart the informed and granular consumer choice that the CCPA endeavors to provide to California consumers. In the past, the California legislature considered global privacy controls and elected to refrain from enshrining them in law.[9] Requiring such settings to be honored now, therefore, would not be in line with legislative intent in passing the CCPA. Such a requirement would also be ripe for intermediary tampering with no way for businesses to authenticate whether a signal is a genuine consumer set preference. Intermediaries can inject signals into the marketplace and are able to change settings that may not accurately reflect a consumer's wishes. This capability has the potential to obstruct consumers' expressed choices. Furthermore, entities such as browsers and others can block the individualized signals set by consumers with various businesses. As noted in our prior submission, intermediaries are interfering with businesses using cookies, plugins, JavaScript and other technologies to maintain consumer preferences. Without preventing such interference, consumer preferences and choices cannot be respected.

W277-3 (cont.)

Mandating that businesses honor user-enabled global privacy settings could have the unintended result of turning the CCPA's opt out regime into an opt in regime. After receiving a global privacy setting opt out signal, businesses would have no choice but to contact consumers on an individual by individual basis to see if they would like to opt in to sales of personal information to continue receiving the products and services they expect. In passing the CCPA, the California legislature set forth an opt out right to sales of personal information.[10] It was not the aim of the legislature to require consumers to opt in to every business's sale of personal information associated with them. As such, the user-enabled privacy control requirement would have the effect of thwarting legislative intent. Moreover, the draft rules do not clarify how businesses should operationalize consumers' subsequent requests to opt in to sales of personal information after a global privacy setting has been set. Browser-based global privacy settings would continue to broadcast opt out signals to businesses across the Internet in direct violation of the express opt in choice a consumer made with respect to a particular business. The regulations would limit a business's ability to seek "opt in" consent to once every twelve months. It is not clear how this restriction would affect the ability of companies to communicate with consumers in regard to these choices. The lack of clarity on this issue will likely hinder consumers' ability to make choices in the marketplace about data associated with them.

Although the CA AG's updates to the draft rules allow businesses to inform consumers if a global privacy control conflicts with a consumer's existing business-specific privacy setting and give the consumer the ability to indicate their intentions, this change does not fix the practical, consumer choice issues that are inherent in the requirement. This new term gives an advantage to certain businesses over others, particularly businesses that have a direct relationship with consumers through which they may confirm a consumer's choices. Certain entities who do not have a direct touchpoint with consumers will not have the ability to surface a notice to consumers asking if they intended to opt out of personal information sale. Additionally, as the revised proposed rules are presently drafted, businesses *must* treat user-enabled privacy controls as a valid request to opt out of personal information sale. Consequently, any subsequent

[9] *See* AB 370 (Cal. 2013).
[10] Cal. Civ. Code § 1798.120.

clarification the business receives from a consumer about their intentions to opt out would be too little too late; the business would have to honor the global privacy control, which would result in the consumer's loss of any number of products and services, as well as access to valuable content online. If the consumer did not intend to make such a selection, the business would not be able to reverse the effects of the opt out after complying with the mandated global privacy control.

A better approach to user-enabled privacy settings would be to adopt a rule allowing businesses that sell personal information to *either* (1) honor user-enabled privacy controls as valid requests to opt out, *or* (2) offer another effective mechanism for the consumer to submit a request to opt out, such as a "Do Not Sell My Info" link and an interactive form that enables the consumer to opt out of personal information sale. This approach would provide consumers with the ability to express individualized choices about particular entities' use of data. Updating the draft rules in this fashion would place the power and control back where it should be in the hands of consumers instead of concentrating it in the intermediary or browser that controls the global privacy control or setting. There is no privacy-enhancing reason to require businesses to respect user-enabled privacy controls over choice provided by a business.

W277-3 (cont.)

IV. Update the Household Definition to Better Reflect Appropriate Business Practices

The revised proposed regulations set forth a new definition of the term household. Pursuant to the updated draft rules, a "household" is a person or group of people "who (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier."[11] While this definition represents an improvement from the definition that was in the original release of the draft rules, it still risks exposing consumer information to others. It also does not accurately reflect the way that businesses identify individuals who are part of the same household in the ordinary course of business. We therefore ask the CA AG to make slight alterations to the definition of household so it provides more protection for California consumers, better reflects the intent and purpose of the CCPA, and aligns with businesses' actual practices.

W277-4

We suggest that the CA AG update the household definition to apply to a person or group of people who (1) reside at the same address, (2) share a common device, (3) share the same service provided by the business, and (4) are identified by the business as sharing the same group account or unique identifier. Without this change, consumers would be put at risk of having personal information associated with them exposed to other individuals in the household, including to individuals that do reside together who should not have access to such information. Providing data in response to a household request to know, for example, has risks of exposing data associated with a consumer to a person the consumer may not want to receive the information. Consumers should have the right to keep data associated with them private if they do not wish for that information to be shared with other individuals in their home. Updating the draft rules to better define "household" would consequently provide more privacy protection for consumers, thereby furthering the purposes of the CCPA. Moreover, this change to the definition of household would better reflect actual business practices in categorizing individuals as part of the same household. We therefore respectfully ask the CA AG to alter the definition of

[11] Cal. Code Regs. tit. 11, § 999.301(k) (proposed Feb. 10, 2020).

household so it better provides consumers living in the same household with the protections set forth in the CCPA and its implementing regulations.

W277-4 (cont.)

V. Add a Provision Clarifying that Information Businesses Collect, Use, and Share for Fraud Prevention Purposes is Not Subject to Certain CCPA Rights

The revised proposed regulations do not address businesses' use of personal information for fraud prevention purposes, and the CCPA's exemptions do not provide a clear carve out for such activities to ensure that beneficial uses of data for fraud prevention can persist. The use of data for anti-fraud purposes provides consumers with considerable benefit by protecting them from harmful activities and making markets more efficient. We therefore request that the CA AG clarify that the fraud exemption to the deletion right applies to the collection, use, and sharing of personal information to create and distribute fraud prevention and detection tools. We also ask the CA AG to clarify that a similar exemption exists for the right to opt out of personal information sale so consumers may not prevent a business from sharing information necessary to detect fraudulent activity.

The fraud exemption to the CCPA's data deletion right applies to entities that "maintain the consumer's personal information in order to… protect against malicious, deceptive, fraudulent, or illegal activity."[12] As a result, the exemption covers the users of important fraud tools that are necessary for businesses to protect consumers from deceptive or illegal activity on their accounts, but it does not explicitly cover data suppliers that provide the information necessary to create vital fraud prevention services. This is because those data suppliers do not necessarily maintain the imperative information that makes fraud tools work in order to protect against fraudulent activity.

W277-5

Additionally, there is no exemption to the opt out right for data that is used to prevent fraud, which could cause vital information that industry members use to detect fraud to be removed from the marketplace. Many businesses regularly use and share personal information for legitimate fraud prevention purposes, and this sharing of information benefits consumers by providing enhanced protection for the purchases, interactions, and services they undertake on a daily basis. Businesses' ability to connect, associate, and share personal information with partners for fraud prevention is imperative for helping to prevent and monitor fraudulent activity on consumers' accounts.

To clarify that the CCPA should not restrict the ability to gather information needed to create, provide, enhance, or deliver anti-fraud tools and services, we urge the CA AG to provide additional detail on the scope of the fraud exemption to the deletion right. We also ask the CA AG to clarify that such an exemption exists for the opt-out right in the CCPA. In particular, the CA AG should issue a rule clarifying that the CCPA fraud exemption to the consumer deletion right covers the collection, use, and sharing of personal information to create and distribute fraud prevention and detection tools. We also ask the CA AG to clarify that an analogous exemption exists for the opt out right so consumers may not opt out of a business's sharing of personal information for fraud prevention purposes.

[12] Cal. Civ. Code § 1798.105(d)(2).

VI. Enable Flexibility for Providing the CCPA-Required Notice at Collection to Consumers Through the Telephone and in Person

The revised proposed regulations state that when a business collects personal information over the telephone or in person from consumers, the business may provide the CCPA-required notice at collection orally.[13] We respectfully ask the CA AG to clarify that businesses may satisfy the CCPA's notice at collection requirement by directing consumers to a physical or online location where they may find and read the applicable privacy notice.

Providing oral CCPA disclosures to consumers on the phone and in person would cause substantial friction in consumers' ability to seamlessly interact and transact with businesses. Furthermore, oral CCPA notices would significantly hinder consumers' ability to efficiently access products and services. For example, if a consumer transacts with a business and provides personal information to that business through the telephone, and if the business representative reads the consumer the business's CCPA-required notice at collection, the consumer will be forced to stay on the phone with a business for a much longer period of time than the consumer would have been required to prior to the effective date of the CCPA solely for the purpose of satisfying the business's legal obligations. This outcome will result in consumer frustration and will likely not serve the purpose of appropriately notifying consumers of the business's data practices. W277-6

We ask the CA AG to affirm that a business may direct a consumer to a privacy notice posted online or elsewhere in order to satisfy the notice at collection requirement when personal information is collected by a business on the phone or in person. Such an express clarification in the regulations will reduce the potential for significant inconvenience to consumers and will decrease the likelihood that consumers will be forced to listen to a privacy notice orally. This outcome would better serve the CCPA's ultimate goal of providing consumers with clear and understandable notice of the business's data collection and use practices.

VII. Remove New Duplicative and Unclear Transparency Requirements

The updates to the proposed regulations require a business that collects personal information from consumers' mobile devices to provide just-in-time notice of any data collection "that the consumer would not reasonably expect."[14] We ask the CA AG to remove this requirement, as it provides an indefinite standard that forces businesses to attempt to guess what a consumer would reasonably expect and as a result does not provide clear privacy protections for Californians. This rule is also unnecessary because the CCPA and the draft regulations already contain consumer notice requirements mandating that businesses provide specific disclosures about their data practices. W277-7

Requiring businesses that collect information from mobile devices to provide just-in-time notice of any data collection the consumer would not "reasonably" expect is a legal requirement that gives no clear instructions to businesses. Tying the requirement to a reasonable person standard will not provide strong, clear, or definite protections for consumers and will leave

[13] Cal. Code Regs. tit. 11, § 999.305(a)(3)(d) (proposed Feb. 10, 2020).
[14] *Id*. at § 999.305(a)(4).

entities guessing at a reasonable consumer's expectations. Businesses would have no way to clearly understand when such a notice would be required. It would be difficult if not impossible for businesses to understand what rises to the level of a data collection activity that is not reasonably expected by consumers. The CA AG should remove this directive to minimize the number of vague requirements included in the CCPA's implementing regulations. More clarity and less ambiguity will better ensure that Californians receive the privacy protections that are intended by the law.

W277-7 (cont.)

Additionally, the law already requires businesses to notify consumers of the categories of personal information to be collected and the purposes for which such categories of personal information will be used in a notice at collection.[15] This mandate appears in both the proposed regulations and the CCPA itself. It is therefore duplicative for the CA AG to require businesses to notify consumers of data collection they would not reasonably expect, as the CCPA and the draft rules plainly state that a business must provide information about their data collection practices at or before the time period when data collection occurs. As a result, we suggest the CA AG remove the requirement from the proposed rules to provide just-in-time notice for mobile application data collection practices that a consumer "would not reasonably expect."

VIII. Remove the Limitation on Service Providers' Internal Use of Personal Information

The revised proposed regulations state that a service provider may not retain, use, or disclose personal information obtained in the course of providing services to a business unless a certain expressly listed exception in the draft rules applies.[16] One of the explicit exceptions listed in the draft rules is that a service provider may retain, use, or disclose personal information obtained in the course of providing services for internal use by the service provider to build or improve the quality of its services, "provided that the use does not include building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source…."[17] We respectfully ask the CA AG to remove this limitation on service providers' ability to internally use data to improve services, as building consumer profiles and engaging in data hygiene activities enable service providers to improve their offerings in ways that provide considerable value to consumers.

W277-8

Service providers internally use the personal information they receive for a variety of beneficial purposes, including improving the ability of their services to detect fraudulent activity on a consumer's account. If service providers cannot internally use data to build or modify profiles to improve their services' ability to detect anomalies in consumers' purchases or account activities, consumers will no longer receive robust protection from fraud in the marketplace and may be hindered in their ability to receive alerts or information about potentially harmful or illegal activities that could impact them.

In addition, consumers benefit from the data hygiene activities service providers undertake to improve their services, as these activities help ensure that the offerings service

[15] Cal. Civ. Code § 1798.100(b); Cal. Code Regs. tit. 11, § 999.305(a)(1) (proposed Feb. 10, 2020).
[16] Cal. Code Regs. tit. 11, § 999.314(c) (proposed Feb. 10, 2020).
[17] *Id*. at § 999.314(c)(3).

providers bring to the market are working on the most accurate and up-to-date information. Data hygiene activities like change of address information ensure consumers receive information they want and avoid receiving messages they do not want. Moreover, data hygiene activities do not give marketers leads or identify customers for a brand; they simply enable entities to maintain accurate records, thereby bolstering data integrity. Data hygiene makes markets more efficient, and it ensures consumers do not receive inaccurate information or too much information. Removing service providers' ability to internally use personal information to better their products through cleaning data acquired from another source could cause data integrity issues and would severely limit the value and accuracy of the services that consumers receive and expect.

W277-8 (cont.)

The CCPA itself already requires service providers to maintain contracts with businesses that limit their ability to use personal information for purposes outside of the services specified in the contract.[18] This statutory requirement provides consumers with considerable protection that personal information will not be used externally in a manner that is outside of the scope of the services requested. Service providers should be empowered to use personal information internally to improve their products and services without unreasonable limitations. We therefore urge the CA AG to remove the language in the draft rules stating that service providers cannot retain, use, or disclose personal information internally to build or modify household or consumer profiles or clean or augment data acquired from another source.

IX. Clarify the Requirement to Obtain Parental Consent for Minors "in addition to" Verifiable Parental Consent Under COPPA

The revised proposed regulations require a business that has actual knowledge it collects or maintains the personal information of children under thirteen to establish, document, and comply with a reasonable method for determining that a person affirmatively authorizing the sale of personal information about the child is the parent or guardian of the child.[19] The CA AG did not alter the requirement to obtain such affirmative authorization "in addition to" any verifiable parental consent required under COPPA in the most recent update to the draft rules.[20] We therefore renew our request for the CA AG to clarify that a business may satisfy this additional consent requirement by sending a single consent communication to a parent or guardian with separate consent requests or check boxes for CCPA and COPPA.

W277-9

Although the CCPA notes that affirmative authorization to sell a child's information must be in addition to any verifiable parental consent obtained to comply with COPPA, the law provides no guidance on how a business may satisfy this additional consent requirement. It is unclear if this provision will be interpreted by the CA AG to require separate consent communications or if a business may use a single communication with multiple consents in order to satisfy the requirements of both laws. The lack of guidance also creates ambiguities when it comes to interpreting parents' choices, as it is unclear what should happen if a consumer consents to personal information sale under the CCPA but rejects personal information collection, use and/or disclosure under COPPA. The draft rules also do not address or seem to

[18] Cal. Civ. Code § 1798.140(v).
[19] Cal. Code Regs. tit. 11, § 999.330(a) (proposed Feb. 10, 2020).
[20] *Id*.

contemplate the fact that COPPA could potentially preempt the CCPA requirement to obtain affirmative authorization to sell personal information.

We urge the CA AG to clarify how the additional consent requirement should function in practice. Specifically, ANA asks the CA AG to confirm by rule that a business may provide a parent or guardian with a single consent communication that is acceptable under both the CCPA and COPPA. Such a clarification would help to consolidate the number of consent requests a parent or guardian may receive and field and would provide enhanced clarity regarding what is required from businesses under the CCPA. W277-9 (cont.)

X. Remove the Requirement to "Permanently and Completely" Erase Personal Information

The draft rules implementing the CCPA still state that a business may comply with a consumer's request to delete personal information by "permanently and completely erasing" the personal information on its existing systems.[21] While the draft rules also offer businesses the option of deidentifying or aggregating the data to satisfy a consumer's request to delete,[22] the "permanently and completely" erasing language could create compliance challenges for businesses that do not aggregate or deidentify data and may use certain database architectures that do not allow for permanent and complete deletion of information.

For certain businesses, it is a technical impossibility to "permanently and completely" delete all records. Certain records may remain in cold storage for extended periods of time, and it may not be possible for some businesses to remove certain "ghost" copies or files of such information. Moreover, a business taking steps to effectuate "permanent and complete" deletion could also conflict with the proposed regulations' existing requirements for businesses to maintain records of consumer requests.[23] We therefore request that the CA AG replace this provision with an option to refrain from using, processing, sharing, or disclosing personal information that a consumer requested to delete in the event that "permanent and complete" deletion is not possible. Such a change would still provide consumers with the same level of protection because it would ensure they have control over data and are able to limit its use and disclosure. This change would also help ensure businesses can comply with deletion requests in a way that their database systems allow and avoid technical violations of the law in responding to consumer requests to delete. W277-10

XI. Remove the Requirement to Provide a General Toll-Free Contact Number to Receive Consumer CCPA Requests

The CA AG did not address the toll-free number method of submitting CCPA requests in the revisions to the draft regulations. The proposed rules require certain businesses to provide a toll-free number as a method for receiving requests to know and state that a business may provide one for receiving requests to delete and opt out of personal information sale.[24] We ask W277-11

[21] *Id*. at § 999.313(d)(2)(a).
[22] *Id*. at §§ 999.313(d)(2)(b), (d)(2)(c).
[23] *Id*. at §§ 999.313(d)(5), 317(g).
[24] *Id*. at §§ 999.312(a), (b); 999.315(a).

the CA AG to remove the requirement to provide a toll-free number for receiving requests to know. Businesses incur extra costs to offer such numbers to the public. While larger companies may be able to absorb such costs, smaller and start-up businesses may have difficulty complying with the requirement to offer a toll-free number. The CCPA recognizes that certain businesses may need to operationalize the law in different ways due to their size or other practices. We ask the CA AG to extend that understanding to this requirement and clarify that businesses *may* offer a toll-free number as a method of submitting a request to know, but they are not required to offer a toll-free number. Such a clarification would help provide flexibility for the methods businesses may provide to consumers to submit requests to know.

W277-11 (cont.)

XII. Clarify How Businesses Must Respond to CCPA Requests When They Maintain Personal Information In A Manner that Is Not Associated With An Identifiable Person

The draft regulations still state that if "a business maintains personal information in a manner that is not associated with a named actual person, the business may engage in verification by requiring the consumer to demonstrate that they are the sole consumer associated with the non-name identifying information."[25] ANA asks the CA AG to clarify that businesses that do not already maintain information sufficient to verify a consumer's identity are not required to collect additional data from a consumer in an attempt to do so.

The CA AG's updates to the draft rules added an example stating that a business that collects personal information about a consumer through a mobile application but does not require the consumer to create an account may ask the consumer to provide additional information or respond to a notification sent to their device in order to verify the consumer's identity.[26] This example does not address situations when businesses do not maintain personal information that is associated with a named actual person. It also does not address how a business that does not have a direct relationship with a consumer could ask the consumer to verify their identity. For example, a consumer's provision of his or her name to a business in response to a business's request for additional information to verify the consumer's identity will not enable the business to verify the consumer if the business only holds information in a manner that is not associated with a named actual person. The draft rules are therefore unclear with respect to how a consumer's provision of any additional information could verify the consumer if the business only holds unique online identifiers or other information that a consumer would not reasonably know or be able to submit in order to verify their identity.

W277-12

Moreover, because the non-name identifying information businesses may hold, such as unique online identifiers, could be associated with or encompass the information of multiple consumers, it may be impossible for a user to demonstrate that he or she is the sole consumer associated with non-name identifying information. For this same reason, requiring a consumer to respond to a notification sent to a device would similarly be an insufficient method of verifying identity. Because unique online identifiers may cover entire households, libraries, universities, and shared devices, they may be linked to personal information from many individuals. Additionally, any number of individuals may be able to access a given mobile

[25] *Id*. at § 999.325(e)(2).
[26] *Id*.

application and respond to the notification presented through it. As a result, the methods listed in the draft rules for businesses that do not maintain information associated with a named actual person to verify consumers are insufficient and do not provide any clarity regarding how businesses should field or respond to consumer CCPA requests.

For these reasons, ANA asks the CA AG to clarify that businesses that do not already maintain data sufficient to verify a consumer's identity are not required to collect additional data in an attempt to engage in verification. Without such a clarification, the draft rules may be perceived to impose an obligation on them to collect identifying information about consumers when they would not have chosen to do so in their normal course of business. This result is not privacy protective for consumers, as it facilitates the provision of additional consumer information to a business when the business does not want to receive such information and when receiving such information may do little to actually enable the business to verify the consumer's identity.

W277-12 (cont.)

XIII. Clarify and Alter the Disclosures Required of Businesses that Buy, Receive, Sell, or Share Personal Information of 10 Million or More Consumers

The draft regulations require "[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 10,000,000 or more consumers" to disclose certain information in a privacy policy about their responses to CCPA requests.[27] ANA requests that the CA AG remove the phrase "for commercial purposes" from this provision. ANA also asks the CA AG to consider removing the privacy policy disclosure obligations from this provision and replacing them with a requirement to report such information to the CA AG upon request.

W277-13

ANA asks the CA AG to remove the phrase "for commercial purposes" from this provision because it could be interpreted to include sharing personal information about a consumer with service providers. Such an interpretation could drastically increase the number of businesses that would be subject to this additional reporting requirement and is likely not in line with the CA AG's intent. Sharing information with service providers should not be within the scope of the calculation for determining whether a business is subject to the extra reporting requirements listed in Section 999.317(g) of the proposed rules. The CA AG should remove the phrase "for commercial purposes" from the text of that section to help clarify that sharing information with service providers should not count towards the 10 million consumer threshold listed in the provision.

Additionally, ANA asks the CA AG to reconsider the mandatory privacy policy disclosures associated with this requirement. Businesses subject to this additional reporting requirement must disclose in a privacy policy annual numbers of CCPA requests received, complied with in whole or in part, and denied, as well as information about the timeline within which the business typically responds to such requests. Obligating businesses to make such information public in a privacy policy will not provide consumers with information that will help them better understand the business's data practices. Also, the public nature of this information could have anticompetitive effects, as it would be visible to competitors and could potentially

W277-14

[27] *Id*. at § 999.317(g).

reveal confidential or proprietary insights about the business. ANA therefore asks the CA AG to consider replacing the privacy policy aspects of this requirement with an obligation to maintain the same records and report them to the CA AG upon request. Making such an update to the draft rules would serve the purpose of protecting consumers by holding businesses accountable for meeting CCPA requests but would relieve the potential anticompetitive effects of requiring such disclosures in a privacy policy.

W277-14 (cont.)

XIV. Affirm that Required Notices May Be Provided in a Privacy Policy

The proposed rules require a business to provide a privacy policy, a notice at collection, a notice of the right to opt out of the sale of personal information (if the business engages in sales), and a notice of financial incentive (if the business offers financial incentives or price or service differences to consumers).[28] The CA AG should clarify that a business may satisfy these consumer disclosure requirements by providing all of the necessary notices in a privacy policy accessible to consumers where required. Such a clarification would helpfully enable all privacy-related disclosures to be provided to consumers in one place, so consumers do not need to access many different pages or obtain various forms in order to receive important information about businesses' data practices. Giving consumers a centralized disclosure through which they may receive required privacy-related information will better enable consumers to review the information and refer back to it at a later date if they desire to do so. Specifically, we ask the CA AG to add a term to Section 999.304 stating that all of the required notices listed in that section may be provided in a privacy policy so long as they meet all of the content and other requirements set forth in Sections 999.305 through 999.308 of the proposed rules.

W277-15

XV. Grant Online Businesses that Do Not Maintain Personally Identifying Information Flexibility to Provide Effective Opt Out Mechanisms

According to the draft rules, a business that operates a website must provide an interactive form accessible via an online link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info" to enable consumers to opt out.[29] However, information provided to businesses through such a webform may not actually enable the business to effectuate the consumer's opt out request. The CA AG should clarify that online businesses that do not maintain information in a manner that can identify a named actual person do not need to provide an interactive form for consumers to submit opt out requests and may instead use another effective method to allow consumers to submit a request to opt out, such as through other standard channels used for customer service.

W277-16

While an interactive form may work efficiently for businesses that maintain personally identifiable information such as a consumer's name, email address, or postal address, an interactive form may not adequately enable a business that does not maintain personally identifiable information to facilitate an opt out. For example, businesses that hold unique online identifiers and do not associate personally identifiable information with such identifiers may not be able to process a consumer's opt out request if it is submitted through an interactive form. Additionally, consumers may not have access to these identifiers, so they may not be able to

[28] *Id*. at §§ 999.304 – 308.
[29] *Id*. at § 999.306(c)(2), 315(a).

submit any information that the business can use to verify the consumer's identity by matching the information the consumer provides to the information maintained in the business's systems.

The proposed regulations recognize that methods for submitting consumer rights requests may need to be different depending on the way the business interacts with a consumer. The rules should similarly address the differences that may be necessary for businesses that collect personally identifiable information and businesses that do not collect information that is associated with a named actual person. We therefore respectfully ask the CA AG to clarify that online businesses that do not maintain personally identifiable information or information in a manner that can identify a named actual person do not need to provide an interactive form for consumers to submit requests to opt out of personal information sale and may use another method, such as other common channels used for customer service, to enable a consumer to submit a request to opt out.

W277-16 (cont.)

* * *

Thank you for the opportunity to provide input on the revised proposed regulations implementing the CCPA. We look forward to continuing to work with the OAG on these important matters. Please do not hesitate to contact us with any questions you may have regarding these comments.

From: Brent Smoyer
To: Privacy Regulations
Subject: PBSA Commentary on the February 2020 Draft Proposed CCPA Regulations
Date: Tuesday, February 25, 2020 10:24:29 AM
Attachments: image001.png
PBSA CCPA Regulation Commentary February 2020 Updates.pdf

Attached, please find commentary from the Professional Background Screening Association (PBSA) regarding the Attorney General's draft regulations pertaining to the California Consumer Privacy Act (CCPA).

We thank you for your time and consideration.

Brent Smoyer, JD
State Government Relations and Grassroots Director

Direct: [redacted]
Main: 919.459.2082

NAPBS is now the Professional Background Screening Association

February 24, 2020

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

RE: CALIFORNIA CONSUMER PRIVACY ACT PROPOSED REGULATIONS – 02/10/2020 Edition

On behalf of the Professional Background Screening Association (PBSA), whose members include California residents and businesses, we write to you with commentary regarding the second draft of the Department of Justice's draft rules for the California Consumer Privacy Act, dated February 10, 2020.

As a nonprofit organization consisting of over 900 small and large companies engaged in the background screening profession, PBSA has been dedicated to providing the public with safe places to live and work since 2003. The PBSA member companies conduct millions of employment and tenancy-related background checks each year, helping employers, staffing agencies, and nonprofit organizations make more informed decisions regarding the suitability of potential employees, contractors, tenants and volunteers.

Millions of background screening reports are requested in the United States each year. Our members are hired to verify the education, employment, financial, and criminal histories of applicants. There are a number of important reasons for conducting these searches, including: (i) ensuring a safe working environment by reducing the likelihood of workplace violence; (ii) ensuring property managers have the ability to provide safe living environments for tenants, including where

hiring of individuals based on fraudulent credentials; (v) avoiding legal exposure for negligent hiring and (vi) meeting state law requirements designed to protect vulnerable populations like the elderly, the disabled, and children.

Background screening is a "unique animal" in the data usage world and has been acknowledged as such by the California Legislature with the exemption outlined in CCPA Section 1798.145(d). Screeners are Consumer Reporting Agencies (CRA's) and as such are highly regulated under the Federal Fair Credit Reporting Act (FCRA) by the Federal Trade Commission and Consumer Financial Protection Bureau. Additionally, our members are also regulated by a patchwork of federal, state, and local rules pertaining to data security and privacy laws including the California Investigative Consumer Reporting Agencies Act ("ICRAA"). We follow specific privacy and safety guidelines -- both through statute and standard industry practices -- for identity theft prevention, fraud alerts, unauthorized dissemination of information, disposal of records, and other important security practices.

Further, employment-related background checks are done with full disclosure of the background check, and the express authorization and consent of the worker whose personal information is being accessed (as explicitly required by the FCRA). The current FCRA required "opt-in" ensures that policy concerns regarding a worker's knowledge that their data is being collected are already addressed for the worker. Data that is collected, exchanged, and/or aggregated to compile the consumer report is done so with a worker's knowledge and express permission or written instructions.

Additionally, the FCRA, a consumer protection-based statute, addresses consumer protection by placing requirements on both CRAs and end-users (employers or property managers) who request background reports on potential employees or tenants. The regulation requires disclosure and authorization before a report is prepared and provides consumers with the right to dispute the completeness or accuracy of a report. In the event of a dispute, a CRA is also required to reinvestigate at no charge to the consumer and with strict guidelines while doing so. Please see the attached enclosure describing the many consumer protections provided within the FCRA when consumer reports are prepared for employment and tenant related background screening.

We understand that our colleagues at the Consumer Data Industry Association (CDIA) have produced a very thoughtful analysis that they are submitting, highlighting key areas where the most recent draft of these draft regulations could be improved and help consumers and business alike to easily understand their rights and obligations under the CCPA. We at PBSA have serious concerns about several sections of the proposed regulations that, if finalized, would impose greater requirements and restrictions than those provided for in the CCPA. As CDIA described in their highly detailed original analysis, these sections do not implement any particular provision in the CCPA and exceed the law's authorization for the OAG to adopt regulations "necessary to further the purposes of" the law.

PBSA shares these concerns with CDIA and fully endorses those same suggestions for improvement. As such, we will not unnecessarily revisit them here. What we would do is emphasize two critical concerns that remain from the initial draft regulations that we at PBSA feel are most notable:

1) **Strike the requirement that businesses treat user-enabled privacy controls as opt-out requests.**

Section 999.315(c) requires that businesses treat user-enabled privacy controls that communicate or signal a consumer's choice to opt out of the sale of their personal information to third parties as a valid request to opt out for that browser or device or, if known, for the consumer. The CCPA protects *"personal information,"* which is, as stated in CCPA section 1798.140(o)(1), information that reasonably may be linkable to a particular person or household, not merely a device.

ISSUE: The CCPA does not protect information that cannot reasonably be linked to a particular person or household, regardless of whether the business can detect that the information relates to a particular device. To require this exceeds the scope of the CCPA and, as such, the OAG would be exceeding its authority under the law by attempting to impose this requirement. W278-1

To the extent that information may reasonably be linked to a particular consumer or household, consumers can install browser privacy controls for a variety of reasons, many of which do not equate to desiring for their information not to be sold to third parties. The CCPA does not provide for a right to be opted out from the sale of personal information by installing any browser privacy control. Furthermore, this technology is evolving and there will likely be compatibility problems with these controls.

PROPOSED SOLUTION*: Eliminate the requirement that user-enabled privacy controls be treated as opt-out requests.*

2) **Properly balance the timing of regulation enactment and business compliance.**

Given the high level of technicality of these proposed regulations, businesses will need significant time to develop and implement processes compliant with these requirements.

Due to the effort it will take for businesses to adapt with proper compliance measures, we would respectfully request that the Attorney General provide for an implementation period of at least 6 months after publication of the final rule before the regulations would become effective. W278-2

Additionally, because of the nature of certain requirements, PBSA would respectfully request that any responsibility that is contingent upon the providing of notice prior to taking certain action either be subject to a later effective date or subject to a *delayed enforcement date of at least 3 months* after the effective date of the primary rule.

We believe that these are reasonable requests in order to allow businesses to adapt to the regulations and that adopting regulations with delayed effective and enforcement dates will fully comply with the directive given to the Attorney General under the CCPA.

W278-2 (cont.)

While we harbor greatest concern over the previously listed points, PBSA would once again state our vigorous support of the concerns and solutions stated in the CDIA commentary as the OAG works to improve these draft regulations.

We thank you for taking the time to hear our concerns and consider our requests. PBSA and its members are prepared to discuss any questions you may have and look forward to working with you further. Please feel free to contact me directly with any questions at [redacted] or [redacted].

Sincerely,

Brent Smoyer, JD
PBSA State Government Relations &
Grassroots Director

PBSA
PROFESSIONAL BACKGROUND SCREENING ASSOCIATION

From: Mike Stinson
To: Privacy Regulations
Subject: Comments on Revised CCPA Regulations
Date: Tuesday, February 25, 2020 9:58:15 AM
Attachments: image001.png
Comments on CCPA Regulations 2.0 - final.pdf

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

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

Michael C. Stinson, JM
Vice President of Government Relations & Public Policy

MPL MEDICAL PROFESSIONAL LIABILITY ASSOCIATION

2275 Research Blvd., Suite 250
Rockville, MD 20850
Direct: [redacted]
Cell: [redacted]
www.MPLassociation.org

MPL | MEDICAL PROFESSIONAL LIABILITY ASSOCIATION

February 25, 2020

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

ATTN: Privacy Regulations Coordinator

Subject: Comments on Proposed CA Consumer Privacy Act Regulation

Dear Attorney General Becerra:

On behalf of the Medical Professional Liability Association and our medical professional liability (MPL) insurers that conduct business in California, we appreciate this opportunity to share our perspective on the most recent proposed California Consumer Privacy Act (CCPA) Regulations.

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

The MPL Association supports the adoption of consumer data privacy measures that enhance transparency and data protections related to consumers' personal information without restricting its member companies' ability to use consumer data that is necessary to conduct a full range of insurance services to its insureds. We believe the latest draft regulations are a step in the right direction, but that additional improvements could be made to protect consumers without unduly burdening businesses.

To begin, we would like to applaud you for the numerous changes made to the regulations that aim to clarify businesses' responsibilities under the CCPA and reduce the administrative burden associated with compliance. Among the improvements are the clarification that only "materially different" uses of consumer personal information than those previously disclosed are prohibited (§ 999.305(a)(5)), providing flexibility for businesses to describe the "general" process used to verify consumer requests (§ 999.308(c)(2)c), and clarifying that businesses are not required to delete information from archived or backup systems until the data is "restored to an active system" or "used for…a commercial purpose" (§ 999.313(d)(3)). We also believe

W279-1

W279-2

W279-3

the new guidance provided on the definition of "personal information" is a positive development (§ 999.302(a)). W279-4

The changes made to § 999.313(c)(3) are certainly helpful, however, improvements could be made to make this provision more functional. Specifically, we believe the list of circumstances under which a business is not required to search for personal information need not be entirely mutually exclusive. As such, we recommend that the provision be amended as follows:

(3) In responding to a request to know, a business is not required to search for personal information if ~~all~~ the following conditions are met:

a. The business does not maintain the personal information in a searchable or reasonably accessible format; or

b. The business maintains the personal information solely for legal or compliance purposes;

and

c. The business does not sell the personal information and does not use it for any commercial purpose; and

d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.

W279-5

Such a change would clarify reasonable and recognized circumstances under which a data search would not be necessary, while still maintaining adequate consumer data protections.

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

Sincerely,

Brian K. Atchinson
President & CEO

From: Alan Thiemann
To: Privacy Regulations
Cc: William Harris; Lauren Scheib
Subject: Re: Comments on Modified Regulations
Date: Tuesday, February 25, 2020 8:54:38 AM
Attachments: Cal. AG letter 02252020.pdf

Please find the attached comments for the Assocaition of Test Publishers.

On Tue, Feb 25, 2020 at 11:47 AM Alan Thiemann <[redacted]> wrote:

> Ms. Kim,
>
> Please find the attached letter from the Association of Test Publishers commenting on the Modified Regulations. These comments augment those filed in our initial letter dated December 6, 2019.
>
> If you have any questions, please let me know.
>
> Alan J. Thiemann
> General Counsel
> [redacted]
>
> --
> Alan J. Thiemann
> Han Santos, PLLC
> 700 12th Street, NW
> Suite 700
> Washington, DC 20005
> [redacted]
> (202) 558-5101 fax

--
Alan J. Thiemann
Law Office of Alan J. Thiemann
700 12th Street, NW
Suite 700
Washington, DC 20005
[redacted]
(202) 558-5101 fax

Global ATP Association of Test Publishers
The intelligent voice for testing

601 Pennsylvania Ave., N.W.
Suite 900
Washington D.C. 20004
+1.717.755.9747
www.testpublishers.org

February 25, 2020

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

Re: **Comments of the Association of Test Publishers**

Dear Ms. Kim,

The Association of Test Publishers ("ATP") submits these comments on behalf of the testing industry to address the Modified Regulations for implementing the California Consumer Privacy Act ("Modified Regulations"), as published by your office on February 7, 2020. This submission is being made by the required date of February 25, 2020. The ATP previously submitted comments addressing the initial Proposed Regulations on December 6, 2019, in which we made numerous recommendations that have not yet been acted on by the Attorney General; we remain hopeful that further modifications to the Proposed Regulations will occur before July 1, 2020.

1. §999.302. Guidance on Interpretation of Definition of "Personal Information"

The Modified Regulations provide a single example to aid in the understanding of the definition of "personal information." The new language states that, "…if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be 'personal information.'" While this example helps explain why the Legislature added the word "reasonably" to the statute, from the ATP's perspective, it does not go far enough in exploring all of the variations of how a linkage between the information collected and a person must exist, including "how the information is maintained." Additionally, the ATP continues to assert that even if some information may be associated with a consumer, if it was not provided by the individual, but rather was generated or

W280-1

derived by the business as a result of a services contract, it should not be considered "personal information" (e.g., test results/scores). W280-1 (cont.)

2. §999.315(d)(1) and (2). Requests to Opt-Out.

The Modified Regulations discuss "global privacy controls" in browsers that might be developed and require anyone collecting personal information online to treat this approach as a valid "opt-out" or otherwise have to check with the consumer about a conflict with his/her specific browser setting. This requirement places an extreme and unnecessary burden on a covered business to consider possible future browser settings, even ones with which it is not familiar or that are rarely used. The ATP contends that a business should not be obliged to support all possible browser plugins, including those that are not commonly used. W280-2

3. §999.305. Employee-related Information.

The ATP is extremely concerned that the new language in §999.305 regarding employee-related information is not consistent with the terms of AB 25, enacted by the California Legislature last September and signed into law by the Governor in October.[1] The Legislature established a one year "moratorium," excluding "employee-related information" from being considered as "personal information" under the CCPA until 2021. [2] Consistent with the well-accepted legal definition of the word "moratorium," the intention of the Legislature was to delay the effectiveness of the CCPA as to employee-related information for one year in order to allow itself time to consider further actions in 2020. Rather than give effect to this clear legislative intent, the Modified Regulations improperly require that a business must still apply much of §999.305 to employees/job applicants. W280-3

The Modified Regulations state that, until January 1, 2021, unless there is a further amendment to the CCPA, a covered business is only exempt from the following provisions in Section 305:

[1] The Modified Regulations completely fail to address the second moratorium enacted as part of AB25, concerning treatment of "business contact" information during 2020. As the ATP noted in its December 6 letter, when a business deals with another business, and a representative of the second business provides his or her contact information, 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 a "consumer" and the business is not "a natural person" as defined in Section 17014 of Title 18 of the California Code of Regulations. *See* Cal. Civ. Code §1798.140(g).

[2] The Modified Regulations also add definitions for the terms "employment benefits" and "employment-related information (*see* §999.301(h) and (i)). Nevertheless, the ATP remains concerned that the definition of "employment-related information" is too narrow (e.g., focused on covering the administration of employment benefits) and is not broad enough to encompass the "business purposes" associated with the use of personal information of any employee, job applicant, and/or contractor, including their test results/scores.

1) The notice at collection of employment-related information does not need to include the link or web address to the link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info;" and

(2) The notice at collection of employment-related information may include a link to, or paper copy of, a business's privacy policies for job applicants, employees, or contractors in lieu of a link or web address to the business's privacy policy for consumers. W280-3 (cont.)

But these two elements of Section 305 clearly do not comprise the full responsibilities that a business would normally have to meet if employee-related information were considered "personal information." Accordingly, the ATP submits that the Modified Regulations, as written, are inconsistent with, and do not conform to, the "moratorium" as enacted into law.

4. §999.313. Enforcement of the CCPA.

One of the references added to Modified Regulations is Douglis, et al., "How the CCPA impacts civil litigation" (January 28, 2020) (available at https://iapp.org/news/a/how-the-ccpa-impacts-civil-litigation/#). As the article notes, "It is not hard to imagine the CCPA could become weaponized against businesses...." The ATP strongly agrees with the authors that a solution to this "weaponization" problem is for the final regulations to allow a business to refuse to provide access to information that is clearly part of a pre-litigation mining activity by the plaintiffs' bar. In our view, the CCPA does not restrict a business's ability to "exercise or defend legal claims." The final regulations should allow a covered business to refuse to respond to mass-access requests that are clearly aimed at pre-litigation discovery. This problem is especially critical for testing organizations that engage in employment-related and certification testing services, which are highly vulnerable to such "weaponized" requests for personal information surrounding actions by covered businesses that use testing services. W280-4

5. §999.314. "Service provider" regulations.

In its December 6 letter, the ATP contended that the Proposed Regulations should not be interpreted in such a manner as to prevent specific business contracts from being entered into and performed (*see* page 10, fn. 18).

The modified language of §999.341(b)(1) adopts a position consistent with the one advocated by the ATP in its December 6 letter, namely, that a service provider may use or disclose personal information it obtains in the course of providing services to a covered business "to perform the services specified in the written contract with the business that provided the personal information." Although this modification represents a major improvement over the original proposed regulations, the ATP remains tremendously concerned about the Attorney General's apparent refusal to clarify the definition of what constitutes a sale and what is "other valuable consideration." Again, the ATP extensively explained the appropriateness of "sharing" personal information between a covered business and its service providers in order to fulfill a W280-5

consumer's contract for testing services – it would be useful to have the definitions of "sale" and "valuable consideration" clarified in the context of service providers. W280-5 (cont.)

Moreover, the Modified Regulations also permit a service provider to use customers' personal information to retain/employ another subcontractor, improve its services, comply with law or legal obligations, and defend or pursue legal claims – and importantly, to detect data security incidents, or protect against fraudulent or illegal activity."[3] The ATP applauds this clarification; however, further modifications should be made to clarify that, in the context of a services contract, the service provider may give the required notice to a consumer. In performing such internal activities, however, the service provider is not allowed to use personal information to build consumer profiles, "clean" personal data, or augment the data with data obtained from another source. Unfortunately, since none of these terms are defined, the ATP fears that the meaning for services providers remains unclear and will result in inadvertent violations. We urge the Attorney General to provide definitions and clarity around these restrictions in the final regulations. W280-6

6. §999.312. "Methods for Submitting Requests to Know and Requests to Delete"

The Modified Regulations clarify that a business does not need to maintain three methods for receiving consumer requests, including no longer requiring in-person methods for receiving requests. As such, a business operating exclusively online only needs to provide an email address for receiving requests to know and delete. All other types of businesses must provide two methods to receive requests, but because the Modified Regulations provide that "a business only needs to provide one method that reflects the way in which it primarily interacts with consumers" there remains a huge concern over the use of toll-free numbers. The ATP identified a number of issues with the use of toll-free numbers in its December 6, 2019 comments. W280-7

Further, a business now will have 10 business days to confirm receipt of a request to know or delete instead of 10 calendar days. The timeline to comply with a request to opt-out is being expanded from 15 calendar days to 15 business days. These extensions are welcome, but they do not address the main concern raised by the ATP that no confirmation notice ought to be required, given that a full response is required within 45 days – confirmation takes time away from working on the actual verification/response to meet the deadline. W280-8

However, the ATP sees the most important change in this section of the Modified Regulations (see §999.312(a)) is that a business is now able to deny a request to know or delete W280-9

[3] Similarly, the Modified Regulations (§999.314(e)) clarify that when a service provider is handling a request from a consumer, "the service provider shall either act on behalf of the business in responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider." The ATP recommended a similar approach to this in its December 6, 2019 letter; accordingly, we believe this modification resolves a major conflict between responses by a covered business and its service providers.

if the request cannot be verified within 45 days. If a business cannot verify a request to delete, it no longer must treat the unverified request as a request to opt-out. W280-9 (cont.)

7. (§ 999.316) Request to opt-in after opting out.

The Modified Regulations allow a business to obtain an opt-in if the customer initiates a post-opt-out purchase of a service. This approach requires that, in response to a sale of goods or services initiated by the customer, the business is permitted to request an opt-in once it informs the customer the purchase or requested transaction requires the selling of personal information to third parties. The ATP submits that this requirement is inconsistent with the revised §999.341(b)(1), that a service provider may use or disclose personal information it obtains in the course of providing services to a covered business "to perform the services specified in the written contract with the business that provided the personal information." We see no reason why the business must execute a second step to inform the consumer that the purchase requires the "selling" of personal information – indeed, as we noted, *supra.* in paragraph 5, when the purchase only requires a "sharing" of personal information with a service provider, there is absolutely no need to inform the consumer because no "sale" of personal information is taking place. W280-10

8. §999.318. Verification for non-account holders

The Modified Regulations added the ability of verifying a consumer to include a response to an in-app and (for retailers) providing a transaction amount or item purchased (instead of credit card number). In its December comments, the ATP urged the Attorney General to use this same concept of verification through transaction information, applying it to testing events that would be known by the test taker/consumer. We request that the Attorney General confirm that the language of the Modified Regulations covers the testing event situation. W280-11

The Modified Regulations also clarify that when any member of a household is under 13, verified parental consent must be obtained before a business may fulfill requests for access or deletion of specific personal information. In its December letter, the ATP contended that affirmative parental consent ought to be sufficient, so we are gratified that the Attorney General now seems to agree with that position. However, the testing industry would welcome further clarification that affirmative parental consent is also sufficient across the board for the collection and use of personal information of a child under the age of 13. W280-12

CONCLUSION

Once again, the ATP appreciates your consideration of these comments on behalf of the testing industry about the Modified Regulations. The ATP remains available to answer any questions the Attorney General's Office may have in response to these comments or to arrange a

face-to-face meeting. If such follow up is appropriate, 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

Alan J. Thiemann
General Counsel
Han Santos, PLLC
700 12th Street, NW, Suite 700
Washington, DC 2005
[redacted]

From: Katy Johnson
To: Privacy Regulations
Cc: Jan Jacobson
Subject: American Benefits Council Comment on the Modifications to the Proposed Rules on the California Consumer Privacy Act
Date: Tuesday, February 25, 2020 8:14:34 AM
Attachments: privacy_ccpa_ca-letter022520.pdf

Dear Sir or Madam,

Please find attached comments to the Modifications to the Proposed Rules on the California Consumer Privacy Act by the American Benefits Council. If you have questions about these comments or would like to discuss feel free to contact Katy Johnson at [redacted] or Jan Jacobson a[redacted].

Thank you for the opportunity to comment.

-Katy Johnson

Katy Johnson
Senior Counsel, Health Policy
American Benefits Council
1501 M Street NW, Suite 600
Washington, D.C. 20005
(202) 289-6700
[redacted] (direct)
(cell)
[redacted]
www.americanbenefitscouncil.org

February 25, 2020

Submitted electronically at PrivacyRegualtions@doj.ca.gov

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

Attention: Lisa B. Kim, Privacy Regulations Coordinator

Re: Comments to Modifications to Proposed Rules on California Consumer Privacy Act

Dear Attorney General Becerra,

We write on behalf of the American Benefits Council ("the Council") to provide comments in connection with the recently issued modification to the proposed regulations under the California Consumer Privacy Act (CCPA).

The Council is a Washington D.C.-based employee benefits public policy organization. The Council advocates for employers dedicated to the achievement of best-in-class solutions that protect and encourage the health and financial well-being of their workers, retirees and families. Council members include over 220 of the world's largest corporations and collectively either directly sponsor or support sponsors of health and retirement benefits for virtually all Americans covered by employer-provided plans. Many of our members are headquartered in California and they, together with companies headquartered elsewhere, have many employees who work in California or administer health and retirement plans for individuals working or retired in California.

The Council appreciates the opportunity to provide comments on the modifications to the CCPA proposed regulations. As both the California legislature and the Attorney General have recognized, "employment-related information," particularly information related to employee benefits, is unique from personal information that is collected by a for-profit businesses in the marketplace.

1501 M Street NW Suite 600 Washington, DC 20005 202-289-6700 Facsimile 202-289-4582 www.americanbenefitscouncil.org

The legislature passed, and the governor signed, an amendment allowing a one-year delay from the CCPA's requirements (except for the general notice requirement) with respect to information that is necessary for an employer to administer employee compensation and benefits. The Council supported that legislation and worked to make the bill's sponsor aware of concerns related specifically to employee benefits.[1] The bill summary explained that the legislature thought it was important to determine whether and how this benefits-related information should be subject to the CCPA.

To that end, the Council supports the Attorney General's modification to the proposed rules that specifically defines "employment-related information" as a separate category of personal information. The proposed definition includes employment-related information collected for the purpose of administering employment benefits and further defines "employment benefits." W281-1

These new proposed definitions will help employers differentiate the information they collect and use related to employee benefits from the consumer information they may collect in their "business" capacity. This employment-related information is used by the employer, the employee benefit plans they sponsor and the plans' service providers to provide medical, retirement, disability, life insurance, and other fringe benefits to employees and their dependents. This type of information should be recognized as separate and distinct from "marketplace" information.

More generally, we urge the legislature and Attorney General to make permanent the exception for information related to employee benefits. It is critical that information collected about current or former employees and their spouses and dependents within the context of the employee's employment not be treated as personal information within the meaning of the CCPA. Such an exemption is necessary to ensure that employees in California can continue to receive valuable health and retirement benefits offered through work. Employers and the vendors they hire to administer benefit plans must collect certain information in the ordinary course to properly administer the benefit plans; this includes information necessary to deliver those benefits to the employee, or the employee's spouse, dependent, or beneficiary. If ordinary information used to administer plans is subject to CCPA's rules, employers may decide to limit the scope of benefits to employees in California, and may be unable to properly collect and store contact information for spouses, dependents, and beneficiaries who are due benefits. Making permanent the exception provided for 2020 is an important step in preventing California employees from losing valuable benefits. W281-2

If it is not currently feasible to provide a permanent exception, an extended delay would be necessary to avoid adverse consequences for employee benefit plans were the CCPA to take effect with respect to employment-related information. In fact, the legislature recognized that employee benefits information is unique from consumer W281-3

[1] https://www.americanbenefitscouncil.org/pub/2D218002-1866-DAAC-99FB-B5CBD256BF31.

information collected by a for-profit business and that there needs to be more time to study how the CCPA should apply to employment-related information. For example, the Attorney General could issue non-enforcement guidance that provides that no enforcement will be brought with respect to employment-related information or benefits-related information until further guidance is issued with respect to this particular category of information.

W281-3 (cont.)

As the trade association representing the employee benefit plans of over 220 of world's largest employers, the Council would be pleased to provide the California legislature or the Attorney General with more information about how employee benefit information is collected and used. We would be happy to work with the legislature or the Attorney General's office to provide research on privacy protections already in place with respect to this type of information or to provide input from an employer's perspective related to employee benefit plan information.

W281-4

On behalf of the many Council members who employ or administer benefits to employees in California, we appreciate the opportunity to comment on this important matter. Please feel free to reach out to the Council at any time, and thank you for considering these comments. If you have any questions or would like to discuss these comments further, please contact us at (202) 289-6700.

Sincerely,

Jan Jacobson
Senior Counsel, Retirement Policy

Katy Johnson
Senior Counsel, Health Policy

From: Dale Smith
To: Privacy Regulations
Subject: CCPA Written Comment on Proposed Regulations Due February 25 (Transmitting)
Date: Tuesday, February 25, 2020 8:04:08 AM
Attachments: footerNew2.bmp
CCPA_Comments_20200225.pdf

Dear Privacy Regulations Coordinator:

Attached to this email is our .pdf document containing PrivacyCheq's submission of comment for the TEXT OF MODIFIED REGULATIONS published February 7, 2020 (comment period closing on February 25).

Thank you for the opportunity to comment.

Dale Smith

DALE R. SMITH, CIPT
Futurist [redacted]
View my blog at: ***privacyelephant.com***

PrivacyCheq

February 25, 2020

Lisa B. Kim
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

Attn: Honorable Xavier Becerra, Attorney General

Re: Comments on TEXT OF MODIFIED REGULATIONS Released February 7, 2020

Dear Mr. Becerra:

We are writing to express our positive support for the proposed introduction of the "just-in-time" notice concept[1] as an additional means of providing Notice at Collection and Notice of Right to Opt-Out of Personal Information (PI) Sale to California consumers.

The term "just-in-time" does not appear in the CCPA law currently in force, nor did it appear in the October 10 PROPOSED TEXT OF REGULATIONS. We welcome the introduction of this fresh concept in the February 7, NOTICE OF MODIFICATION TO TEXT because we believe it brings into play a simple and practical means for businesses to implement the spirit of CCPA in a way that can build transparency and trust with Californian consumers. W282-1

While the term "just-in-time" is new to CCPA, it is not new to the privacy field. Research focused on consumer privacy at institutions such as Carnegie Mellon

[1] § 999.305 (a)(4) When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a **just-in-time notice** containing a summary of the categories of personal information being collected and a link to the full notice at collection. For example, if the business offers a flashlight application and the application collects geolocation information, the business shall provide a **just-in-time notice**, such as through a pop-up window when the consumer opens the application, which contains the information required by this subsection.

University[2], University of Michigan[3], and American Law Institute[4] has posited for years that providing consumers with relevant and focused privacy information in the moment when they commit to sharing their information with others (the just-in-time notice moment) is a highly desirable best practice.

The introduction of just-in-time notice technology into CCPA leverages strong 2020 trends in today's digital marketplace. Mobile device access for commerce and internet usage has outstripped desktop usage and continues to grow at a robust rate[5]. Mobile use is now the rule, rather than the exception. CCPA's performance-based[6] approach correctly dictates that consumer notices be clearly and well presented on both desktop and mobile devices, and with equal clarity and ease of access.

W282-1 (cont.)

Businesses today face growing regulation from an increasing number of jurisdictions, many of which mandate disparate notice and consent requirements for different consumer sets (jurisdiction, age, language, etc.). Accommodating this complexity by adding paragraphs to a business' legal Privacy Policy renders that document outsized, complex, and practically unfit for compliant Notice at Collection. Recent proposals[7] have suggested that a just-in-time notice be employed as a sub-layer to the mother Privacy Policy.

Consumers today are more aware of their privacy rights than ever before, especially their right to have businesses refrain from selling their personal information. Under CCPA rules, **businesses who do sell** PI may display the new Do Not Sell My Personal Information (DNSMPI) button as a means for consumers to signal the business to stop. (Figure 1)

W282-2

[2] Schaub, et al., A Design Space for Effective Privacy Notices, Symposium on Usable Privacy and Security (SOUPS) 2015, Available at https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf
[3] Florian Schaub, Rebecca Balebako, and Lorrie Faith Cranor, Designing Effective Privacy Notices and Controls, 21 IEEE INTERNET COMPUTING 70 (2017)
[4] Solove, Daniel J. and Schwartz, Paul M., ALI Data Privacy: Overview and Black Letter Text (January 24, 2020). Available at SSRN: https://ssrn.com/abstract=3457563
[5] https://techjury.net/stats-about/mobile-vs-desktop-usage/#gref
[6] https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf
[7] https://www.brookings.edu/blog/techtank/2020/01/06/hitting-refresh-on-privacy-policies-recommendations-for-notice-and-transparency/

But there is a substantial number of **businesses who <u>do not sell</u>** PI and have no future plans to sell. While these businesses do not need to display the (redundant) DNSMPI button, this writer believes that in practice, many consumers could wrongly conclude that the absence of the DNSMPI button (i.e. absence of a Do Not Sell choice) could infer that this "white hat" business is noncompliant with the spirit of CCPA and should be avoided.

W282-2 (cont.)

This negative confusion could be turned into a huge benefit for consumers and businesses alike with the addition of a displayable We Do Not Sell Your Personal Information (WDNSYPI) symbol or logo to display this DNS commitment to the consumer just in time with the presentation of other privacy facts. (Figure 2)

The OAG's February 7 release provided no information about how just-in-time notices might appear as implemented in daily practice. For your consideration, here are some snapshot examples of "just-in-time" use cases in a CCPA collection moment using the Privacy Facts Interactive Notice (PFIN) paradigm as described in our previous submission[8]:

[8] http://model.consentcheq.com/20191205-ccpa1010-comment.pdf

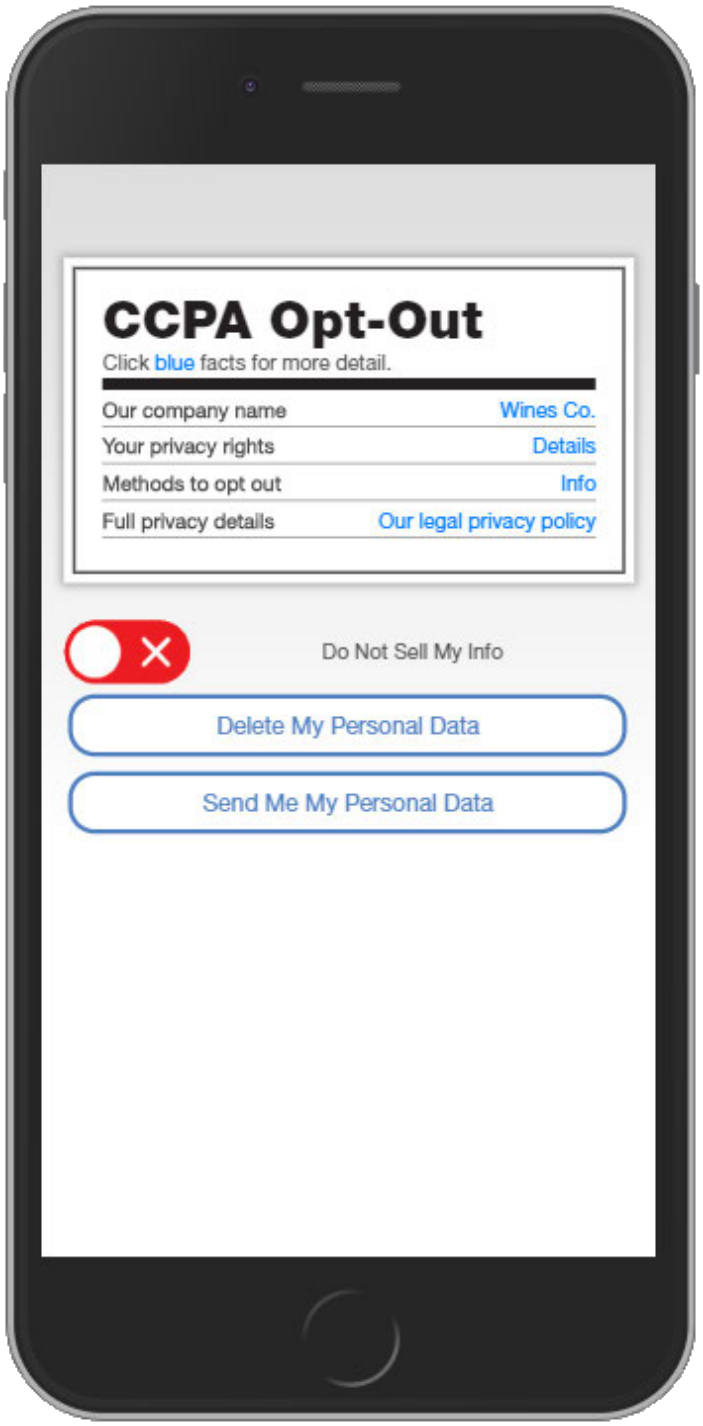


Figure 1 – Snapshot of a CCPA "Just in Time" Notice at Opt-Out

W282-2
(cont.)

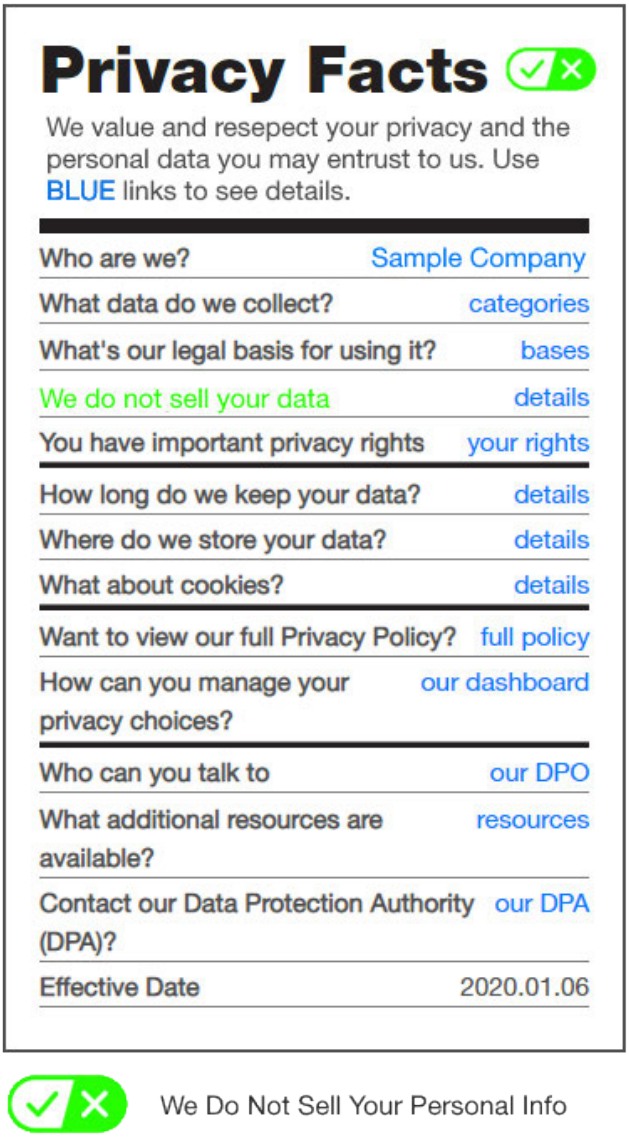


Figure 2 – Snapshot of a WDNSYPI logo used to signal "We Do Not Sell"

W282-3

PrivacyCheq

In conclusion, the flexibility, simplicity, and clarity of just-in-time notice technology enhances California consumers' positive and effective control over their personal information as it simplifies their notice and choice. For businesses, employing "just-in-time" notices provides a simplified means for building consumer dialogue and trust. It is an important and welcomed addition to the CCPA regulations.

W282-1 (cont.)

Additional information on practical CCPA just-in-time notice implementation can be found in PrivacyCheq's previous comment submission to the CCPA Proposed Regulation (closed on December 6, 2019), available here:

http://model.consentcheq.com/20191205-ccpa1010-comment.pdf

W282-3 (cont.)

Thank you for these opportunities to comment.

Sincerely,

Dale R. Smith, CIPT
Futurist
[redacted]

via email to: PrivacyRegulations@doj.ca.gov

From:	Vael
To:	Privacy Regulations
Subject:	CCPA Comments - Vael, Inc.
Date:	Monday, February 24, 2020 9:24:05 PM
Attachments:	Marriott Emial Chain.pdf CCPA Comment Letter Vael Inc..pdf

---

Hello,

Please find the attached letter regarding our organization's comments on CCPA and corresponding email chain.

Thank you,

Vael Team

Vael, Inc.

February 24, 2020

Attn: Privacy Regulations Coordinator, California Office of the Attorney General
Lisa B. Kim
300 South Spring Street, First Floor
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

Re: California Consumer Privacy Act (CCPA) Updates February 2020

Dear Lisa,

Vael, Inc., is an early stage data privacy startup based out of San Francisco, CA. From personal experience coupled with small consumer surveys, we have found that exercising CCPA rights on one's own is far more challenging and time consuming than expected. Thus, Vael is creating a solution where we can act on behalf of consumers as their authorized agent under the proposed CCPA regulations, in order to help consumers easily exercise their CCPA rights.

After contacting a few large companies, we have become increasingly concerned with the efficacy of deletion requests for consumers and how it could impact the effectiveness of the authorized agent role. Specifically, we believe the proposed regulations still provide companies the ability to discriminate their services against consumers who choose to exercise their CCPA rights. This is in reference to **§999.336**

Attached you will find an example of this, an email chain between one of our co-founders (Garrett Gillett) and Marriott's privacy team. As you can see in the beginning of the chain, we email Marriott's privacy team to inquire how a deletion request would impact one's status and accumulated points within Marriott's rewards system. In response, Marriott's privacy team confirms a CCPA deletion request would completely delete a customer's account, including all accumulated points. When asked why this was the case, Marriott responds by saying a Marriott customer's account (in its entirety), points, and status within the company are all a part of a customer's information. It seems they are unwilling to discern between those parts in order to maintain their relationship with their customer.

W283-1

Currently, companies with reward systems can effectively provide customers with two choices: 1) Let the company retain the customer's personally identifiable information or 2) the customer can choose to submit a request to delete, suffering the consequence of complete elimination of one's account, status, and points. Companies are able to get away with this treatment to customers, because they are exploiting a flaw within the proposed CCPA regulations. The current proposed CCPA regulations do not differentiate between previously accumulated financial incentives and the ability to earn future financial incentives from a company. Thus, discriminating against customers who opt to be private online. To Vael, this is an extremely binary option that disincentives privacy. Ultimately, this creates a conflict for the consumer. Companies force consumers to

thevael@protonmail.com

choose between privacy or rewards. Consumers should be able to submit a requests of their own volition rather than in a coercive environment.

What Vael proposes is the following:

1. When a consumer or authorized agent submits a request to delete, they can choose to only have personally identifiable information and behavioral data collected by the company about the consumer deleted.

2. While a request to delete should delete all data relating to the the consumer by default. If the consumer desires that only certain information be deleted (i.e. account numbers and other unique identifiers required for reward systems), it can be specified and honored in the request.

3. If a consumer or authorized agent submits a request to delete, companies should be required to honor a customer's already accrued financial incentives. Meaning, the consumer will still have access to use their already accumulated rewards, points, miles, dollars, etc. with the company, similarly to a customer who has not submitted a CCPA request to delete.

4. Removal of financial incentives to the consumer due to a deletion request, should not begin until the request to delete is received by the company. From the day the request was received by the company and moving forward, financial incentives from the company may end (if the company chooses to do so).

5. The consumer should neither be forced to receive their previously accumulated and unused financial incentives in a lump-sum, as there are circumstances where this can also be of disservice to the consumer. Should companies not allow consumers to use their already earned and unused financial incentives, companies should be required to pay the consumer fair market value (in dollars) for the rewards the company is forcing the consumer to take in a lump-sum.

W283-1 (cont.)

The goal of CCPA requests should be to achieve the highest degree of effectiveness for consumers. Allowing them to know what information they want to know, delete information they want deleted, and opt-out of any sale of their data. We want this to work and help create an environment in which this regulation can benefit consumers and enable them to achieve the privacy they want online. Vael believes authorized agents have the opportunity to create lasting and meaningful change in this new age of the Internet. We hope to add convenience, trust, and effectiveness to the lives of those wishing to take action on their data rights.

Thank you for your time and below is our contact information, we would welcome the opportunity to open a dialogue regarding our comments, concerns, and CCPA in general.

Regards,

Garrett Gillett

Co-Founder, COO

Vael, Inc.

[redacted]

[redacted]

Connor Gafner

Co-Founder, CEO

Vael, Inc.

[redacted]

[redacted]

thevael@protonmail.com

Fw: Re: Privacy Question

Received: **Monday, February 24, 2020 8:42 PM**

From: [redacted]

To: **TheVael@protonmail.com TheVael@protonmail.com**

Garrett Gillett
Co-Founder, COO
Vael, Inc.

Sent with ProtonMail Secure Email.

------- Original Message -------
On Tuesday, February 18, 2020 12:48 PM, PRIVACY <PRIVACY@marriott.com> wrote:

> Dear Garrett,
>
> A request to delete will delete a customer's information, and points and status are a part of a customer's information. The deletion will also close the customer's account because the account is considered a part of a customer's information.
>
> Sincerely,
>
> Marriott Privacy Center
>
> **From:** [redacted]
> **Sent:** Monday, February 17, 2020 7:35 PM
> **To:** PRIVACY <PRIVACY@marriott.com>
> **Subject:** Re: Privacy Question
>
> Interesting - Do you know why that is the case?
>
> Thank you,
> Garrett
>
> Sent with ProtonMail Secure Email.
>
> ------- Original Message -------
> On Monday, February 17, 2020 10:16 AM, PRIVACY <PRIVACY@marriott.com> wrote:
>
> > Dear Garrett,
> >
> > A request to delete will cause all of a guest's account to be deleted, including accumulated points and status with Marriott.
> >
> > Sincerely,
> >
> > The Marriott Privacy Team
> >
> > ---
> >
> > **From:** [redacted]
> > **Sent:** Monday, February 17, 2020 12:08 PM
> > **To:** PRIVACY <PRIVACY@marriott.com>
> > **Subject:** Privacy Question
> >
> > Hi,
> >
> > If I am a California resident and I would like to submit a Request to Delete, will that completely delete my accumulated points and status within Marriott?
> >
> > Thank you,
> >
> > Garrett
> >
> > Sent with ProtonMail Secure Email.

From: [redacted]
To: Privacy Regulations
Cc: Marc Rotenberg; Caitriona Fitzgerald
Subject: EPIC Comments RE: NOTICE OF MODIFICATIONS TO TEXT OF PROPOSED REGULATIONS
Date: Monday, February 24, 2020 6:24:51 PM
Attachments: FINAL EPIC-CCPA-Feb2020 .docx

The Electronic Privacy Information Center ("EPIC") submits these attached comments in response to the Notice of Modifications on the California Consumer Privacy Act (CCPA). EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.

We are happy to answer any questions you may have.

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

CALIFORNIA OFFICE OF THE ATTORNEY GENERAL

NOTICE OF PROPOSED RULEMAKING

THE CALIFORNIA CONSUMER PRIVACY ACT

February 25, 2020

The Electronic Privacy Information Center ("EPIC") submits these comments in response to the Notice of Modifications[1] on the California Consumer Privacy Act (CCPA). EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC has long supported the establishment of comprehensive federal privacy law and also argued that federal law should not preempt stronger state laws.[3] EPIC has also previously provided comments on the CCPA.[4]

The proposed regulations make clear that the OAG intends to establish strong data privacy protections in the CCPA for Californians. EPIC supports the efforts of the Attorney General. EPIC submits these comments to further safeguard the privacy of California consumers.

---

[1] California Dept. of Justice, Updated Notice of Modifications to Text of Proposed Regulations and Addition of Documents and Information to Rulemaking File, Title 11 (Feb. 10, 2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-mod-020720.pdf.

[2] *About EPIC,* EPIC (2020), https://epic.org/epic/about.html.

[3] EPIC, *Grading on a Curve: Privacy Legislation in the 116th Congress* (Dec. 2016) **Error! Hyperlink reference not valid.**https://epic.org/GradingOnACurve; Testimony of EPIC Exec. Dir. Marc Rotenberg on *Privacy in the Commercia World*, before the House. Subcomm. on Comm. Trade, and Cons. Protection, Comm. on Energy and Comm., 107th Cong., 1st Sess. ___ (Mar. 1, 2001), https://epic.org/privacy/testimony_0301.html

[4] Comments of EPIC to the California Office of the Attorney General, Notice of Proposed Rulemaking, the California Consumer Privacy Act (Dec. 6, 2019), https://epic.org/apa/comments/EPIC-CCPA-Dec2019.pdf . *See also EPIC Backs Strong Implementation of California Privacy Law* (Dec. 6, 2019), https://epic.org/news/2019/default.html

Section § 999.301 Definitions

The draft proposes to add the following text to the definitions of "categories of sources" and "categories of third parties:"

> (d) "Categories of sources" means types or groupings of persons or of entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They may include ~~including but not limited to~~ the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers ~~from which public records are obtained, and consumer data resellers.~~ W284-1
>
> (e) "Categories of third parties" means types or groupings of third parties with whom the business shares ~~of entities that do not collect~~ personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include ~~directly from consumers, including but not limited to~~ advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and ~~consumer~~ data brokers ~~resellers~~. W284-1 (cont.)

EPIC supports these changes. The clarifications will help consumers understand who is collecting, processing and receiving their personal information. However, actual transparency requires that consumers have specific knowledge of which third parties have access to their data and the reason for the access. EPIC encourages the OAG to consider future changes that will allow consumers to know precisely who has obtained their data and for what purpose.

The draft proposes adding the following language to the definition of "Price or Service Difference":

> (l) "Price or service difference" means (1) any difference in the price or rate charged for any goods or services to any consumer related to the disclosure, deletion, or sale of personal information, including through the use of discounts, financial payments, or other benefits or penalties; or (2) any difference in the level or quality of any goods or services offered to any consumer related to the disclosure, deletion, or sale of personal information, including the denial of goods or services to the consumer. W284-2

However, under the CCPA, a business is currently not allowed to charge a consumer for disclosing their personal information.[5] Therefore, EPIC recommends the following change deleting "disclosure" from this definition.

> (l) "Price or service difference" means (1) any difference in the price or rate charged for any goods or services to any consumer related to the ~~disclosure~~, deletion, ~~or~~ sale of personal information, including through the use of discounts, financial payments, or other benefits or penalties; or (2) any difference in the level or quality of any goods or services offered to any consumer related to the ~~disclosure~~, deletion, ~~or~~ sale of personal information, including the denial of goods or services to the consumer.

W284-2 (cont.)

Section § 999.302. Guidance Regarding the Interpretation of CCPA Definitions

The draft proposes to add the following text:

> (a) Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "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." For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be "personal information."

W284-3

EPIC recommends revising the example in the guidance as IP addresses are explicitly referenced in the definition of personal information in the CCPA[6]. As currently drafted, the provision allows companies to collect and retain IP information about users that could in fact be

[5] 1798.100(d) states: *A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section.*

[6] *1798.140**(o)(1)** states (Emphasis added): "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:* ***(A)*** *Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier,* ***internet protocol address****, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.*

made personally identifiable. That is clearly not the intent of the provision and the example should be revised.

Therefore, EPIC favors this addition with the following clarification:

(a) Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "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." For example, even if a business that collects the IP addresses of visitors to its website and does not link the IP address to any particular consumer or household, ~~and any party not reasonably link the IP address with a particular consumer or household, then~~ the IP address would ~~not~~ still be "personal information." 1798.140(o)(1)(A).

W284-3 (cont.)

Section § 999.304. Overview of Required Notices

The draft regulations propose adding the following language:

a) Every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and these regulations, including section 999.308.

(b) A business that collects personal information from a consumer shall provide a notice at collection in accordance with the CCPA and these regulations, including section 999.305.

(c) A business that sells personal information shall provide a notice of right to opt-out in in accordance with the CCPA and these regulations, including section 999.306.

d) A business that offers a financial incentive or price or service difference shall provide a notice of financial incentive in accordance with the CCPA and these regulations, including section 999.307.

W284-4

EPIC appreciates the "Overview of the Required Notices" and recommends that it is included in the final rules. The overview gives businesses clear guidance of what is required if they are a business as defined by the CCPA. However, we caution that while these notices provide effective mechanism for privacy enforcement, they typically place unfair unburdens on consumers. There is also a risk that privacy notices might operate as waivers or disclaimers, depriving consumers of rights to which they would otherwise be entitled,

Section § 999.305 Notice at Collection of Personal Information

The draft regulations propose adding the following changes:

> *(*3)(a) When a business collects consumers' personal information online, it may ~~conspicuously~~ post a conspicuous link to the notice on the introductory page of the business's ~~website homepage or the mobile application's download page, or~~ and on all webpages where personal information is collected.

EPIC appreciates the guidance for businesses about when they have to post a "conspicuous link." In fact, EPIC led a coalition of California consumer organizations in 2008 to enforce the conspicuous link provision of the California Online Privacy Protection Act of 2003 against Google when the company refused to make a link to its privacy policy accessible from its homepage.[7] We therefore recommend that the substitution of the word "must" for "may" so that the provision would read: W284-5

> *(*3)(a) When a business collects consumers' personal information online, it ~~may~~ must ~~conspicuously~~ post a conspicuous link to the notice on the introductory page of the business's ~~website homepage or the mobile application's download page, or~~ and on all webpages where personal information is collected.

We also recommend that the drafters clearly define the term "Conspicuous Link." EPIC suggests adding the following language:

> A Conspicuous Link is a hypertext link that is written in capital letters equal to or greater in size than the surrounding text; is displayed in a type, font or color that contrasts with the surrounding text of the same size; or is otherwise distinguishable from surrounding text on the homepage.[8]

---

[7] Letter from Privacy Organizations to Google CEO Eric Schmidt, June 3, 2008 ("We are writing to you on behalf of California consumers and Internet users around the world to urge Google to include a direct link to its privacy policy on its homepage."), https://epic.org/privacy/ftc/google/Google_Letter060308.pdf. *See also,* Jaikumar Vijayan, *Google Asked to Add Link to Privacy Policies,* Computerworld, June 3, 2008, https://archive.nytimes.com/www.nytimes.com/idg/IDG_852573C400693880002574 5D006675FE.html ("Rotenberg called Google's stance 'very bizarre' and said it appears to put the company in violation of California's Online Privacy Protection Act of 2003. One of the provisions in the act calls for companies to incorporate a prominent link to their corporate privacy on their home pages.") Saul Hansell, *Is Google Violating a California Privacy Law?* N.Y. Times, May 30, 2008, https://bits.blogs.nytimes.com/2008/05/30/is-google-violating-a-california-privacy-law/. Eventually, we prevailed. EPIC, *Google Adds Link to Privacy Policy*, July 7, 2008.

[8] This definition of "conspicuously posts" borrows from current California Law, the California Online Privacy Protection Act of 2003 (CalOPPA). This is the definition in CalOPPA: (*b) The term "conspicuously post" with respect to a privacy policy shall include posting the privacy policy through any of the following:*

The draft regulations propose the addition of the following language:

> (*4) When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection. For example, if the business offers a flashlight application and the application collects geolocation information, the business shall provide a just-in-time notice, such as through a pop-up window when the consumer opens the application, which contains the information required by this subsection.*

W284-6

EPIC supports the new clarifications around special just-in-time notice requirements for businesses that collect personal information that consumers may not expect. The drafter's example of the flashlight app gained national attention[9] and it would be helpful for consumers to know if other apps are following similar practices.

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

W284-7

The draft regulations propose adding the following language:

---

(1) A Web page on which the actual privacy policy is posted if the Web page is the homepage or first significant page after entering the Web site.
(2) An icon that hyperlinks to a Web page on which the actual privacy policy is posted, if the icon is located on the homepage or the first significant page after entering the Web site, and if the icon contains the word "privacy." The icon shall also use a color that contrasts with the background color of the Web page or is otherwise distinguishable.
(3) A text link that hyperlinks to a Web page on which the actual privacy policy is posted, if the text link is located on the homepage or first significant page after entering the Web site, and if the text link does one of the following: (A) Includes the word "privacy."
(B) Is written in capital letters equal to or greater in size than the surrounding text.
(C) Is written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size or set off from the surrounding text of the same size by symbols or other marks that call attention to the language.
(4) Any other functional hyperlink that is so displayed that a reasonable person would notice it.
(5) In the case of an online service, any other reasonably accessible means of making the privacy policy available for consumers of the online service.
https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC

[9] Cecilia Kang, *Flashlight app kept users in the dark about sharing location data: FTC*, Wash. Post (Dec. 5, 2013), https://www.washingtonpost.com/business/technology/flashlight-app-kept-users-in-the-dark-about-sharing-location-data-ftc/2013/12/05/1be26fa6-5dc7-11e3-be07-006c776266ed_story.html

(e) A business shall not sell the personal information it collected during the time the business did not have a notice of right to opt-out notice posted unless it obtains the affirmative authorization of the consumer.

W284-7 (cont.)

EPIC appreciates the clarification that if a business changes their privacy policy to state that they in fact do collect personal information, that business is prohibited from selling personal information it previously collected unless it subsequently obtains opt-in consent from the consumer.

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

The draft regulations propose adding the following language:

(a) A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to know

EPIC recommends that all businesses that collect personal data about consumers must provide at least two methods of contact whether or not they have a direct relationship with consumers. Many businesses, including the major social media companies, collect personal information about consumers with whom they do not have a direct relationship. It is important that those consumers can also easily contact these businesses to access their personal information.

W284-8

Therefore, EPIC recommends striking the following from §999.312(a):

~~A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to know.~~

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

W284-9

The draft regulations propose adding the following language:

(a) Upon receiving a request to know or a request to delete, a business shall confirm receipt of the request within 10 business days and provide information about how the business will process the request.

(b) Businesses shall respond to requests to know and requests to delete within 45 calendar days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request.

W284-9 (cont.)

EPIC supports the clarification. It is an important that the right to know process does not take an excessive period of time. We recommend these changes should be codified in the final regulations.

The draft proposes the following additions:

(3) In responding to a request to know, a business is not required to search for personal information if all the following conditions are met:

(a) The business does not maintain the personal information in a searchable or reasonably accessible format;
(b) The business maintains the personal information solely for legal or compliance purposes;
(c) The business does not sell the personal information and does not use it for any commercial purpose; and
(d) The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.

W284-10

EPIC opposes this proposed addition. While EPIC respects the effort of the drafters to narrow the exception and to create multiple requirements, this addition is problematic. For example, telephone companies are required by the FCC to retain call detail records on their customers.[10] That data is not searchable, it is maintained for compliance purposes, and is not sold to third parties. Even if telephone customers in California were told of this business practices, they would not have the right to obtain their personal data held by the telephone company. The provision should be removed.

The draft regulations propose adding the following language:

(4) A business shall not at any time disclose in response to a request to know 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, or unique biometric data generated from measurements or technical analysis of human characteristics.

W284-11

[10] https://www.fcc.gov/tags/record-retention

EPIC recognizes that if a business collects certain categories of sensitive personal information disclosure to a consumer of the actual information could create some privacy risks. However, whether or not it is possible to make the disclosure without risk, a consumer should still know that a business collects these types of information. Therefore, we advise that the regulations add the following language:

W284-11 (cont.)

> A business that collects such information shall disclose to the consumer which particular types of information the business has collected. For example, if a business collects a social security number it shall disclose that fact to the consumer without disclosing the specific social security number.

The draft regulations propose adding the following language:

> (d)(1) If the business sells personal information and the consumer has not already made a request to opt out, the business shall ask the consumer if they would like to opt out of the sale of their personal information and shall include either the contents of, or a link to, the notice of right to opt-out in accordance with section 999.306.

W284-12

EPIC supports the change eliminating the requirement that if a business cannot delete a consumer's personal information it should treat that deletion request as an opt-out. It is important to note that the right to opt-out of the sale of personal information is different from the right to delete personal information and some consumers may not want to opt-out of the sale of personal information especially if the business offers different financial incentives to consumers who do not opt-out of the sale of their personal information. EPIC supports this addition.

Section § 999.314 Service Providers

The draft regulations propose adding the following "permissible use":

> (3) For internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source;

W284-13

EPIC is opposed to this addition and recommends striking this language. EPIC believes that this is a loophole for service providers to use personal information in ways other than to provide the service requested by the consumer. The CCPA is clear that if personal information is disclosed to service

providers to perform a business purpose, the service provider can only use that personal information for that purpose[11] and is contractually prohibited from using it for any other purpose.[12] This addition to the regulations goes beyond the scope of what is allowed in the CCPA. It may be possible to allow a service provider to use the information provided if that information is provably anonymized or deidentified.

W284-13 (cont.)

The draft regulations propose adding the following language:

> (d) A service provider shall not sell data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business.

W284-14

EPIC recommends adding the following language to clarify that it is the business' obligation to notify any service providers who sell personal information that a consumer has opted-out of the sale of their personal information:

> A business must notify all service providers that sell data on their behalf when a consumer has opted-out of the sale of their personal information and that service provider shall be prohibited from further selling that consumer's personal information.

Section § 999.315. Requests to Opt-Out

W284-15

The draft regulations add the following language:

> (c) A business's methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-

[11] 1798.140 **(C)** The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:
(i) The business has provided notice of 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.

[12] 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.

out. A business shall not utilize a method that is designed with the purpose or substantial effect of subverting or impairing a consumer's decision to opt-out.

EPIC supports this clarification that opt-out should be easy for consumers, while addressing the current trend of businesses making it very difficult for consumers to opt-out of the sale of their personal information.[13] EPIC also recommends adding the following language to shift the burden onto businesses once a consumer has exercised their right to opt-out of the sale of their personal information: W284-15 (cont.)

> If a consumer opts-out of the sale of their personal information, the business shall notify any third parties who collect personal information about that consumer on that businesses platform, service or physical location, that the consumer has opted out of the sale of their personal information and those third parties are prohibited from collecting personal information about those consumers.

Section § 999.323 General Rules Regarding Verification

The draft regulations propose adding the following language:

> (d) A business shall not require the consumer to pay a fee for the verification of their request to know or request to delete. For example, a business may not require a consumer to provide a notarized affidavit to verify their identity unless the business compensates the consumer for the cost of notarization. W284-16

EPIC supports this addition. The CCPA is clear that a business may not charge consumers who exercise their right to know the information a business collects. The authors considered requiring consumers to submit a notarized affidavit when drafting the CCPA but rejected this requirement because it places an undue burden on consumers to exercise their rights.

[13] Geoffrey A. Fowler, *Don't' Sell my data! We finally have a law for that,* Wash. Post (Feb. 2, 2020), https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq/ ("They're not incentivized to make it easy: Amazon hid critical links in legal gobbledygook. Marketing data company LiveRamp asked me to submit a selfie holding my own ID, kidnap-victim style. Walmart asked for my astrological sign to confirm my identity. (Really.) And one business left me a voice mail, but the message included no return number … or even the name of the company. (Please call back!)… Some companies will try to shift work onto you. Airbnb and PayPal, among others, make you email them requests, rather than using web forms. Instead of a simple "do not sell" switch, companies including Mastercard make you manage a series of privacy "preferences" (as if anyone's preference would be to have their data sold). To opt out, Best Buy says you have to change your web browser to block all cookies (breaking some sites) and dig into your phone settings to turn off some advertising tracking.")

Section § 999.336. Discriminatory Practices

The draft regulations propose adding the following language:

> ~~*(b) Notwithstanding subsection (a) of this section, a*~~ *A business may offer a financial incentive or price or service difference if it is reasonably related to the value of the consumer's* ~~*data as that term is defined in section 999.337.*~~ *If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference.*

W284-17

EPIC supports this change. The proposed text will clarify the non-discrimination provision and will shift the burden to business to justify financial incentives it offers consumers.

Conclusion

In EPIC's previous comments to the Attorney General on the CCPA, we noted that much could be done to make the CCPA stronger for consumers.[14] EPIC recent report, *Grading on a Curve: Privacy Legislation in the 116th Congress*, sets out the key elements of a comprehensive federal privacy law: (1) strong definition of personal information; (2) establishment of an independent data protection agency; (3) individual rights; (4) strong data controller obligations; (5) algorithmic transparency; (6) data minimization and privacy innovation; (7) prohibits take-it-or-leave it and pay-for-privacy terms; (8) private right of action; (9) limits government access to personal data; and (10) does not preempt stronger state laws. [15] Many of those provisions could be integrated into a strong state law, and many are missing from the CCPA including stronger enforcement, strong obligations on data controllers such as data minimization, algorithmic transparency, and prohibitions on "pay for privacy" and "take it or leave it" terms. The California Legislature should consider strengthening the CCPA with these provisions.

W284-18

[14] *See supra* note 4.
[15] *See supra* note 3.

EPIC supports the Attorney General's leadership on privacy issues and work on the proposed regulations.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Mary Stone Ross*
Mary Stone Ross
EPIC Associate Director

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

From: Walsh, Kevin [redacted]
To: Privacy Regulations
Cc: Levine, David [redacted]
Subject: Comments on the proposed California Consumer Privacy Act Regulations
Date: Monday, February 24, 2020 5:33:47 PM
Attachments: SPARK CCPA Regulations Comment Letter 2-20-20 FINAL.pdf

Please find attached The Spark Institute, Inc.'s comments on the proposed text of the California Consumer Privacy Act Regulations. We appreciate this opportunity to participate in this rulemaking initiative.

Regards,

Kevin Walsh

February 18, 2020

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

Re: California Consumer Privacy Act of 2018 Regulations

Dear Attorney General Becerra,

The SPARK Institute, Inc. writes to submit comments supporting the changes your office made on February 10, 2020 (the "Revised Proposal") to its proposed regulations under Chapter 20 of the California Code that had been published on October 11, 2019 (the "Initial Proposal"). We appreciate your office's notable efforts to address the unique challenges facing employers and their benefit programs, as raised in our prior comments and hearing testimony.

We respectfully request that your office continue to support and enhance the ability of employers to provide benefits to their California employees as the California Consumer Privacy Act of 2018 ("CCPA") is fully implemented. Specifically, it is likely that The SPARK Institute, Inc. will become aware of implementation issues and hopes to maintain a dialogue with your office in the future.

As previously explained, The SPARK Institute represents the interests of a broad-based cross section of retirement plan service providers and investment managers, including banks, mutual fund companies, insurance companies, third party administrators, trade clearing firms, and benefits consultants. Collectively, our members serve approximately 95 million employer-sponsored plan participants. Our comments reflect our unique perspective and our goal of advancing critical issues that affect plan sponsors, participants, service providers, and investment providers.

The SPARK Institute believes in the protection of consumer data and supports the goals of the CCPA. We encourage you to finalize the Revised Proposal as it relates to employment-related benefits and employment-related information, subject to the comments below.

In addition, we ask that your office support efforts in the California legislature to ensure that the employment and benefits specific pieces of CCPA do not sunset at the end of 2020. If CCPA's employment-related information provisions are allowed to expire at the end of 2020, it may become impossible for employers to continue to provide the types of benefits that hard working California employees expect.

COMMENTS FROM THE SPARK INSTITUTE

A vital mission of The SPARK Institute is the promotion of employer-sponsored retirement plans, because those plans play a critical role in helping every hardworking American retire with financial security. We appreciate the time your office has put into addressing our concerns. Rather than rehashing each of the changes requested in our initial letter, this letter notes The SPARK Institute's express support for two items in the Revised Proposal and highlights two of our most significant remaining concerns relating to employment-related benefits. Additionally, we raise one new item for your office's consideration.

- We support the Revised Proposal's definition of "Employment benefits" as "retirement, health, and other benefit programs, services, or products to which consumers or their beneficiaries receive access through the consumer's employer". The SPARK Institute believes it is important to define benefits broadly. In employment-related benefits space, there has been a proliferation of health wellness programs that are employer-based but that are not generally part of a federally regulated plan. For example, many employers are offering smoking cessation programs. In the financial benefit space, the past few years have seen a focus on student-debt in addition to retirement. Additionally, there is an emerging focus on holistic benefit wellness programs that address employee's health and retirement concerns in a unified format. With employers and their service providers rapidly innovating to better help employees meet their debt and savings needs, it is important that the CCPA be broadly interpreted to permit employers to continue to meet the needs of their employees. W285-1
- We support the addition of "Administering employment benefits" as a "business purpose". As described in our initial comment letter, absent this change, none of the "business uses" fit clearly. This omission could have limited an employer's ability provide a social good by offering retirement, health, and wellness benefits to employees.
- We ask that it be made clearer that a business collecting employment-related information can provide a single notice to the employee which would satisfy the business's obligation to provide a notice at collection to each member of the employee's household. While we believe this outcome to be the intent of the Revised Proposal, this ambiguity could be resolved through a new subsection 999.305(e)(3). To highlight this concern, it is not entirely clear if an employer can allow a parent to enroll their adult daughter or son who does not live with the parent in the employer's health plan as adult children may not fit under the current definition of 'household'. W285-2
- We reiterate or prior request that your office provide a model notice to minimize the burden on employers.
- More and more plans and service providers are facing fraudulent distribution requests. These include phone calls from fraudsters and attempts to hack online benefit interfaces. Section 999.323 recognizes that when a business receives a request for information or for deletion of data that "a more stringent verification process" is warranted where personal information would be more attractive to fraudsters and that a "verification process" should be "robust to protect against fraudulent requests or being spoofed or fabricated." One technique being developed by benefit service providers to detect and prevent employee retirement savings and health records is to record and share with other service providers the W285-3

voice prints from calls from known fraudsters and the IP addresses from which fraudulent requests are made. We ask that your office make clear that the collection and sharing of this information, to prevent fraud and identity crimes is not within the scope of CCPA such that no notice before collection is required or right of deletion or other provision of CCPA would be interpreted to prevent employers and their service providers from developing tools and sharing information to prevent the theft of employment benefits.

W285-3
(cont.)

The SPARK Institute believes that CCPA can operate in a manner that protects consumers while avoiding interference with retirement plans, employer provided student-loan assistance programs, financial wellness programs, health plans, and other initiatives where employers provide non-monetary benefits or access to benefits to their employees.

We look forward to continued engagement with California as we seek to ensure that CCPA advances the privacy goals of California residents while also not interfering with the employee benefit programs that California residents rely upon today.

* * * * *

The SPARK Institute appreciates the opportunity to provide these comments to the Attorney General. If you have any questions or would like more information regarding this letter, please contact me or the SPARK Institute's outside counsel, David Levine and Kevin Walsh, Groom Law Group, Chartered ([redacted] or [redacted]).

Sincerely,

Tim Rouse
Executive Director

From:	Brad Batig
To:	Privacy Regulations
Subject:	CCPA Proposed Regulations Comment re Section 999.314(b)
Date:	Monday, February 24, 2020 4:36:14 PM

Agency: California Office of the Attorney General
Docket No.: OAL File No. 2019-1001-05
GC Services Limited Partnership | California Consumer Privacy Act Regulations

Please allow this to serve as our comment in response to the California Office of the Attorney General's revised proposed regulations regarding the California Consumer Privacy Act ("CCPA").

Our comment is a request for clarification regarding proposed **Section 999.314(b)**. The revised rule currently reads:

> To the extent that a business directs a second business to collect personal information directly from a consumer on the first business's behalf, and the second business would otherwise meet the requirements and obligations of a "service provider" under the CCPA and these regulations, the second business shall be deemed a service provider of the first business for purposes of the CCPA and these regulations.

We are asking for a modification of or clarification in Section 999.314(b) so that a Service Provider is a business that is asked by another business to "collect personal information directly from a consumer, or about a consumer, on the first business's behalf."

W286-1

We are a business processing outsourcing company who primarily serves as a call center or collection agency for our clients. For certain third party collection programs, our clients ask us to help them, among other things, find good contact information about their customers so that our clients are able to update their records regarding their customers' current information, including such items as mailing address and preferred phone numbers. Most of the time, the information we obtain comes directly from our clients' customers (i.e., the "consumers"). However, we also obtain possible contact information potentially about our clients' customers from data enrichment vendors or from other third parties.

Since enactment of the CCPA, many of our clients have taken the position we are their "Service Provider." We believe the Attorney General's currently proposed regulations confirm our clients' interpretation of the CCPA. However, making our requested modification – or providing clarification on this topic – would assist us, and companies like us, in understanding our compliance requirements for the CCPA and implementing regulations.

Thank you for your consideration.

Brad Batig
Chief Compliance Officer & General Counsel
GC Services Limited Partnership
6330 Gulfton
Houston, Texas 77081

Office: [redacted]
[redacted]

From: Ide, Kimberly
To: Privacy Regulations
Subject: CCPA Modified Proposed Regulations technical comment
Date: Monday, February 24, 2020 4:24:00 PM
Attachments: image001.png
CCPA technical comment (2.24.2020).pdf

I have attached a technical comment from the Office of the County Counsel, County of Santa Clara.

Kimberly Ide | Confidential Legal Secretary
Office of the County Counsel, County of Santa Clara
70 West Hedding Street, East Wing, 9th Floor | San José, CA 95110
Office: [redacted] | Facsimile: (408) 292-7240
[redacted]

OFFICE OF THE COUNTY COUNSEL
COUNTY OF SANTA CLARA

County Government Center
70 West Hedding Street
East Wing, 9th Floor
San José, California 95110-1770

[redacted]
(408) 292-7240 (FAX)

James R. Williams
COUNTY COUNSEL

Greta S. Hansen
CHIEF ASSISTANT COUNTY COUNSEL

Robert M. Coelho
Steve Mitra
Douglas M. Press
Gita C. Suraj
ASSISTANT COUNTY COUNSEL

February 24, 2020

VIA EMAIL

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

Re: Comment of the Office of the County Counsel, County of Santa Clara on the Attorney General's Modified Proposed Regulations Implementing the California Consumer Privacy Act (OAL File No. 2019-1001-05)

Dear Ms. Kim:

I write on behalf of the Office of the County Counsel, County of Santa Clara to provide a technical comment on the Attorney General's Modified Proposed Regulations dated February 10, 2020, implementing the California Consumer Privacy Act (CCPA). The County has robust privacy and data security protections for all personal information gathered by the County and is one of the few counties in the country to have a dedicated chief privacy officer. The County is committed to privacy protections for all individuals and looks forward to implementation of the CCPA and the regulations. The Office of the County Counsel recommends a technical edit to the regulation to clarify the scope of the CCPA's requirements for service providers.

The CCPA's requirements apply to "businesses" and "service providers." The CCPA's definition of "business" includes only certain for-profit entities that collect consumers' personal information.[1] The definition of "service provider," in turn, includes for-profit entities that "process[] information on behalf of a *business*" in certain circumstances.[2] Accordingly, when a for-profit entity is processing information on behalf of a government entity, it is not acting as a

W287-1

[1] Cal. Civ. Code § 1798.140(c).

[2] *Id.* at § 1798.140(v) (defining a service provider as "a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a *business*…") (emphasis supplied).

"service provider" within the meaning of the CCPA. Section 999.314(a) of the modified proposed regulation addresses the CCPA's definition of "service provider." The section states:

> A business that provides services to a person or organization *that is not a business*, and that would otherwise meet the requirements and obligations of a "service provider" under the CCPA and these regulations, shall be deemed a service provider for purposes of the CCPA and these regulations. (Emphasis supplied.)

This Section could be interpreted as deeming businesses that provide services to government entities as "service providers" subject to the CCPA, which is contrary to the definition of "service provider" in the CCPA.

For these reasons, the Office recommends the following clarification to Section 999.314(a) of the regulation (proposed addition in underline): W287-1 (cont.)

> (a) A business that provides services to a person or organization that is not a business, and that would otherwise meet the requirements and obligations of a "service provider" under the CCPA and these regulations, shall be deemed a service provider for purposes of the CCPA and these regulations. Notwithstanding the foregoing, a business shall not be deemed a service provider for purposes of the CCPA and these regulations to the extent the business is providing services to a government entity.

This clarification is consistent with the CCPA's definition of service provider and would provide additional guidance to for-profit entities that perform services for a government entity.

Very truly yours,

JAMES R. WILLIAMS
County Counsel

From:	Annie Bai
To:	Privacy Regulations
Cc:	Compliance
Subject:	Comment on proposed CCPA regulations [OAL File No. 2019-1001-05]
Date:	Monday, February 24, 2020 2:31:29 PM
Attachments:	Comment on CCPA Proposed Regs of 10.feb.2020 .pdf

To the Office of the Attorney General:
Please see the attached comments submitted by Socure, Inc., a leading identity verification solution.

--

Annie C. Bai, Esq., CIPP/US, CIPM, FIP, CIPP/C
Privacy & Compliance Officer
[redacted]

Follow us on: LinkedIn, Instagram, facebook and Twitter

REAL IDENTITY VERIFICATION

To: Xavier Becerra, Attorney General of California

By: Socure, Inc.

Subject: California Consumer Privacy Act ("CCPA") Proposed Regulations

Comment on the Notice of Modifications to Text of Proposed Regulations Issued by the California Attorney General February 10, 2020 [OAL File No. 2019-1001-05]

Date: February 24, 2020

Socure submits this comment with regards to the requirement to verify consumer requests for access or deletion under §1798.100, §1798.105, §1798.110, and §1798.115. The purpose of the CCPA is to empower consumers with knowledge and control over the use of their personal information ("PI"). However, it is critical that the rights not be misappropriated to acquire valuable PI or otherwise negatively impact consumers and businesses. Warnings have been repeatedly trumpeted on the possible ways in which this could happen -- impersonating consumers with stolen data can range from manual to automated or mass requests, spoofing to deceive call centers, and other forms of deception, including but not limited to corporate espionage, throughout the request process.

As a company that works on the front lines of preventing identity fraud, Socure is concerned that the proposed guidance does not sufficiently require businesses to verify the identity of CCPA requestors at a standard comparable to our industry's best practices. Although identity verification as a science may be new to compliance officers, there is an entire industry of expertise that deals with the challenges of verifying digital and remote interactions. We know that identity verification can be conducted in a empirical, reliably accurate, and secure manner, but it requires expertise and technical solutions beyond those set forth in the draft guidance.

W288-1

The Rulemaking File includes reports and findings on the effects of massive data breaches and the extent of identity theft in our modern digital world. Such stolen data and other identity misrepresentation exploits are readily available to be leveraged for spoofing CCPA requests. Malicious or vexatious CCPA requests will expose individuals to additional risks of identity harms, as well as businesses to risks of data breach and impact to data-dependent processes and systems.

Currently, Article 4 of the proposed guidance, at §999.323(b)(1), advises business to *either* match submitted personal information against a business' data *or* to use a third-

party independent verification service *whenever feasible.* There are multiple flaws with this limited instruction.

> (1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section.

First, the standard of *whenever feasible* is vague and not aligned with the risk-based principles espoused in §999.323(b)(3)b. and c. It is possible that this phrase was intended to only qualify the clause on using already maintained data to verify requestors. Moreover, it is always feasible to conduct some manner of identity verification.

Second, it is woefully insufficient to permit a business to verify identity solely upon the basis of data that it already holds. Due to massive data breaches and hacks, static forms of data are unreliable for verification purposes. They must be paired with, or correlated to, real-time data such as IP address, browser or device information, or image features such as selfie upload or liveliness check.

W288-1 (cont.)

Socure recommends that Article 4 mandate a two-factor verification process.

> (1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, ~~or~~ and
>
> (2) Independently verify that the requestor is the consumer via an additional element of trust such as in-person checks, documentary submissions, real-time digital verification, or the use an identity verification service that complies with this section.

CCPA's consumer verification requirements are the gateway to accessing valuable new rights or engendering new risks to privacy. We in the fraud prevention field are keenly familiar with the pitfalls around trying to verify identity on a mass and impersonal scale. It is our hope that the Attorney General will direct businesses to employ best practice techniques and services to conduct accurate, reliable and secure verified consumer requests.

From:	Frank Salinger
To:	Privacy Regulations
Cc:	Toni A. Bellissimo
Subject:	Comments of the Card Coalition-OAL File No. 2019-1001-05
Date:	Monday, February 24, 2020 1:57:36 PM
Attachments:	CCCAAGCCPAFinal22420filed.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] (office)
[redacted] (mobile)
[redacted]
For my tweets about politics: https://twitter.com/KStreetLawyer

Card Coalition P.O. Box 802 Occoquan, VA 22125-0802 ☏ 703.910.5280

February 24, 2020

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 Updated Notice of Modifications to the Text of Proposed Rulemaking published on February 10, 2020 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 Enforcement Date of Final Regulation Should Be Delayed

W289-1

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]

[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] *See:* https://oag.ca.gov/system/files/initiatives/pdfs/Title%20and%20Summary%20%2819-0021A1%29.pdf2020 (Ballot Initiative No. 19-0021)

Given how rapidly technology, and individual expectations in light of that technology, is evolving, as well as the difficultly of responding to ever-changing referendum language, going forward with this rulemaking is precipitous.

As you will see below, we believe a number of the proposed regulations make substantive changes beyond the scope of CCPA, which ideally would be better addressed through the legislative process or by referendum. Absent this, there must be an acknowledgment that the ability for businesses to assess and develop processes to ensure maximum compliance while addressing the requirements under the law itself is incredibly onerous and necessitates a reasonable amount of time for businesses to prepare for compliance. W289-1 (cont.)

With this current political backdrop, we again urge you to postpone the enforcement date of the final regulations for a reasonable period after they become effective until the totality of the CCPA's impact on consumers and businesses is understood 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 regulation around the use and disclosure of personal data, the payment card industry is subject to comprehensive federal regulation, including a robust and effective privacy regime. We urge policymakers to recognize that the global payment system requires transparent and consistent rules of the road on a national scale.

While we acknowledge 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] W289-2

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 con-

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).

sumers 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). Each likewise have substantial data security requirements to protect this personal information.

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.

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 notices[6], which are a safe harbor for financial institutions that use them – virtually all do.

W289-2
(cont.)

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]

---

[5] Ibid.

[6] *See* Appendix to 12 CFR §1016.

[7] op. cit.

While the CCPA does contain a— limited and rather clunkily drafted—GLBA exception[8], it should be supported with a safe harbor for already comprehensively regulated businesses like financial institutions. We note that, unlike unregulated businesses, financial institutions are required to undergo regulatory compliance examination by state a federal agencies.

c. The Need for a Safe Harbor Remains

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]

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]

W289-2 (cont.)

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 continue to recommend the Attorney General use the authority granted by the CCPA to provide a safe harbor for businesses that maintain appropriate data security practices promul-

---

[8] CCPA §1798.145(e)

[9] Initiative 17-0039.

[10] A brief history and timeline are available at https://www.caprivacy.org/about-us

[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.

gated by federal regulators or recognized national and international standards-setting organizations.[13]

W289-2 (cont.)

d. The Regulations May Inadvertently Be Used by Fraudsters

Financial institutions and payment networks constantly combat fraudsters seeking access to consumers' money and financial information. Certain provisions in the draft regulation, although well-intended, may open up vectors for fraudsters to gather information concerning banks' identity theft and fraud prevention methods and may conflict with other bank and network obligations.

W289-3

For example, proposed section 999.308(c)(1)(c) and (2)(c): [The privacy policy shall] state a business must: "Describe in general the process the business will use to verify the consumer request [for access or to delete], including any information the consumer must provide." Furthermore, proposed section 999.325 states: "If the business has no reasonable method by which it can verify any consumer, the business shall explain why it has no reasonable verification method in its privacy policy."

We are concerned these provisions may provide operational insight to fraudsters and hackers and urge you to review the draft regulations to minimize these impacts.

II. AREAS OF OPERATIONAL CONCERN IN THE PROPOSED REGULATION

a. Proposed §999.305(a)(4) – data collection a consumer would not reasonably expect

Section 999.305(a)(4) requires just-in-time notice of collection that for a purpose "that the consumer would not reasonably expect" and provides a clear description of an extreme case: A consumer would not reasonably expect a flashlight app to collect geolocation information. It is not clear, however, which lesser extreme situations would similarly trigger this requirement.

For example, many fraud-prevention mechanisms employed by the financial services industry use device geolocation as one factor among many in assessing whether a particular requested transaction is indicative of fraud.

W289-4

Although the fact of collecting geolocation would be disclosed appropriately in the notice at collection, an additional pop-up notification could prove difficult to implement and may subvert the purpose of the fraud-prevention mechanism in the first instance, by alerting fraudsters to the timing and structure of banks' fraud prevention methodologies. We would argue that consumers would reasonably expect their bank to protect them from fraud in a variety of ways, but inclusion of this provision introduces ambiguity.

---

[13] *See, for example:* International Organization for Standardization (ISO), Payment Card Industry Security Standards Council (PCI SSC).

b. Proposed §999.305(a)(5) – 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 a purpose materially different than what was disclosed in the notice 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. W289-5

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 information[14], participation in an entity's financial incentive program[15], and retention of a consumer's personal information for the purposes of peer-reviewed scientific, historical, or statistical research in the public interest[16].

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.

c. Proposed Section § 999.308 (b)(1)(d) - collection of personal information

While this section has been improved, it continues to 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. W289-6

d. Proposed Section § 999.313 (c)(3) - disclosure of personal information

The wholesale deletion of a critical security control opens businesses to significant security risk and unnecessarily exposes consumer personal information to potential theft and misuse. As articulated in the original draft regulations, businesses that could demonstrate that the release of certain personal information would create, "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," were not compelled to enable the creation of those risks by disclosing the data in response to a data access request. W289-7

Now, by removing this important clause without proposing any alternative language to protect against these risks, the regulations weaken the security of personal information by facilitating the creation of new avenues for hackers and other fraudsters to, as described above, leverage the

---

[14] 1798.120(d).

[15] 1798.125(b)(3).

[16] 1798.105(d)(6).

CCPA to attack businesses and steal the personal information of consumers for their own purposes. The original draft text set out specific criteria for businesses to meet so as to ensure that businesses would not leverage the exemption as a larger loophole for compliance with the CCPA. Only when a risk can be shown to be 1) substantial, 2) articulable, and 3) unreasonable could the exclusion be leveraged. W289-7 cont.

We urge you to reinstate the original language and allow businesses to have the ability to protect both their networks and the personal information they hold.

e. 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—originally forced covered entities to treat an unverified request from an unidentified person as a valid request to opt-out of the sale of information. As modified, a business must ask a consumer whether they want to opt out the sale of information. While a marginally better requirement, this continues to present operational challenges. W289-8

We urge you to strike this section.

f. Proposed §999.313(d)(3) – deletion on backup systems

We believe this section has been clarified and our earlier concerns have been addressed. W289-9

g. 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). W289-10

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.

h. §999.314(d) – service providers

We believe this section has been somewhat clarified and our earlier concerns are largely addressed. 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. W289-11

While we welcome the clarification, we remain concerned with the ability for a service provider to unilaterally respond to a consumer's access or deletion request without the benefit of allowing the business with whom the consumer has the actual relationship undertake appropriate verification to determine the validity of the request and/or whether the business believes the applicable information should not be deleted because of one of the enumerated CCPA exceptions.

i. 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 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? W289-12

The modified text recognizes that this is an issue by adding *en futuro* text presumably referring to, as yet undeveloped technology, *e.g.*, "Any privacy control developed in accordance with these regulations…shall require…and shall be designed….". Will your office accredit the technology when it is developed? Will your office publish an announcement that it has been developed?

We believe this section continues to find both covered entities and your office unprepared from the consumer, business, regulatory compliance, and enforcement perspectives. We urge you to strike this section.

j. Proposed §999.317(g)(1) – required metrics display

This section requires a covered entity that receives, sells, or shares the personal information of 10 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. W289-13

While we welcome the change from 4 to 10 million customers, the 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.[17] 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.[18]

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. While itemizing the reasons for denial may be a slight amelioration, doing that requires additional systemic build at significant expense which many businesses may not be in a position to perform. W289-13 (cont.)

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 right of action under the CCPA. We urge you to strike this potentially barratrous section issued under questionable authority.

k. Proposed §999.323 (d) – verification of requests

The new requirement that businesses not charge consumers for proper identity verification is poorly constructed and over-broad. Paired with the example highlighted in the modified draft, this new language effectively discourages the use of notaries, which is a commonly accepted legal method for authenticating the identity of an individual. The Uniform Statutory Form Power of Attorney (Cal. Probate Code Section 4401) even references the attachment of a required notary certification[19]. W289-14

When read in tandem with Proposed §999.326 (b), which explicitly references the Probate Code's requirements as a means for businesses to streamline the verification of Authorized Agents, the new text in Proposed §999.323 (b) creates an unnecessary barrier to consumer choice and a direct conflict with Proposed §999.323 (e)'s requirement that businesses "implement rea-

---

[17] Cal Civ. Code §1798.185(a)(4)

[18] Cal Civ. Code §1798.185(b)(2)

[19] The form explicitly states, "Include certificate of acknowledgment of notary public in compliance with Section 1189 of the Civil Code or other applicable law." Cal. Probate Code Section 4401.

sonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information."

Businesses required to ensure the security of the personal information they are tasked with disclosing or deleting should not be penalized for employing a separately required method for authenticating legal affidavits signed by consumers. W289-14 (cont.)

We recommend that the regulations make clear that use of a notary to verify the identity of the consumer does not trigger a monetary penalty to businesses looking to secure personal information when a consumer chooses to exercise his or her rights under the CCPA.

l. Proposed §999.331 – relating to minors

We believe this section has been clarified and our earlier concerns are largely addressed. W289-15

III. CONCLUSION

The Card Coalition appreciates the opportunity to share our views on the Modifications to the Text of Proposed Regulation and the underlying text as originally proposed and would be pleased to discuss our specific concerns outlined above. Thank you for your consideration.

Respectfully submitted,

Toni A. Bellissimo
Executive Director

Frank M. Salinger
General Counsel

Card Coalition P.O. Box 802 Occoquan, VA 22125-0802 ☏ 703.910.5280

https://cardcoalition.org

From: Shawn Yadon
To: Privacy Regulations
Subject: California Trucking Association Comments To the Revised Proposed Regulations Modified Feb 10, 2020--CCPA
Date: Monday, February 24, 2020 1:05:19 PM
Attachments: image002.png
image003.png
CTA - 2nd Letter to AG with CCPA Comments Feb 2020.PDF

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

On behalf of the California Trucking Association (CTA), attached please find comments pertaining to the revised proposed regulations (as modified February 10, 2020) concerning the California Consumer Privacy Act (CCPA).

Should you require any further information, please do not hesitate to contact me.

Kind regards,

Shawn Yadon | CEO
California Trucking Association
4148 East Commerce Way
Sacramento, CA 95834
T: [redacted] | **E**: [redacted]
W: www.caltrux.org

We drive for a living. Safety is our priority.

February 21, 2020

Attorney General Xavier Becerra
Office of Attorney General
1300 "I" Street
Sacramento, CA 95814-2917

Re: Transportation Industry Comments on Proposed Modified CCPA Regulations

Dear Attorney General Becerra,

The California Trucking Association (CTA) appreciates the interest of the Attorney General's Office in CTA's concerns regarding the modified proposed regulations (the "Modified Regulations") published by the California Attorney General's Office under the California Consumer Privacy Act (the "CCPA"). We appreciate the continuing efforts of the Attorney General's Office to craft regulations under the CCPA in order to fulfill its mandate under the statute. We have certain fundamental concerns with how the Modified Regulations may be interpreted, however, and the resulting potential impact across the package transportation industry.

1. The CCPA and the Package Transportation Industry.

The CCPA will regulate package transportation providers as businesses operating in California that collect personal information relating to California consumers. For package transportation companies, certain unique CCPA issues arise from the fact that a significant portion of the personal information processed in core, day-to-day operations is received not directly from consumers, but instead from retailers and other corporate customers. This information takes the form of addressing details and package-related information, such as package dimensions and weight (collectively, "Shipping Information").

When a consumer purchases a product online, the consumer does so knowing that the retailer will either ship the product to the consumer by common carrier, or hold the product for pickup. Consumers fully understand, when they enter a "ship to" address online, that the retailer will share that information with a delivery provider. This clear consumer direction, and the associated need of package transportation providers to use Shipping Information not only to effect each individual delivery but to operate and improve their databases of addressing and mapping information and their

transportation networks, raise several key questions under the CCPA. Our comments below relate to the issues we view as most critical:

A. Sharing Shipping Information with package transportation companies should not constitute a "sale" of personal information. This is critical because a different finding would mean transportation providers receive Shipping Information only as "service providers" – a result that would be inconsistent with consumer expectations and would significantly impair the transportation industry, with no corresponding consumer benefit. W290-1

B. The Modified Regulations remove the very narrow limitation that the original version of the proposed regulations would have imposed on how service providers can use personal information. But the new limitations, while admittedly more broad, do not correct the fundamental problem that the regulations create for the package transportation industry. W290-2

2. Sharing Data with Package Transportation Companies to Ship Packages Should be Deemed a Consumer-Directed Transfer of Personal Information that Does not Constitute a "Sale."

It is critical to the package transportation industry to confirm that retailers and other corporate customers do not "sell" Shipping Information when they provide that information to transportation providers. This clarification is of fundamental importance to the transportation industry, due to the scope of the definition of "sell" in the CCPA, because transportation providers inherently use Shipping Information for more than simply to deliver each individual package to each individual address. Shipping Information is inherently embedded into the operations of transportation providers, similar to how an organization might consume and integrate fuel or other supplies into its operations. For example:

- Carriers use Shipping Information continuously and on an automated basis for package routing within their networks; transportation and delivery planning and optimization; and to make decisions about package network optimization (including locations of facilities, retail outlets, staffing, "drop boxes" where consumers can pick up and leave packages, and capital investment). They do not simply use the information to deliver a specific package and then forget it.

- Shipping Information constitutes a combination of information received from customers, plus information carriers append from their own historical information and operations (including very specific details of package handling, status, and routing within a package network), and information they receive from third parties. The individual elements received from customers are integrated into this data and are not reasonably capable of being pulled back out.

    - Carriers continuously and automatically update Shipping Information about individual packages with additional information concerning individual shipment attributes, and operational details and requirements for shipments meeting such attributes (e.g., handling of a particular package due to its dimensions and weight ("DimWeight") or service level (e.g., standard vs. priority)) in order to fulfill deliveries and operate and improve the carrier's package transportation network. Carriers do this in order to route large numbers of deliveries to the right place at the right time, to manage the transportation network, and to improve the shipping network for future deliveries.

W290-1 (cont.)

- One of the more prominent examples of this is addresses: annually, carriers often correct tens or hundreds of millions of addresses that customers have submitted to them using information carriers collect while delivering packages, or from data acquired from, e.g., the US Postal Service. Once an address is corrected, it enables future shipments from any other corporate customer to reach that same address as desired by the consumer(s) resident at that address.

The use of Shipping Information by transportation providers beyond the simple delivery of each individual package to each individual address, when requested not by the individual consumer but by a retailer or other corporate customer, could therefore be considered to result in a sale of that information by the retailer to the carrier, but for the exception in Cal. Civ. Code § 1798.140(t)(2)(A).

- Subsection 1798.140(t)(2)(A) provides that a business does not "sell" personal information when consumers "direct the business to intentionally disclose personal information." This is precisely what happens when consumers order goods from carriers' corporate customers that need to be shipped.

- Specifically, when consumers buy products, they are directing retailers and other corporate customers to disclose Shipping Information to a transportation provider, instead of making their own separate arrangements with a transportation provider directly or, when applicable, directly picking up the merchandise from the corporate customer's facility. In fact, consumers generally pay a separate and extra charge for shipping, arguably affirmatively obligating the corporate customer to share information with a transportation provider for shipping purposes.

- To exempt consumer-directed data disclosures from being a "sale," the CCPA does not require that the consumer specify precisely who should receive their personal information. Instead, the § 1798.140(t)(2)(A) requires only that the consumer "direct" a retailer or manufacturer to "intentionally disclose" their information. Consumers who purchase merchandise from retailers or manufacturers have exactly this in mind – that their data will be provided to a carrier that will deliver the merchandise to them.

W290-1 (cont.)

Shipping Information remains protected under the CCPA in the hands of the carrier. Carriers are businesses that determine the purposes and means of the processing of Shipping Information and must comply with the CCPA, including the various privacy obligations and protections established by the statute. This information is also protected by a longstanding federal law that regulates its handling and disclosure.[1]

We believe the plain meaning of the CCPA establishes that retailers and other corporate customers transfer Shipping Information to transportation providers outside the definition of a "sale" pursuant to the direction of the consumer purchasing the product. But our members are seeing certain corporate customers interpret the law differently, positioning carriers as "service providers" as defined in the CCPA, out of a concern that disclosing data to a separate "business" carries a "sale" risk. This result would narrowly limit how package transportation providers can use Shipping Information in a manner that would impair the quality, competitiveness, and efficiency of transportation services with no corresponding benefit to consumers.

[1] See 49 U.S.C. § 14908.

3. **The Modified Regulations Would Prohibit the Package Transportation Industry from Using Shipping Information for Common and Essential Internal Purposes without any Corresponding Benefit to Consumers.**

W290-2 (cont.)

A finding that transportation providers receive Shipping Information as "service providers," and not pursuant to the direction of the consumer under Cal. Civ. Code § 1798.140(t)(2)(A), would fundamentally impair transportation industry operations and would be inconsistent with consumer expectations.

a. Consumers Have Direct Relationships with Package Transportation Providers.

When an individual consumer directly hires a carrier to ship a package, that carrier clearly acts as a business with respect to the consumer, not a service provider. The carrier thus has the corresponding obligations of a business under the CCPA, such as to accept and fulfill requests to know and requests to delete.

W290-3

But if carriers are deemed to constitute service providers, and not businesses, when the shipper happens to be a corporate customer, then the carrier's obligation will be to direct a consumer submitting a request back to the corporate customer. This is an inefficient result which would create a risk of consumer confusion. Indeed, our members' experience is that consumers continue to see themselves as having direct relationships with the individual carriers delivering shipments to them, whether in connection with tracking shipment status, submitting claims, or requesting privacy-related information.

b. A "Service Provider" Designation under the CCPA Will Create Fundamental Operational Issues for the Package Transportation Industry.

The designation of transportation providers as "service providers" would also create a more fundamental problem. This is because, as we discuss in Part 2 above, transportation providers inherently use Shipping Information received about an individual package for more than simply to deliver that package to the designated destination address. Shipping Information is inherently embedded into the operations of transportation providers and is therefore used for other transportation, planning, and operational purposes in the future.

W290-2 (cont.)

While we believe that the uses described in Part 2 fall within the permitted uses for service providers under the statutory language in the CCPA, both the original proposed CCPA regulations and the new Modified Regulations would preclude this finding.

- The CCPA permits corporate customers to share personal information with service providers for "business purposes" subject to appropriate contractual terms. The statute defines "business purposes" to include using personal information for 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." Cal. Civ. Code § 1798.140(d)

- We believe that, if deemed service providers, carriers' uses of Shipping Information would fall within this definition as "operational purposes, or other notified purposes" that have been notified via carriers' consumer-facing privacy policies, and which are "reasonably necessary and proportionate . . . or . . . compatible with the context in which the personal information was collected [by the corporate customer]." Id.

Even if this interpretation is correct – which we believe to be the case – we anticipate corporate customers may take a different position as a risk management measure because of concerns about other potential constructions of the law. The Modified Regulations make this situation even more perilous for the industry.

c. If Deemed a "Service Provider" Subject to the Restrictions in the Proposed Regulations, Package Transportation Providers Will Need to Disregard and Ultimately Discard Shipping Information about Each Individual Package after Delivery. This Result Would Impair Commerce and Harm Consumers, with no Corresponding Consumer Benefit.

The draft text of § 999.314(c) within the Modified Regulations would limit the ability of service providers to use personal information received from customers to certain defined purposes, including:

> For internal use by the service provider to build or improve the quality of its services, ***provided that the use does not include building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source*** . . . .

Modified Proposed CCPA Regulations, § 999.314(c)(3) (emphasis added).

As stated above, we believe that package transportation providers are businesses, and not service providers, and that when retailers and other corporate customers share Shipping Information with carriers they do so at the direction of consumers pursuant to Cal. Civ. Code § 1798.140(t)(2)(A). But unless this is clarified through the Attorney General's rulemaking process, we anticipate corporate customers will continue to insist on carriers accepting the designation as "service providers" under the CCPA. The current language of § 999.314(c), if adopted, would therefore preclude transportation providers from using Shipping Information for fundamental, inherent, and accepted purposes that do not create privacy risks for consumers. W290-2 (cont.)

- For example, if deemed a service provider, then once a carrier delivers a package, the carrier would not be able to use that delivery address (which in and of itself may qualify as personal information under the CCPA) or any details about the delivery (e.g., the precise location of a drop-off point) to facilitate the next delivery to that address. This is because the Modified Regulations would prohibit "cleaning or augmenting data acquired from another source." Fundamental address correction processes discussed in Part 2 above would be prohibited, as would the retention and use of Shipping Information to update existing transportation operations data to manage the transportation network or improve the shipping network for future deliveries.

- This is not in the consumer's interest – as correct address information and details about the delivery point enable carriers to operate more efficiently, provider a higher level of service, and lower costs. And this finding would provide no consumer benefit. Carriers themselves are directly accountable to consumers under the CCPA.

- Carriers would also apparently be precluded from taking the position that accepted uses such as address correction are "proportionate" and "compatible" uses for a permitted "business purpose." We believe this would be an anomalous result that would not provide any consumer benefit.

Therefore, if the Attorney General declines to clarify the application of Cal. Civ. Code 1798.140(t)(2)(A) to Shipping Information processed by the package transportation industry, then we believe the final regulations promulgated by the Attorney General under the CCPA should make clear that the use of Shipping Information by carriers to provide services to other customers – and indeed to others residing at the same address – and for other internal transportation operations-related purposes is permissible. W290-2 (cont.)

4. **The Clarifications Requested above are also Consistent with the law under the European Union General Data Protection Regulation, which Provides that Package Transportation Providers Are Controllers, not Processors, as to Shipping Information.**

The European Union General Data Protection Regulation (the GDPR) is arguably the most comprehensive and protective privacy law in the world. Even in the EU, under the GDPR, package transportation providers are deemed controllers that have the right to determine the purposes and means of the processing of Shipping Information.

- As the Attorney General's Office will be aware, the definition of "controller" in the EU is analogous to the definition of "business" in the CCPA, in that both a controller and a business "determine[] the purposes and means" of the processing of personal information. Cal. Civ. Code § 1798.140(c)(1); GDPR Art. 4(7). The GDPR also contains the concept of a "data processor", which, similar to a service provider under the CCPA, is defined as an entity that processes data on behalf of a controller. The controller/processor concepts have existed at the EU level since 1995, when the EU's Data Protection Directive was passed, and they continue in effect under the GDPR.

- European regulators who have addressed the issue have consistently found that package transportation companies are best classified as "controllers," not as "processors." As an example, the United Kingdom's Information Commissioner's Office issued guidance in 2014 stating that a delivery service "will be a data controller in its own right in respect of any data it holds to arrange delivery or tracking … such as individual senders' and recipients' names and addresses."[2] More recently, the Bavarian Office for Data Protection Supervision issued 2018 guidance stating that "postal services for letter or package transportation" are generally "not data processing," but instead "specialized services" offered by "an independent controller."[3]

W290-3 (cont.)

We respectfully suggest that the European practice reflects a recognition of the fundamental, inherent, and accepted purposes for which package transportation providers must use personal information to perform their daily operations at the level expected by both consumers and customers. We request the Attorney General to take a similar approach under the CCPA by clarifying the application of Section 1798.140(t)(2)(A) to Shipping Information that transportation providers receive W290-1 (cont.) W290-3 (cont.)

---

[2] *See* Information Commissioner's Officer, *Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Are* at 12 (June 5, 2014), available at https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf.

[3] *See* Bayerisches Landesamt für Datenschutzaufsicht [Bavarian Office for Data Protection Supervision], *FAQ zur DS-GVO: Auftragsverarbeitung, Abgrenzung* [GDPR FAQs: Data Processing, Distinguishing [between Controllers and Processors]] at 2 (July 20, 2018), available (in German) at https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf.

from businesses, pursuant to the Attorney General's rulemaking authority under Cal. Civ. Code § 1798.185(b)(2).

W290-1 (cont.) W290-3 (cont.)

* * * * * *

The California Trucking Association appreciates the efforts of the California Attorney General to ensure balance in the application of the CCPA to the business community in the State of California. We are available to answer any questions or to provide any additional information regarding our concerns.

With kind regards,

Shawn Yadon
CEO
California Trucking Association

From: Tanzer, Theodore
To: Privacy Regulations
Cc: Feldman, Peter
Subject: Comm. Feldman - CCPA Comments [OLA File No. 2019-1001-05]
Date: Monday, February 24, 2020 12:35:07 PM
Attachments: Feldman Comments on CA Privacy Regulations -- FINAL.PDF

Ms. Kim,

Please find attached Commissioner Feldman's comments on the updated notice of modifications to text of proposed regulations and addition of documents and information to rulemaking file [OLA File No. 2019-1001-05]. Please let me know if you have any questions.

Sincerely,

-Teddy

Theodore R. Tanzer
Attorney Advisor
Office of Commissioner Peter Feldman
U.S. Consumer Product Safety Commission
Office: [redacted]

UNITED STATES
CONSUMER PRODUCT SAFETY COMMISSION
4330 EAST WEST HIGHWAY
BETHESDA, MD 20814

COMMISSIONER PETER A. FELDMAN

February 24, 2020

Transmitted via e-mail to Lisa B. Kim, Privacy Regulations Coordinator,
PrivacyRegulations@doj.ca.gov

The Honorable Xavier Becerra
Attorney General of California
300 South Spring Street, First Floor
Sacramento, CA 90013

Re: Comments of the Hon. Peter A. Feldman, U.S. CPSC Commissioner, on the Updated Notice of Modifications to Text of Proposed Regulations and Addition of Documents and Information to Rulemaking File
[OAL File No. 2019-1001-05]

Dear Attorney General Becerra:

I am providing comments on the newly proposed regulations issued by the California Attorney General on October 11, 2019, to implement the California Consumer Privacy Act (CCPA).[1] I thank you for the opportunity to submit these comments, and for your response to my March 2019 letter urging you to consider the impact of the statute's "Right to Delete" provision on the ability of retailers, manufacturers, and others to conduct efficient recalls of hazardous consumer products. I appreciate your willingness to engage on this issue and your commitment to solicit feedback from diverse stakeholders. I hope these comments and background materials will assist you in your efforts to promulgate effective regulations that do not frustrate the important safety mission of federal agencies like the U.S. Consumer Product Safety Commission (CPSC). W291-1

The CPSC is an independent federal regulatory agency charged with protecting the public from unreasonable risks of injury or death associated with the use of thousands of types of consumer products under the agency's jurisdiction. Established by Congress in the Consumer Product Safety Act, the CPSC has jurisdiction over approximately 15,000 different types of products used in and around the home, in schools, in recreation, and otherwise.[2] Deaths, injuries, and property damage from consumer product incidents cost the nation more than $1 trillion annually. CPSC is committed to protecting consumers and families from products that pose fire, electrical, chemical or mechanical hazards. CPSC's work to help ensure the safety of consumer products -- such as toys, cribs, power tools, cigarette lighters and household chemicals -- contributed to a decline in the rate of deaths and injuries associated with consumer products over the past 40 years. CPSC

[1] California Consumer Privacy Act of 2018, ch. 55, 2018 Cal. Stat. 91 (codified at Cal. Civ. Code tit. 1.81.5); Cal. Civ. Code § 1798.105(a) (effective Jan. 1, 2020).
[2] Consumer Product Safety Act, 15 U.S.C. §§ 2051 – 2089 (2020).

W291-1
(cont.)

often works with companies to identify potentially hazardous consumer products and assists in developing and implementing corrective action plans to address the hazard.

Because CPSC is not a privacy regulator, I take no position with respect to the merits of the broader consumer privacy considerations underpinning the CCPA. However, given CPSC's extensive work on consumer product recalls, I would like to call your attention to the ways in which CPSC and recalling firms rely on industry-collected personally identifiable information (PII) of consumers purchasing consumer products to advance safety.

CPSC is constantly striving to improve both the timeliness of recalls and the effectiveness of the recall programs negotiated with companies. In doing so, CPSC compliance staff often works with manufacturers, distributors, and retailers to develop mutually acceptable programs that include a variety of notification methods to alert affected consumers about product recalls. Research shows, and the CPSC has long recognized, a powerful positive relationship between direct notification of consumers and recall success.[3] Direct notification is not possible without affected consumers' PII. Often, CPSC will encourage a recalling firm to use the information it collects through registration cards, records, catalog orders, retailers loyalty cards, or other means, to effect direct notification. [4] In other situations, companies may purchase commercially-available mailing lists of consumers who are likely to use a particular product.[5] Industry-collected consumer PII, and the direct notification it enables, is therefore an important tool to locate and remove hazardous product as quickly as possible.

Because CCPA's "Right to Delete" provision, and updated implementation and streamlining regulations, could result in the deletion of this critical consumer PII, it is my hope that you will consider language to preserve its availability to allow for the efficient transmission of recall notifications. The CCPA states that "[a] consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer."[6] While the CCPA contains a number of exemptions under which failure to fulfill a consumer's request to delete PII would be permissible, no exemption for consumer safety or

[3] *See e.g.* Dennis R. Murphy & Paul H. Rubin, *Determinants of Recall Success Rates*, 11 J. OF PROD. LIAB. 17, 17-28 (1988); *and see* U.S. CONSUMER PROD. SAFETY COMM'N, RECALL EFFECTIVENESS WORKSHOP REPORT 5 (2018), *available at* https://www.cpsc.gov/s3fs-public/Recall_Effectiveness_Workshop_Report-.pdf?R1VyLltrl8M_id.2vkAklHoUZjaSCab *(*last visited Mar. 25, 2019) (CPSC staff finding that "[d]irect notice recalls have proven to be the most effective recalls").

[4] *See* U.S. CONSUMER PROD. SAFETY COMM'N, RECALL HANDBOOK 19 (2012), available at https://www.cpsc.gov/s3fs-public/8002.pdf (last visited Feb. 13, 2020). NOTE: The CPSC regulations create no affirmative legal obligation for private sector firms to collect such information. *See* 16 C.F.R. pt. 1000 et seq. (2018).

[5] Because such lists are generally available from businesses that sell personal information about consumers to third parties, the CCPA "Right to Opt-Out" provision raises additional concerns with respect to the commercial availability, accuracy, and completeness of consumer PII for these purposes. *See* Cal. Civ. Code § 1798.120 (effective Jan. 1, 2020).

[6] Cal. Civ. Code § 1798.105(a) (effective Jan. 1, 2020).

W291-1
(cont.)

recall efficiency currently exists.[7] Regulatory language to this effect would be appropriate to further consumer safety.

I appreciate the opportunity to submit these comments and I look forward to working with you on developing final regulations to implement the CCPA. I stand ready to assist further in any way I can.

Sincerely,

Peter A. Feldman
Commissioner

Attachments:

Dennis R. Murphy & Paul H. Rubin, *Determinants of Recall Success Rates*, 11 J. OF PROD. LIAB., 17-28 (1988).

U.S. CONSUMER PROD. SAFETY COMM'N, RECALL EFFECTIVENESS WORKSHOP REPORT (2018).

U.S. CONSUMER PROD. SAFETY COMM'N, RECALL HANDBOOK (2012).

[7] Cal. Civ. Code § 1798.105(d)(2)-(9) (enacted by ch. 55) (exempting business from complying with a request when there are fraudulent activities, problems with their systems, questions of free speech, compliance issues with the California Electronic Communications Privacy Act, ongoing studies, or other legal obligations).

Journal of Products Liability, Vol. 11, pp. 17–28 (1988). Pergamon Press. Printed in U.S.A.

W291-1
(cont.)

Determinants of Recall Success Rates

R. Dennis Murphy
Paul H. Rubin

1. Introduction

The Consumer Product Safety Commission (CPSC) oversees more than 100 product recalls annually. These "Corrective Actions" involve millions of individual items and the widest range of consumer products subject to the recall authority of any Federal agency. Despite the importance of these actions and the availability of a rich source of data in the CPSC investigative files, no systematic analysis has been undertaken to explore which factors have been the most important determinants of recall success rates.[1]

This paper develops and tests an econometric model of the determinants of CPSC recall effectiveness using data the authors collected from the investigative files of approximately 130 recalls initiated by the CPSC from 1978 to 1983. The study provides two basic types of information. First, the results can be used to predict the expected success rate for a recall. Second, the analysis identifies which notice techniques, product characteristics, and cost and benefit factors have been most closely associated with variations in recall success rates as measured by the percentage of targeted items that are repaired or returned for exchange or refund. This information will be useful both for the CPSC and for firms engaged in recalls.

For the CPSC, the results can be used as a planning tool to predict in advance any proposed recall's likely success rate; they can also be used at the conclusion of a Corrective Action Plan (CAP) to determine if further effort is justified. This will enable the agency to close its files in a timely manner and therefore more efficiently utilize its resources. Moreover, by identifying those factors associated with greater success, the Compliance staff will be able to help draft more efficient CAPs.

For respondents in CPSC actions, predictive data on recall success can

R. Dennis Murphy is an economist with the Federal Trade Commission. His views do not reflect the position of the F.T.C. or other members of its staff.

Paul H. Rubin is with Glassman-Oliver Economic Consultants in Washington, D.C. and is former Chief Economist of the Consumer Product Safety Commission.

1. The Commission's Office of Strategic Planning attempted such a study in 1978. However, the statistical analysis was limited to simple cross-tabulations of correction rates and a single explanatory variable that failed to control for other determinants of recall effectiveness. In addition, no significance tests were conducted. *See* Loren Lang, RECALL EFFECTIVENESS STUDY, Office of Strategic Planning, U.S. Consumer Product Safety Commission, May, 1978.

0363-0919/88 $3.00 + .00

Table I. Number of Sampled Recalls by Year

Year	Number
1978	17
1979	41
1980	35
1981	17
1982	9
1983	13

help budget for the likely direct costs of a recall. Firms will also have a basis for claiming that a recall has been successful and should be terminated. Finally, and perhaps most importantly, in product liability litigation there will be data to use both in designing recall plans and in determining if a sufficient effort has been made in a recall. Further, even though this model has been estimated using CPSC data, with some modifications it should also be applicable to recalls by other agencies (e.g. FDA and NHTSA).

II. Sample Composition

The sample of 128 recalls selected for the study includes all completed corrective actions initiated from 1978-1983 for which data on key variables could be obtained from CPSC investigative files.[2] The time period chosen for analysis was dictated by practical time and data constraints. Final correction rates and other summary statistics were not available for major recalls initiated after 1983, since these investigations generally have not yet been officially closed. Further, those recent recalls that have been completed tend to be quite routine and involve product defects with low hazard ratings. The start date of 1978 was imposed by data gathering time constraints.

Table I lists by year the number of recalls in the sample that were initiated during the period 1978-83.[3] Despite the potential for a bias toward low-hazard recalls, the average hazard rating of the sampled recalls is very close to that of all recalls initiated from 1983-1985.[4] CPSC recall hazard ratings

2. This same data was used in estimating the stock market costs of CPSC recalls; *see* Paul H. Rubin, R. Dennis Murphy, and Gregg Jarrell, *Unsafe Products, Risky Stocks*, REGULATION, 1988 (forthcoming).

3. The small number of cases from 1978 reflects an exceptionally high incidence of missing data (even though virtually all of the investigations had been closed.)

4. Average hazard ratings for recent recalls were computed from data contained in memoranda that the Corrective Action Division has transmitted to the Commission annually since 1983.

W291-1
(cont.)

range from a low of C to a high of A. Translating these letter grades into numerical ratings of 1-3, the average rating of all 1983-85 recalls was 1.64 (C+). The average for the 128 recalls in the sample was only slightly lower at 1.55.[5]

III. Choice of Explanatory Variables

A defective product cannot be recalled or otherwise corrected successfully unless three conditions hold. First, the product must be available in the distribution chain or, if sold to consumers, still be in their possession. Second, distributors and consumers must be aware of the recall. Third, the perceived benefits to the consumer of complying with the terms of the recall must exceed the perceived cost in time, effort, and lost product services. The explanatory variables chosen for the study attempt to measure the extent to which these considerations hold for any given recall.

Number of Items in Use

One of the most important determinants of the proportion of defective items still available for recall should be the average age of the product in question. Holding all else constant, consumers are more likely to have discarded a product the greater the time that has elapsed between the start of distribution and the start of the recall. Further, for any given time period between product introduction and recall, average product age will be higher if sales stopped before the recall began, since there will be no infusion of new products to offset the depreciating stock of products already sold.

Thus, two product age variables were selected for the recall effectiveness model. The first measures the number of months a product was in distribution before the start of the recall. The second measures in months any lag between the end of distribution and the recall start date. We would expect an inverse relationship between recall success and each of these variables, with the "lag" variable being most important.

The percentage of items available for recall clearly also depends on the average useful life of the product. The CPSC staff was able to provide estimates of average product life for virtually all of the recalled products in the sample using prior analyses that had been prepared by the Directorate of Economics for Commission policy planning and monitoring purposes.

5. Prior to 1981, substantial product hazards were classified as either of moderate, high, or very high severity. Beginning in 1981, the procedure for assigning hazard ratings was made more systematic and letter grades replaced the previous descriptive terms. Although the two systems are not strictly comparable, classifying moderate, high, and very high severity ratings as C, B, and A hazards should introduce no systematic bias.

W291-1
(cont.)

Notice Level

The second class of explanatory variables measures the level of notice and general publicity associated with each sampled recall. In the simplest case of a product that has not yet been sold to consumers, manufacturers of a recalled product need only contact retailers and any intermediate distributors. Once the product reaches consumers, however, notice options become more complex. If the names and addresses of all owners are known, consumers presumably can be contacted directly without the need for additional notice or publicity. When such information is unavailable, alternatives are to have the manufacturer issue a company press release, conduct a joint press conference with the Commission, place media advertisements, and/or post point-of-purchase notices.

Cost and Benefit Variables

The final class of explanatory variables attempts to measure the costs and benefits to affected parties of complying with a recall. At the outset, it should be noted that the ratio of benefits to costs for any recall should generally be higher for distributors and retailers than for consumers. Because of their continuing commercial relationship with producers and concern for their reputations and fear of liability suits, retailers should have a strong incentive to respond to product recalls. At the same time, the cost of notifying distributors and retailers and the cost to these parties of complying with recalls should be relatively low, since correspondence and product returns are a routine fact of business life.

Thus, simply accounting for the percentage of defective products sold to consumers should explain a substantial portion of the variance in recall success rates. It should also be fruitful to distinguish between inventory held by retailers and distributors and that held by the factory or importer, since shipping and notification costs for the latter will be virtually nonexistent. This was accomplished by specifying for each sampled recall the percentage of products sold to consumers and the percentage held by retailers and distributors. The proportion of recalled products in factory inventory is by definition one minus the proportion held by retailers and consumers.

We would predict that recall effectiveness would be highest when all inventory is still at the factory. Correction rates for retailers should be at least slightly lower than for producers. Correction rates for products held by consumers would be lowest.

Whatever the distribution pattern, the benefits of cooperating with a recall should vary directly with the severity of the safety hazard (assuming that retailers and consumers correctly judge the degree of hazard). This hypothesis was tested by measuring degree of product hazard on the A,B,C scale discussed above.

W291-1
(cont.)

The benefit of complying with a recall should also be higher for more expensive products, since the items are presumably of greater value to consumers. For inexpensive products it is more likely that consumers will simply discard the item rather than taking the trouble to return it to the retailer or manufacturer. Although discarding the product will eliminate the hazard and is thus consistent with the goal of the recall, such actions will not be captured by the reported correction rate (absent a follow-up consumer survey).

Finally, the benefit that consumers expect from cooperating with a recall may depend on the type of remedy provided. Consumers may view a complete refund or exchange as superior to a repair. This was tested by a variable that measures refund and exchange compared with repair.

Virtually no recalls impose any significant out-of-pocket costs on consumers other than transportation expenses incurred to return a product to retailers or deliver it to the post office or United Parcel for shipment to the factory. Manufacturers reimburse consumers for shipping charges if products have to be returned to the factory, and, of course, consumers are not charged for the actual repair. Thus, the real cost to consumers is the time and trouble needed to comply with the recall and the value of product services lost while the defect is corrected or a new replacement product is received.

Measured in these terms, the most costly recalls would appear to be those that require consumers to return items to the factory. Consumers generally will have to both package the product and transport it to the shipping or mailing point. It is also reasonable to assume that the entire process of packaging, mailing, repair (or exchange), and return will take longer than an equivalent remedy provided at the point of purchase. The next most costly remedy would seem to be a dealer-performed repair or exchange. This conclusion is not absolutely certain, however, since consumers will face an added trip back to the dealer or retailer to pick up repaired items, while products performed at the factory will be shipped directly to owners.

Third in order of hypothesized cost to consumers is a repair-kit remedy. In such instances consumers are able to call a toll-free line and arrange to have do-it-yourself repair kits sent to their homes. These fixes generally require little effort or skill. If consumers are reluctant to undertake the project themselves, they will in any event usually have the option of returning the defective item to the point of purchase for repair.

The least burdensome remedy for consumers is almost certainly an in-home repair. These usually involve major appliances or furnaces where retailers know the addresses and phone numbers of most customers. Thus, consumers usually do not have to take the initiative to arrange for a correction of the defect.

These various hypotheses were tested using three separate variables representing (1) recalls requiring that products be returned to the factory, (2) recalls where products are to be returned to the point of purchase for repair,

W291-1
(cont.)

exchange, or refund, and (3) recalls employing repair kits as a remedy. In the sample data set, these three classes of recalls never occur in conjunction with the fourth category of recalls, repairs in the home. This means that the three recall-cost variables will measure any reduction in recall effectiveness *relative* to in-home corrective actions. If our hypotheses are correct, the factory repair will appear least successful in relation to in-home repair, followed in order by point of purchase and repair kit remedies.

We also tested a theory frequently mentioned in staff file memoranda regarding the relative ease of publicizing recalls of sports enthusiast's products such as scuba diving and mountain climbing equipment. The argument is that participants in these sports are readers of specialized magazines and newsletters and make frequent visits to retailers catering to their needs. Thus, on-site placards and print advertisements announcing a recall of such products are more likely to reach their target audience. It is also probably true that scuba divers and mountain climbers would be particularly anxious to have any safety defect in their support equipment corrected. Thus, a variable representing scuba diving and mountain climbing equipment recalls can be viewed as capturing both cost and consumer benefit considerations and in either event should be positively related to correction rates.

As a final cost variable, the total number of units recalled was included to account for the higher overall cost of conducting large recalls. Such corrective actions could be particularly burdensome if total costs increase more than proportionately with the scale of the recall.

IV. Review of Regression Model

Our analysis of the determinants of recall effectiveness has suggested a total of 18 independent variables (plus an intercept term used routinely in regression analysis) that may help explain variations in correction rates. These are assigned descriptive names and expected coefficient signs in Equation 1 below:

Ignoring the intercept term momentarily, the first three variables attempt to account for the proportion of units sold that are still in use at the start of a recall. The next five variables measure the level of notice and publicity associated with each sampled recall. Beginning with price, the remaining variables represent either cost or benefit variables that should influence recall rates. The intercept term should capture the influence of the percentage of items held in factory inventory and the availability of an in-home repair, variables not explicitly present in the regression equation but whose values are uniquely determined by other included variables.

V. Regression Results

Since the purpose of regression analysis is to explain variations in the

W291-1
(cont.)

dependent variable, it will be useful at the outset to describe the degree of variation found among correction rates in the sample. The average correction rate for the 128 recalls is 54.4 per cent. Success rates span the entire possible range from zero to one hundred.[6] More formally, the standard deviation of the dependent variable is 34.5. This means that about two thirds of the sample correction rates are within 34.5 percentage points of the mean. Thus, one third of the recall success rates is either less than about 20 or more than 89. There is, in short, a great deal of variance in correction rates to be explained.

The complete regression results, which are presented as an appendix, reveal the extent to which our selected explanatory variables succeeded in this task. The general model demonstrates an impressively high level of explanatory power. The "R^2", which reveals the percentage of variation in correction rates that has been explained by the model, is 90. This is exceptionally high for cross-section data of this type. Many of the independent variable coefficients are highly significant and of the expected sign.

As predicted, the coefficient for product life is positive and significant. The direct-consumer-notification variable displays a powerful positive relationship to recall success. The percentage of recalled items in the hands of retailers and of consumers are also significant determinants of recall effectiveness. As noted earlier, the coefficients for these variables measure retailer and consumer recall compliance relative to producer compliance. The results show that retail performance is on average about 10 percent below the producer rate, while correction rates for items in the hands of consumers are on average about 87 percent below levels for producer-held inventory. (Obversely, the high positive value of the intercept term reflects in part the higher success rates that can be expected when no inventory has reached retailers or consumers.) Although it is not directly evident from the data in the appendix table, %consumer proved to be the most powerful explanatory variable in the model.

The conventional wisdom of CPSC compliance officers was confirmed by the performance of the Sports variable. Other factors equal, correction rates for scuba diving and mountain climbing equipment were 14 percentage points higher than for other consumer products. Finally, although the

6. Although correction rates vary widely, they can of course never exceed 100 or fall below zero. When a dependent variable is limited or "truncated" in this fashion, certain assumptions of the classical regression model are violated and it is possible that the estimated independent variable coefficients and their significance levels will be biased either upward or downward. A specialized regression procedure, known as Tobit analysis, overcomes the potential bias problem, but at some cost in ease of interpretation. As is customary in such circumstances, Tobit regressions were run as a check against all simple regression model results. Since no biases were evident, the ordinary least squares results are presented to ease exposition.

W291-1
(cont.)

months-distributed and months-lag variables are not significant by conventional standards, their coefficients conform to our expectations. Both display a negative relationship with correction rates, with the lag coefficient largest in absolute value.[7] Further, in models with fewer explanatory variables, Months Lag consistently revealed a significant coefficient.

The results do not lend support to most of our hypotheses concerning the impact of publicity and cost-benefit considerations on correction success rates. Aside from the Consnote and Sports variables discussed above, none of the notice dummies comes anywhere near significance. Also unconfirmed is the theory that recalls involving more hazardous product defects or recalls employing a refund or exchange remedy will achieve higher success rates because consumers expect greater benefit from compliance.

From the cost side, retail repair remedies appear to be less successful than other forms of repair or replacement. However, subsequent analysis with differently specified equations revealed that the coefficient on Retailrem was extremely unstable, often appearing insignificant and of varying signs depending on the exact variables included in the model. The most successful approach to modeling the impact of cost of remedy was to replace the three repair remedy variables (Factrem, Retailrem, and Repkit) with a single variable representing in-home repair. Under this specification, the in-home repair coefficient indicates whether, other factors constant, correction rates are higher for those recalls that offer in-home repairs. As will be seen from predictive equation below, the results confirm this hypothesis.

VI. Predictive Equation

Our general model of recall effectiveness can be simplified considerably if our goal is to develop a working equation to predict in advance correction rate outcomes. Indeed, only seven variables (including the intercept term) are needed to match the predictive power of the general model.[8] Table II presents the results of this regression equation.

Since the purpose of the Table II regression equation is to predict recall outcomes in advance, the regression standard error is of primary concern. Approximately two times out of three the equation will predict the actual

7. The relatively poor showing of months in distribution is due in large part to its strong association with another explanatory variable in the model—percentage of items in consumer hands. All else equal, a greater proportion of items will be held by consumers the longer the product has been in production. When two explanatory variables are highly correlated with one another, it is not unusual for one of the variables to display an insignificant coefficient even though it is individually related to the dependent variable.

8. The product life variable, which proved significant in the general model, lost much of its explanatory power in simpler models. It was therefore dropped to spare users of the predictive equation the burden of estimating a recalled product's average useful life.

W291-1
(cont.)

Table II. Predictive Equation

Variable	Coefficient	Significance Level*	Mean
ONE	96.724	.000	1.00
Months Lag	−.109	.003	7.25
Consnote	.598	.000	34.44
%retail	−.116	.069	28.60
%consumer	−.896	.000	56.57
Homerep	14.216	.061	.16
Sports	16.537	.020	.05

$R^2 = .90$
Standard Error of Regression = 10.97
*Lower numbers indicate more significant coefficient values.

Equation I

Correct = one − months distrib − months lag + prodlife + consnote + ad + uni-press + jnt-press + placard + price − %retail − %consumer + hazard + refund − factrem − retailrem − repkit + sports − quantity

Where:

Correct	=	final reported correction rate in percentage points
one	=	intercept
months distrib	=	number of months product was distributed before recall
months lag	=	number of months separating end of distribution and start of recall
prodlife	=	estimated average useful life of recalled product (in years)
consnote	=	percentage of products owned by consumers who are notified of recall directly by mail.
ad	=	zero-one dummy, equals one for recalls with print advertisements
uni-press	=	zero-one dummy, equals one for recalls with unilateral company press release
jnt-press	=	zero-one dummy, equals one for recalls with joint CPSC-company press release
placard	=	zero-one dummy, equals one for recalls with point-of-purchase placards
price	=	retail price of recalled product
%retail	=	percentage of items in retail inventory
%consumer	=	percentage of items in hands of consumers

W291-1
(cont.)

Equation I (Continued)

hazard	= zero-one-two dummy, for C, B, and A rated recalls respectively
refund	= zero-one dummy, equals one for recalls with refund or exchange remedy
factrem	= zero-one dummy, equals one for recalls with remedies performed exclusively at factory
retailrem	= zero-one dummy, equals one for recalls with remedies performed at point of sale
repkit	= zero-one dummy, equals one for recalls with repair kit remedies
sports	= zero-one dummy, equals one for recalls of scuba diving or mountain climbing equipment
quantity	= number of units recalled

Table III. Predicted and Actual Correction Rates for Ten Randomly Selected Recalls

ID Number	Reported Correction Rate	Predicted Correction Rate	Error
8353	90.0	98.5	+ 8.5
8153	97.0	81.8	−15.2
8131	34.0	47.1	+13.1
80116	35.0	24.2	−10.8
8062	50.0	48.4	− 1.6
8053	78.0	76.2	− 1.8
79179	35.6	37.4	+ 1.8
7968	16.6	20.1	+ 4.5
7909	92.6	91.9	+ 0.7
78120	97.3	93.1	− 4.2

value plus or minus one standard error. Thus, the results show that 67 percent of our predictions should be within about 11 percentage points of the true outcome, and 95 percent of the predictions should be accurate within plus or minus 22 percentage points.

To place these figures in perspective, remember that the standard error of the dependent variable is about 34.5 percentage points. This means that if we were to make purely random guesses as to recall correction rates, we

W291-1
(cont.)

would come within 34.5 percentage points of the actual figure two-thirds of the time. Relying on our predictive equation should reduce this margin of error by about 23.5 percentage points.

Table III illustrates the equation's reliability more concretely by presenting the predicted and actual correction rate for every twelfth recall in the sample.

VIII. Conclusions

Our analysis of recent CPSC corrective actions demonstrates that it is possible to construct a simple model of the determinants of recall effectiveness that can account for a high percentage of the observed variation in recall rates. The predictive equation derived from this model can forecast CPSC recall success rates with considerable precision. It should certainly prove accurate enough to provide an unbiased ball-park estimate of final correction rates. Thus, our predictive equation should be of value both to CPSC officials and to private firms in planning and monitoring product recalls.

It is interesting to note that, for a product which is entirely in the hands of consumers, with no lag between distribution and the recall, no notice, no home repair, and which is not a "sports" product, the success rate is only 7%, so that low rates of return for products should not be surprising.

Appendix

Regression Results: Complete Model

Variable	Coefficient	Significance Level*	Mean
ONE	94.528	.000	1.0(
Months Distrib	−.585	.270	17.88
Months Lag	−.776	.124	7.2
Prodlife	.791	.018	7.0
Price	−.004	.814	436.0
Consnote	.599	.000	15.9(
Ad	−3.010	.382	.1(
Uni-press	2.712	.377	.1(
Jnt-press	1.318	.680	.4
Placard	2.029	.491	.2
% retail	−.100	.102	28.6
% consumer	−.873	.000	56.5
Hazard	.001	.783	1.5
Refund	−1.186	.706	.4

W291-1
(cont.)

Appendix

Regression Results: Complete Model (Continued)

Variable	Coefficient	Significance Level*	Mean
Factrem	−3.361	.430	.08
Retailrem	−4.338	.095	.39
Repkit	−2.366	.578	.11
Sports	14.337	.015	.05

R^2 = .90

Standard Error of Regression = 11.8 (percentage points)

*Lower numbers indicate more significant coefficient values.

Recall Effectiveness Workshop Report

CPSC in Cooperation with Stakeholders

February 22, 2018

Office of Compliance and Field Operations
Joseph F. Williams, CFEI
Compliance Officer

W291-1
(cont.)

Introduction

The CPSC is charged with protecting consumers from unreasonable risks of injury or death associated with the use of thousands of types of consumer products. One way to protect consumers is to conduct a product recall. CPSC's recalls are generally executed cooperatively with affected companies. Although there are mandatory recalls, the vast majority of CPSC's recalls are voluntary. During the voluntary recall process, the CPSC works with companies that agree to provide notice to consumers and a remedy for potentially hazardous products. This cooperative process facilitates the ability of the CPSC and the recalling company to reach affected consumers.

In furtherance of that cooperation, on July 25, 2017, the CPSC hosted a Recall Effectiveness Workshop. The goal of the workshop was to explore and develop proactive measures that CPSC and stakeholders can take to improve recall effectiveness. Seventy-nine external stakeholders attended the workshop, including various retailers, manufacturers, law firms, consumer interest groups, third party recall contractors and consultants, testing laboratories, and other interested parties. The CPSC facilitated an open discussion among these participants about ways to increase recall effectiveness and also gathered feedback on how CPSC can potentially improve its recall efforts.

Workshop Summary

During the workshop registration and welcome process, participants had an opportunity to post their expectations for the day. Stakeholders said they wanted to learn more about CPSC's procedures and learn about innovative ways to increase recall effectiveness. Stakeholders also said they wanted to discuss the role of technology and social media in recalls, and to address how to achieve consistency between recalls and recalling firms. Several stakeholders expressed interest in the action items that would result from the workshop.

CPSC opened the program with three presentations related to the recall process: (1) "Review of Recall Process and Standard Notifications," (2) "Intro to OCM [Office of Communications Management] and Goals for CPSC Press Releases," and (3) "Recall Data." The first presentation offered an overview of CPSC's standard processes and recall notifications; the second introduced OCM's role in the recall process, and offered information on the goals and guidelines for CPSC press releases. The third presentation supplied statistical analysis of recall results from FY 2014 through FY 2016 for 865 closed Section 15 cases. This analysis demonstrated an overall correction rate of 65 percent, including corrections from manufacturers, distributors, retailers and consumers from CPSC recalls. The presentation provided correction rates based on distribution level, retail price, product category, type of remedy, and recall type. These presentations can be found online at:

- CPSC Defect Recall Data - https://www.slideshare.net/USCPSC/cpsc-recall-effectiveness-workshop-recall-data;
- Review of Recall Process and Standard Notifications - https://www.slideshare.net/USCPSC/cpsc-recall-effectiveness-workshop-recall-process; and
- Goals for CPSC Recall Press Releases - https://www.slideshare.net/USCPSC/cpsc-recall-effectiveness-workshop-goals-for-cpsc-recall-press-releases.

After these background presentations, CPSC encouraged open-forum discussions on the recall process. The first open forum was titled, "What is an effective recall?" Some stakeholders said they were interested in considering multiple factors to measure the effectiveness of a recall. In addition to consumer return rates, some of these stakeholders recommended considering incident rates.

The second open forum was titled, "Communicating the Hazard." Over the past 20 years, the means of communicating recalls has changed substantially and continues to change rapidly as technology evolves. Widespread use of the Internet, email, social media, and other forms of instant communication have changed the ways companies can reach consumers. This session focused on communication channels, the use of marketing strategies, language in recall notices, recall best practices, and limitations and barriers to effective communication. It appeared from the discussions that very few firms develop a marketing strategy for recalls.

The third and fourth forums (held simultaneously as breakout sessions) focused on "Consumer Motivation" and "Technological Advances to Improve Recall Effectiveness." The "Consumer Motivation" forum discussed consumer behavior, challenges to motivating consumers to participate in recalls, incentives, and designing notices to encourage participation. The forum on "Technological Advances to Improve Recall Effectiveness" discussed technological improvements to consumer notification and the effectiveness of recalls, improving direct notification and challenges acquiring and implementing new technology to support more effective recalls.

Reaction to the Workshop

The workshop received positive feedback from stakeholders. Follow-up survey results showed that:

- Respondents felt that the information was useful and that they can share the workshop information with others;
- Ninety-six percent of respondents believed the workshop format helped engage stakeholders in discussion;
- Eighty-eight percent of respondents felt their opinion was heard;

W291-1
(cont.)

- Ninety-six percent of respondents would like additional workshops on this topic; and
- Suggestions from respondents included: offering workshops in this format on other topics; continuing discussion on recall effectiveness during ICPHSO; encouraging additional manufacturers to attend future workshops; and webcasting future workshops.

Stakeholder Suggestions

The workshop resulted in valuable feedback and ideas for improving recall effectiveness. The consolidated notes from the workshop can be found here (Workshop Notes). Key ideas and suggestions from stakeholders included:

- **Explore ways to increase direct notice to consumers**

  The "Recall Data" presentation demonstrated that direct notice has a substantial impact on consumer return rates. Stakeholders noted that improved product registration methods (*e.g.*, retailer opt-in at checkout, home voice assistants, photo texting, QR codes, and incentives) could lead to higher consumer participation.

- **Expand the use of marketing strategies and technology**

  Marketing and technology can play a pivotal role in getting a recall message to consumers. Stakeholders discussed how using marketing and technology (*e.g.*, social media, the use of apps, and targeted messaging) might heighten effectiveness, and several suggested that CPSC share effective practices to a wider audience.

- **Consider consumer and business incentives to promote effective recalls**

  Stakeholders discussed exploring incentives for consumers to participate in recalls, and examine whether it would be helpful to incentivize recalling firms to be creative in their recall efforts.

- **Consider greater differentiation of recalls**

  Stakeholders suggested evaluating whether differentiating between recalls with more and less significant hazards would improve overall effectiveness. Several stakeholders suggested reviewing systems other agencies use to develop and release recalls for possible guidance on whether and how to differentiate actions.

W291-1
(cont.)

- **Consider disseminating additional information on best practices**

  Stakeholders saw value in dissemination of best practices in addition to existing recall information, including information related to the use of marketing, social media, and product registration.

Key Findings for Further Consideration with Stakeholders

We considered these suggestions for follow-up with stakeholders and intend to prioritize the following:

1. **Collaborating on ways to improve direct notice to consumers**

   Direct notice recalls have proven to be the most effective recalls. We intend to work with consumer and industry stakeholders on registration methods or other improvements (*e.g.*, retailer opt-in at checkout, home voice assistants, photo texting, QR codes, and incentives for product registration) to promote direct notice recalls.

2. **Collaborating with firms engaged in recalls to use marketing strategies to promote consumer response**

   We will continue to explore how technology can be used to enhance recall response in appropriate cases, including enhancing firms' recall marketing strategies, use of social media, and improved methods for in-store communication. We intend to identify and share examples of future recall marketing strategies that are innovative and/or successful.

RECALL HANDBOOK

A Guide for Manufacturers, Importers, Distributors and Retailers on Reporting Under Sections 15 and 37 of the Consumer Product Safety Act and Section 102 of the Child Safety Protection Act and Preparing for, Initiating, and Implementing Product Safety Recalls Including CPSC Fast Track Product Recall Program and use of Social Media

U.S. Consumer Product Safety Commission
Office of Compliance & Field Operations
4330 East West Highway, Room 613
Bethesda, Maryland 20814
Telephone: (301) 504-7520
Fax: (301) 504-0359

E-mail address: Section15@cpsc.gov

www.cpsc.gov

www.saferproducts.gov

March 2012

W291-1
(cont.)

Foreword

The U.S. Consumer Product Safety Commission (CPSC) Office of Compliance and Field Operations staff prepared this Recall Handbook to help your company understand your obligations and responsibilities under the Consumer Product Safety Act. It applies to you if you manufacture, import, distribute, or retail consumer products. The latest revision of this Handbook incorporates changes to the statute as a result of the Consumer Product Safety Improvement Act.

No company likes to recall one of its products, but when a safety problem makes a product recall necessary to prevent injuries and save lives, it benefits everyone to move quickly and effectively.

Our staff is constantly striving to improve both the timeliness of recalls and the effectiveness of the recall programs negotiated with companies. Our Fast Track Product Recall Program and use of Social Media to reach consumers in the event of a recall is helping both of these efforts. The Fast Track Product Recall Program is designed for companies willing and able to move quickly with a voluntary recall of their product. The program, described in detail in Section IV, eliminates some of the procedural steps in the traditional recall process, including a staff preliminary determination that the product contains a defect that presents a substantial product hazard.

Many companies have used the Fast Track Product Recall program since CPSC introduced it in August 1995 and have found it to be a useful way to expedite product safety recalls.

We welcome your comments on the Fast Track Product Recall Program or any other information in this handbook.

Office of Compliance and Field Operations

301-504-7520

Section15@cpsc.gov

RECALL HANDBOOK

W291-1
(cont.)

Background

I. Reporting Requirements

A. Section 15 Reports

1. What and Where to Report
2. When to Report
3. Confidentiality of Reports

B. Section 37 Reports

1. What to Report
2. When and Where to Report
3. Confidentiality of Reports

C. Section 102

1. What to Report
2. When and Where to Report
3. Confidentiality of Reports

II. Identifying a Defect

III. CPSC Evaluation of Section 15 Reports

- Class A Hazards
- Class B Hazards
- Class C Hazards

IV. Fast Track Product Recall Program

V. Putting Together a Corrective Action Plan

A. Preparing for a Product Recall
B. Elements of a Recall

VI. Communicating Recall Information

A. News Releases
B. Video News Releases
C. Posters
D. Social media

W291-1
(cont.)

E. Other Forms of Notice
F. Toll-Free Numbers

VII. Monitoring Product Recalls

VIII. Developing a Company Policy and Plan to Identify Defective Products and to Undertake a Product Recall

A. Designating a Recall Coordinator
B. Role of the Recall Coordinator

IX. Records Maintenance

A. Records of complaints, warranty returns, insurance claims, lawsuits
B. Production Records
C. Distribution Records
D. Quality Control Records
E. Product Registration Cards

X. Conclusion

RECALL HANDBOOK[1]

Background

The U.S. Consumer Product Safety Commission (CPSC) is an independent regulatory agency responsible for protecting the public from unreasonable risks of injury and death associated with consumer products. Established by Congress in the Consumer Product Safety Act (CPSA), 15 U.S.C. §§ 2051-2089, the CPSC has jurisdiction over approximately 15,000 different types of products used in and around the home, in schools, in recreation, and otherwise ("consumer products").[2]

This handbook is for companies that manufacture, import, distribute, retail, or otherwise sell consumer products. It has three purposes: (1) to familiarize companies with their reporting requirements under sections 15(b) and 37 of the CPSA, 15 U.S.C. § 2064(b) and § 2084, and Section 102 of the Child Safety Protection Act, Pub. L. 103-267, 108 Stat. 722, 6/16/94; (2) to help companies learn how to recognize potentially hazardous consumer products at an early stage; and (3) to assist firms that discover they have manufactured, distributed or retailed such products to develop and implement "corrective action plans" that address the hazards. The term "corrective action plan" (CAP) generally includes any type of remedial action taken by a firm. A CAP could, for example, provide for the return of a product to the manufacturer or retailer for a cash refund or a replacement product; for the repair of a product; and/or for public notice of the hazard. A CAP may include multiple measures that are necessary to protect consumers. The Commission staff refers to corrective actions as "recalls" because the public and media more readily recognize and respond to that description.[3]

This handbook is not an all-inclusive reference source of information describing how to recall products. The goal of a corrective action plan should be to retrieve as many hazardous products from the distribution chain and from consumers as is possible in the most efficient, cost-effective manner. Reaching this goal often requires creative planning. Companies developing specific corrective action plans to address unsafe or potentially unsafe products typically work closely with the Commission staff to take advantage of the staff's expertise in designing and carrying out such plans. This results in greater protection for consumers against injury or death.

W291-1
(cont.)

[1]This handbook does not replace the Commission's statutes or interpretative regulations set out in 16 C.F.R. Parts 1115, 1116, and 1117. If there is any discrepancy, the statutes and regulations supersede this handbook. This material is available on the CPSC web site at: http://www.cpsc.gov .

[2]The Commission does not have jurisdiction over foods, drugs, cosmetics, medical devices, firearms and ammunition, boats, motor vehicles, aircraft, or tobacco. Specific questions about the Commission's jurisdiction over particular products should be directed to the Office of the General Counsel.

[3]This handbook uses the term "recall" to describe any repair, replacement, refund, or notice/warning program.

I. Reporting Requirements.

A. Section 15 Reports

Section 15(b) of the Consumer Product Safety Act establishes reporting requirements for manufacturers, importers, distributors and retailers of consumer products, or other product or substances distributed in commerce over which the Commission has jurisdiction. Each must notify the Commission immediately if it obtains information which reasonably supports the conclusion that a product distributed in commerce (1) fails to comply with an applicable consumer product safety rule or with a voluntary consumer product safety standard upon which the Commission has relied under section 9, (2) fails to comply with any other rule, regulation, standard or ban under the CPSA or any other Act enforced by the Commission, including the Flammable Fabrics Act, 15 U.S.C. §1193-1204; the Federal Hazardous Substances Act, 15 U.S.C. § 1261-1278; the Children's Gasoline Burn Prevention Act, 110 Public Law 278 (July 17, 2008), the Virginia Graeme Baker Pool and Spa Safety Act, 110 Public Law 140 (with amendments), the Poison Prevention Packaging Act, 15 U.S.C. § 1471-1476, and the Refrigerator Safety Act; 15 U.S.C. § 1211-1214; (3) contains a defect which could create a substantial product hazard, or (4) creates an unreasonable risk of serious injury or death. The Commission has issued an interpretive regulation, 16 C.F.R. Part 1115 that further explains a reporting company's obligations.

In enacting section 15(b), Congress intended to encourage the widespread reporting of timely, accurate and complete information that is necessary to protect public health and safety. In addition to assisting the Commission to discover substantial product hazards, reporting would identify risks of injury that the Commission could address through voluntary or mandatory standards, or information and education.

Although CPSC uses sources other than company reports to identify potentially hazardous products, reporting by companies under section 15 can provide the most timely and effective source of information about such products. This is

because firms often learn of potential product safety problems at an early stage. For this reason, companies involved in the manufacture, importation, distribution, or sale of consumer products should develop a system for maintaining and reviewing information about their products that might suggest that their product has a defect or poses an unreasonable risk of serious injury or death. Such information includes, but is not limited to, consumer complaints, warranty returns, insurance claims or payments, product liability lawsuits, reports of production problems, product testing, or other critical analyses of products.

W291-1 (cont.)

Reporting a product to the Commission under section 15 does not automatically mean that the Commission will conclude that the product creates a substantial product hazard or that corrective action is necessary. The CPSC staff will evaluate the report and works with the reporting firm to determine if corrective action is appropriate. Many of the reports received require no corrective action because the staff concludes that the reported product defect does not create a substantial product hazard.

[4]As of January 2012, there were two such standards—the voluntary standards for chain saws and for unvented gas space heaters, See, Appendix to Part 1115, Voluntary Standards on Which the Commission Relied Under Section 9 of the Consumer Product Safety Act .

1. What and Where to Report

A company should file its report with the Office of Compliance and Field Operations. The report should be filed electronically through the CPSC website (SaferProducts.gov). Alternatively, a firm can file its request by mail or telephone (301-504-7520). A company should assign the responsibility of reporting to someone with knowledge of the product and of the reporting requirements of section 15. That individual should have the authority to report to CPSC or to quickly raise the reporting issue to someone who does.

Reporting firms should be prepared to provide the information described below. However, no company should delay a report because some of this information is not yet available. The following information should be transmitted:

- identification and description of the product;
- name and address of the manufacturer and/or importer of the product if known. If not known, then the names and addresses of all known distributors and retailers of the product;
- nature and extent of the possible defect, the failure to comply, or the risk;
- nature and extent of injury or risk of injury associated with the product;
- name and address of the person informing the Commission;
- if reasonably available, the other information specified in Section 1115.13(d) of the Commission's regulations; and
- a timetable for providing information not immediately available;

W291-1
(cont.)

Retailers and distributors may satisfy their reporting obligations in the manner described above. Alternatively, a retailer or distributor may send a letter to the manufacturer or importer of a product describing the noncompliance with an applicable regulation, defect, or risk of injury or death associated with the product and forward a copy of that letter to the Office of Compliance and Field Operations. A distributor or retailer may also satisfy their reporting obligations by forwarding to the Office of Compliance and Field Operations reportable information received from another firm. Section 15(b) requires that a manufacturer, retailer, or distributor must immediately inform the CPSC of a failure to comply, a defect, or such a risk unless it has actual knowledge that the Commission has been adequately informed of such failure to comply, defect or risk.

2. When to Report

Section 15 requires firms to report "immediately." This means that a firm should notify the Commission within 24 hours of obtaining information described in section A.1 ("What and Where to Report") above. Guidelines for determining whether a product defect exists, whether a product creates an unreasonable risk of serious injury or death, and whether a report is necessary or appropriate are provided in 16 C.F.R. § 1115.12. Section II of this handbook does the same.

A company **must** report to the Commission within 24 hours of obtaining reportable information. The Commission encourages companies to report **potential** substantial product hazards even while their own investigations are continuing. However, if a company is uncertain whether information is reportable, the firm may spend a reasonable time investigating the matter. That investigation should not exceed 10 working days unless the firm can demonstrate that a longer time is reasonable in the circumstances. Absent such circumstances, the Commission will presume that, at the end of 10 working days, the firm has received and considered all information that would have been available to it had a reasonable, expeditious, and diligent investigation been undertaken.

The Commission considers a company to have obtained knowledge of product-safety-related information when that information is received by an employee or official of the firm who may reasonably be expected to be capable of appreciating the significance of that information. Once that occurs, under ordinary circumstances, five working days is the maximum reasonable time for that information to reach the chief executive officer or the official assigned responsibility for complying with the reporting requirements.

The Commission evaluates whether or when a firm should have reported. This evaluation will be based, in part, on what the company actually knew about the hazard posed by the product or **what a reasonable person, acting under the circumstances, should have known about the hazard while exercising due care including knowledge obtainable upon the exercise of due care to**

W291-1
(cont.)

ascertain the truth of representations. Thus, a firm is deemed to know what it would have known had it exercised due care in analyzing reports of injury or consumer complaints, or in evaluating warranty returns, reports of experts, in-house engineering analyses, or any other information.

3. Confidentiality of Reports

The Commission often receives requests for information reported under section 15(b). Section 6(b)(5) of the CPSA, 15 U.S.C. § 2055(b)(5), prohibits the release of such information unless a remedial action plan has been accepted in writing; a complaint has been issued; the reporting firm consents to the release; or the Commission publishes a finding that public health and safety requires public disclosure with a lesser period of notice than 15 days. In addition, a firm claiming that information it has submitted is a trade secret or confidential commercial or financial information must mark the information as "confidential" in accordance with section 6(a)(3) of the CPSA, 15 U.S.C. § 2055(a)(3). That should be done when the information is submitted to the Commission. The firm will receive an additional opportunity to claim confidentiality when it receives subsequent notice from the Commission's Freedom of Information Office that the information may be disclosed to the public in response to a request. If section 6(b)(5) does not apply, the CPSC staff will not treat information as exempt from disclosure to the public under section 6(a) of the CPSA, 15 U.S.C. § 2055(a), and the Freedom of Information Act, absent a specific claim for confidential treatment.

B. Section 37 Reports

Section 37 of the CPSA requires manufacturers of consumer products to report information about settled or adjudicated lawsuits.[5] Manufacturers must report if:

- a particular model of the product is the subject of at least three civil actions filed in federal or state court;

- each suit alleges the involvement of that particular model in death or grievous bodily injury—mutilation or disfigurement, dismemberment or amputation, the loss of important bodily functions or debilitating internal disorder, injuries likely to require extended hospitalization, severe burns, severe electric shock, or other injuries of similar severity;

- during one of the following two-year periods specified in the law, each of the three actions results in either a final settlement involving the manufacturer or in a court judgment in favor of the plaintiff:

  January 1, 2011 – December 31, 2012
  January 1, 2013 – December 31, 2014
  January 1, 2015 – December 31, 2016
  January 1, 2017 – December 31, 2018

and

- The manufacturer is involved in the defense of or has notice of each action prior to the entry of the final order and is involved in discharging any obligation owed to the plaintiff as a result of the settlement or judgment.

W291-1
(cont.)

[5]The Commission has issued a rule interpreting the requirements of section 37 at 16 C.F.R. part 1116. The Commission recommends that manufacturers considering whether they have section 37 reporting obligations refer to that rule, particularly in determining whether products involved in different lawsuits are the same particular model.

1. What to Report

A report under section 37 must contain:

- The name and address of the manufacturer of the product.
- The model and model number or designation of the product.
- A statement as to whether the civil action alleged death or grievous bodily injury and in the case of the latter, the nature of the injury. For reporting purposes, the plaintiff's allegations as to the nature of the injury are sufficient to require a report, even if the manufacturer disagrees with the allegations.
- A statement as to whether the case resulted in a final settlement or a judgment in favor of the plaintiff. However, a manufacturer need not provide the amount of a settlement.
- In the case of a judgment in favor of the plaintiff, the name and case number of the case and the court in which it was filed.

A manufacturer may also provide additional information, if it chooses. Such information might include a statement as to whether the manufacturer intends to appeal an adverse judgment, a specific denial that the information it submits reasonably supports the conclusion that its product caused death or grievous bodily injury, and an explanation why the manufacturer has not previously reported the risk associated with the product under section 15.

2. When and Where to Report

A manufacturer must report within 30 days after a judgment or final settlement in the last of three lawsuits. The same is true of any additional lawsuits involving the

W291-1
(cont.)

same model that are settled or adjudicated in favor of the plaintiff during the same two-year period.

Companies must file section 37 reports in writing to the Office of Compliance and Field Operations, U.S. Consumer Product Safety Commission, 4330 East West Highway, Bethesda, Maryland 20814 with a copy to Section15@cpsc.gov.

3. Confidentiality of Reports

Under section 6(e) of the CPSA, the Commission and its employees may not publicly disclose c information reported under section 37 except that such information may be furnished to the reporting manufacturer or Congress, under certain circumstances. By law, reporting under section 37 is not an admission of the existence of an unreasonable risk of injury, a defect, a substantial product hazard, an imminent hazard, or any other liability under any statute or common law. Information voluntarily provided that is in addition to information required to be reported under Section 37, is governed by the confidentiality provisions governing Section 15 reports (see above section A.3).

C. Section 102 Reports

Section 102 of the Child Safety Protection Act requires that companies report certain choking incidents to the Commission. Each manufacturer, distributor, retailer, and importer of a marble, a ball with a diameter of 1.75" or less ("small ball"), latex balloon or other small part, or a toy or game that contains such a marble, ball, balloon, or other small part must report information that reasonably supports the conclusion:

1) that a child (regardless of age) choked on such a marble, small ball, balloon, or small part; and

2) that, as a result of the incident, the child died, suffered serious injury, ceased breathing for any length of time, or was treated by a medical professional.

1. What to Report

The report should include the name and address of the child who choked and the person who notified the firm of the incident, a detailed identification of the product, a description of the incident and any resulting injuries or medical treatment, information about any changes made to the product involved or its labeling or warnings to address the risk of choking, and the details of any public notice or other corrective action planned. Firms should refer to 16 C.F.R. Part 1117 for more detailed information about this reporting requirement.

W291-1
(cont.)

2. When and Where to Report

Section 102 reports must be filed within 24 hours of obtaining the information.

A company must file a section 102 report with the Office of Compliance and Field Operations by mail, telephone (301-504-7520), or fax (301-504-0359). Telephone reports must be followed with a written confirmation.

3. Confidentiality of Reports

Section 102 reports receive the same confidentiality treatment as information submitted under section 15 of the CPSA.

II. Identifying a Defect

The Commission's reporting requirements provide information that assists the Commission in evaluating whether some form of remedial action is appropriate. However, in the absence of a regulation that addresses a specific risk of injury, the product in question must contain a defect that creates a substantial risk of injury to the public to warrant such remedial action. The Handbook next discusses the considerations that go into determining whether a product defect exists and, if so, whether the risk presented by that defect is substantial.

A defect could be the result of a manufacturing or production error; or it could result from the design of, or the materials used in, the product. A defect could also occur in a product's contents, construction, finish, packaging, warnings, and/or instructions. (See 16 C.F.R. § 1115.4)

Not all products that present a risk of injury are defective. A kitchen knife is one such example. The blade has to be sharp to allow the consumer to cut or slice food. The knife's sharpness is not a product defect, even though some consumers may cut themselves while using the knife.

In determining whether a risk of injury associated with a product could make the product defective, the Commission considers the following:

1. *What is the utility of the product? What is it supposed to do?*
2. *What is the nature of the risk of injury that the product presents?*
3. *Is the risk obvious to the consumer?*
4. *What is the need for the product?*
5. *What is the population exposed to the product and its risk of injury?*
6. *Are there adequate warnings and instructions that mitigate the risk?*

W291-1
(cont.)

7. *What is the Commission's experience with the product?*

8. *Is the risk of injury the result of consumer misuse, and is that misuse foreseeable?*

9. *Finally, what other information sheds light on the product and patterns of consumer use?*

If the information available to a company does not reasonably support the conclusion that a defect exists, the firm need not report to the Commission under the defect reporting provision of section 15(b)(2) of the CPSA. However, since a product may be defective even when it is designed, manufactured, and marketed exactly as intended, a company in doubt as to whether a defect exists should still report if the potential defect could create a substantial product hazard. A firm that is in doubt as to whether a defect exists should only fail to report if the firm is certain that there is no substantial product hazard. Additionally, a firm must report if it has information indicating the product creates an unreasonable risk of serious injury or death. See 15 U.S.C. §2064(b)(4) and 16 C.F.R. § 1115.6.

If the information obtained by a company supports a conclusion that a product has a defect, the company must then consider whether the defect could create a substantial product hazard. Generally, a product could create a substantial hazard when consumers are exposed to a significant number of units or if the possible injury is serious or is likely to occur. However, because a company ordinarily does not know the extent of public exposure or the likelihood or severity of potential injury when a product defect first comes to its attention, the company should report to the Commission even if it is in doubt as to whether a substantial product hazard exists.

Section 15(a)(2) lists criteria for determining when a product creates a substantial product hazard. Any one of the following factors could indicate the existence of a substantial product hazard:

- **Pattern of defect.** The defect may stem from the design, composition, content, construction, finish, or packaging of a product, or from warnings and/or instructions accompanying the product. The conditions under which the defect manifests itself must also be considered in determining whether the pattern creates a substantial product hazard.

- **Number of defective products distributed in commerce.** A single defective product could be the basis for a substantial product hazard determination if an injury is likely or could be serious. By contrast, defective products posing no risk of serious injury and having little chance of causing even minor injury ordinarily would not be considered to present a substantial product hazard. The number of products remaining with consumers is also a relevant consideration.

- **Severity of risk**. A risk is considered severe if the injury that might occur is serious, and/or if the injury is likely to occur.

- **Likelihood of injury.** The likelihood is determined by considering the number of injuries that have occurred, **or that could occur,** the intended or reasonably foreseeable use or misuse of the product, and the population group (such as children, the elderly, or the disabled) exposed to the product.

A substantial product hazard also exists when a failure to comply with an applicable consumer product safety rule, creates a substantial risk of injury to the public.

III. CPSC Evaluation of Section 15 Reports

When a company reports to the Commission, the staff of the Office of Compliance and Field Operations undertakes the same product hazard analysis as that requested of firms. First, the staff considers whether the product contains a defect. If the staff believes there is a defect, it then assesses the substantiality of the risk presented to the public, using the criteria listed in section 15 (that is, pattern of defect, number of defective products distributed in commerce, severity of the risk, likelihood of injury and other appropriate data). In determining preliminarily whether the product in question creates a substantial product hazard[6], the staff applies hazard priority standards to classify the severity of the problem.

The hazard priority system allows the Commission staff to rank defective products uniformly. For example, a Class A hazard rating is reserved for product defects that present a strong likelihood of death or grievous injury or illness to the consumer. Should the staff make a preliminary determination that a product creates a substantial product hazard; the hazard priority system also provides a guide for selecting the level and intensity of corrective action.

[6]The decision is preliminary because only the Commissioners, after a hearing, can make a formal determination that a product is defective and creates a substantial product hazard.

Class A Hazard

> Exists when a risk of death or grievous injury or illness is likely or very likely, or serious injury or illness is very likely.

Class A hazards warrant the highest level of attention. They call for a company to take immediate, comprehensive, and expansive corrective action measures to identify and notify consumers, retailers and distributors having the defective

product and to remedy the defect through repair or replacement of the product, refunds, or other measures.

W291-1
(cont.)

Class B Hazard

> Exists when a risk of death or grievous injury or illness is not likely to occur, but is possible, or when serious injury or illness is likely, or moderate injury or illness is very likely.

Class C Hazard

> Exists when a risk of serious injury or illness is not likely, but is possible, or when moderate injury or illness is not necessarily likely, but is possible.

Regardless of whether a product defect is classified as a Class A, B, or C priority hazard, the common element is that each of these defects creates a substantial product hazard that requires corrective action to reduce that risk of injury.

The priority given to a specific product defect provides a guideline for determining how best to communicate with owners and users of the defective product and to get them to respond appropriately. While some companies have exemplary track records in communicating with consumers independently, it is still to a company's advantage to work with the Commission staff, using both the company's and the Commission's skills and resources to conduct an effective product recall.

IV. Fast Track Product Recall Program (No Preliminary Determination (PD) of Hazard)

A firm that files a section 15(b) report may wish to use of an alternative procedure that the Commission has established to expedite recalls.[7] The program is called the "Fast Track Product Recall Program" (no PD). If a firm reports a potential product defect and, within 20 working days of the filing of the report, implements with CPSC a consumer-level voluntary recall that is satisfactory to the staff, the staff will not make a preliminary determination that the product contains a defect which creates a substantial product hazard.

In cases where staff is unable to evaluate and approve implementation of the corrective action plan within 20 working days even though the firm has submitted all the necessary information in a timely manner, the firm may still use the Fast Track Product Recall program, and staff generally will not make a preliminary hazard determination despite the delay.

This program allows the staff and company to work together on a corrective action plan almost immediately, rather than spending the time and other resources necessary to investigate the reported defect further to determine whether it rises to the level of a substantial product hazard.

W291-1
(cont.)

To participate in this program, companies must:

- provide all of the information required for a full report (16 C.F.R. § 1115.13(d));
- request to participate in the program; and
- submit a proposed corrective action plan with sufficient time for the Commission staff to analyze any proposed repair, replacement, or refund offer and to evaluate all notice material before the implementation (announcement) of the CAP which is to occur within 20 working days of the report.

[7]This program is described in more detail in the Federal Register of July 24, 1997, 62 Fed. Reg. 39,827-39,828. http://www.cpsc,gov/businfo/frnotices/fr97/frnopd.pdf.

V. Putting Together a Corrective Action Plan

A. Preparing For a Product Recall

It is rare that any two recall programs will ever be identical. Therefore, companies should be prepared to address issues that invariably arise. For instance:

- What is the defect that causes the product hazard?
- What caused the product defect to occur in the first place?
- Where are the unsafe products? How many are there?
- Did the product fail to comply with government safety regulations? How?
- Was the government or the appropriate regulatory body informed about the defect or lack of compliance?
- Has the company discontinued production and shipments of these products to distributors?
- Has the company notified retailers to stop selling the product and asked them to help identify consumers who own the product?
- Has the company started reviewing existing databases to identify potential product owners, *e.g.*, product registration and customer service records?
- Has a press release been prepared announcing the recall? What other forms of public notice are needed? Is the firm utilizing social media and

W291-1
(cont.)

digital and mobile communication platforms to get its message out? If so, how will it do so? If not, why not?

- Has a toll-free telephone service been set up that will be able to handle the number of calls expected after the recall is announced?
- Has the firm's website been modified to announce the recall and accept email requests to participate?
- What is the company's estimate of the cost of the product recall campaign?
- Is the company prepared to deploy manpower and/or fund an effort to provide replacement parts for defective products or to exchange them for new products that do not have the problem?
- Has a plan been developed to ship replacement parts or new units to distributors participating in the product recall, or otherwise repair units in their inventory?
- Has a plan been developed regarding the disposition of returned product? How will the product be reworked, broken down for reclamation of critical components, or destroyed? Are procedures in-place to ensure proper control and tracking of all defective materials returned in the recall?
- Is the company prepared to monitor the product recall and provide timely reports to the Commission on the progress of the recall?
- How is the company upgrading its quality control or risk analysis procedures to prevent a similar product recall in the future?

This list addresses administrative and operational functions of a company involved in a product recall. Even if a product recall is merely potential, a company should be prepared to respond to the questions listed above.

B. Elements of a Recall

A company that undertakes a recall should develop a comprehensive plan that reaches throughout the entire distribution chain to consumers who have the product. The company must design each communication to reach affected consumers, motivate people to respond to the recall and take the action requested by the company.

Once the staff and a company agree on a remedy to correct a product defect, the staff works with the company to put together an effective plan for public notification and implementation of the recall. The information that should be

W291-1
(cont.)

included in a corrective action plan ("CAP") is set forth at 16 C.F.R. § 1115.20(a). A plan must include the company's agreement that the Commission will publicize the terms of the plan to inform the public of the nature of the alleged substantial product hazard and the actions being undertaken to correct that hazard.

The objectives of a recall are:

1. to locate all defective products as quickly as possible;

2. to remove defective products from the distribution chain and from the possession of consumers; and

3. to communicate accurate and understandable information in a timely manner to the public about the product defect, the hazard, and the corrective action. Companies should design all informational material to motivate retailers and media to get the word out and consumers to act on the recall.

In determining what forms of notice to use, the paramount consideration should be the level of hazard that the recalled product presents. Class A hazards warrant the highest level of company and Commission attention. Other considerations include where and how the product was marketed, its user population, the estimated useful life of the product, and how the product is most likely to be maintained and repaired.

A company conducting a recall must take particular care to coordinate the notice portion of the recall so that all participating parties, including traditional and on-line retailers, have sufficient advance notice so that they can carry out the actions agreed upon. Notice also needs to be balanced—the purpose of some elements, such as news releases, press conferences, and video news releases—is to get the media to publicize information about the recall widely. Other elements, such as advertisements and posters, ensure that the information is available to the public throughout the course of the recall and helps reaching consumers who did not hear the original announcement.

VI. Communicating Recall Information

The Commission encourages companies to be creative in developing ways to reach owners of recalled products and motivate them to respond. The following are examples of types of notice that may be appropriate. This list is meant as a guide only, and is by no means all-inclusive. As new or innovative methods of notice and means of communication become available, such as social media, the staff encourages their use.

- a joint news release from CPSC and the company;

W291-1
(cont.)

- targeted distribution of the news release;
- a dedicated toll-free number and fax number for consumers to contact to respond to the recall notice;
- information on company external websites;
- a video news release to complement the written news release;
- a national news conference and/or television or radio announcements;
- use of a firm's social media presence to notify consumers of the recall, including Facebook, Google +, YouTube, Twitter, Flickr, Pinterest, company blogger networks, and blog announcements;
- direct notice to consumers known to have the product—identified through registration cards, sales records, catalog orders, retailer loyalty cards, or other means;
- notices to distributors, dealers, sales representatives, retailers (traditional brick and mortar and on-line), service personnel, installers, and other persons who may have handled or been involved with the product;
- purchase of mailing lists of populations likely to use the product;
- use of mobile scanners to obtain information on recalls from mobile devices;
- paid notices via television, or radio, Google, Facebook, and other online search engines;
- paid notices in national newspapers and/or magazines to reach targeted users of the product;
- paid notices through local or regional media;
- recall posters at stores;
- notices in product catalogs, newsletters, and other marketing materials;
- posters for display at locations where users are likely to visit, such as stores, medical clinics, pediatricians' offices, child care centers, repair shops, equipment rental locations, and others;
- notices to trade groups, utilities, and home/fire inspectors as applicable;

- notices to repair/parts shops;
- service bulletins;
- notices included with product replacement parts/accessories.
- notices to day care centers;
- notices to thrift stores and other secondhand retailers;
- incentives such as money, gifts, premiums, or coupons to encourage consumers to return the product;

The Communications staff must review and agree upon press releases and social media based communications that a company intends to use in a product recall before publication or dissemination. The Compliance staff must also review and agree upon all other notice to be disseminated. It is, therefore, imperative that companies give the staff advance drafts of all notices or other communications to media, customers, and consumers.

CPSC is first to issue the approved public communication messages and then recalling firm follows with issuance of its approved communication messages.

CPSC uses traditional and online media to communicate recalls to the public in plain language using information from agreed-upon joint press releases. Traditional media includes both print and broadcast outlets. Online media includes social media, mobile platforms, and CPSC's external websites. In media platforms that capture two-way communications, CPSC only manages the messages posted by CPSC.

Following are some specific suggestions for communicating recall information.

A. News Releases

Unless a company can identify all purchasers of a product being recalled and notify them directly, the Commission typically issues a news release jointly with the firm. The Compliance staff develops the wording of the release with the recalling company in conjunction with the Commission's Office of Communication. The agreed-upon language for the news release provides the foundation for preparing other notice documents. The Commission discourages unilateral releases issued by companies because they create confusion among the media and public, particularly if CPSC is also issuing a release on the same subject.

The Office of Communications sends the news releases to national wire services, major metropolitan daily newspapers, television and radio networks, and

W291-1
(cont.)

periodicals on the agency's news contact mailing list, and consumers who have signed up to receive direct notification of product recall news. News releases from the Commission receive wide media attention and generate a good response rate from consumers.

Each recall news release must use the word "recall" in the heading and should begin, "In cooperation with the U.S. Consumer Product Safety Commission (CPSC)...."

Recall news releases must include the following:

- the firm's legal and commonly known trade name and the city and state of its headquarters;
- whether the recalling firm is the manufacturer (or importer), distributor, or retailer of the product;
- if the firm is not the manufacturer, the manufacturer, including importers, of the product and the country of manufacture;
- if the product is manufactured outside the U.S., the identity of the foreign manufacturer or U.S. importer must include the city and country of its headquarters;
- all significant retailers, by commonly known trade name, of the product. Significant is defined by 16 C.F.R. § 1115.27 and is in the sole discretion of Staff;
- number of product units covered by recall, including numbers manufactured, imported and/or distributed;
- a description of the product, including product name, the intended consumer population (i.e. infants, children or adults), product's colors and sizes, model numbers, date codes, sku's and tracking labels and their exact location on the product;
- hi-resolution electronic or digital color photographs that clearly show identifying features of the product;
- clear and concise description of the product's actual or potential hazards that give rise to the recall, including product defect and the type of hazard or risk (i.e. laceration, entrapment, burn…);
- for each make and model -- month and year manufacture of product began and ended, retail sales began and ended;
- approximate retail price or price range;
- concise summary of all incidents associated with circumstances giving rise to the recall, including number of incidents, property damage due to incidents, injuries and deaths, including age of persons injured and killed;
- complete instructions for how to participate in the recall described in a manner that will motivate the consumer to take advantage of the remedy.

CPSC posts recall news releases on its external website.

W291-1
(cont.)

B. Video News Releases

A video news release (VNR) is a taped version of the written news release that describes the recall in audio-visual terms. Distributed via satellite to television stations nationwide, it is an effective method to enhance a recall announcement. A VNR increases the chances that television news media will air information about a recall because it effectively provides news of the recall to television news producers in the form that they need.

Commission staff works with firms to produce VNRs announcing recalls. Like news releases, VNRs need to communicate basic information clearly and concisely. VNRs should incorporate the same information as the news release, as well as video images of the product. They often also include brief statements of company officials and/or the Chairman of the Commission. When writing a VNR script, remember that, if this information is to reach consumers, television networks or local stations must pick it up, which means that the script must be written for television producers. The VNR should be produced as a bites and cover package and not be a fully narrated video. At times the CPSC will produce and distribute its own VNR announcing the recall. Appropriate legal notifications and review will be provided to the recalling firm.

A brief guide describing how to produce a VNR is available from the Office of Compliance and Field Operations upon request.

C. Posters

Posters are an effective means of providing continuing notice of recalls to consumers at points of purchase or other locations that they visit. Guidelines for posters and counter cards:

- Keep them BRIEF and eye-catching; in general, a poster requires far fewer words than a news release.
- Describe the hazard and tell consumers what to do.
- Use color to make the poster stand out.
- Use a print font, size, and color that provides a strong contrast to the background color of the poster.
- Include the terms "safety" and "recall" in the heading.
- Use a good quality line drawing or photograph of the product with call outs identifying product information, such as model numbers and date codes.
- The firm’s toll-free telephone number should be in large size type at the bottom of the poster.
- The poster should include "Post until [date at least 120 days from recall announcement]."
- Consider tear-off sheets with each poster with information on the recall for consumers to take home.

- Use a QR code or other mobile scanning code to let consumers act on the recall immediately.

The recalling company should contact the firms or individuals that the company wants to display the posters before the recall is announced. The company should explain the reason for the recall and the contribution to public safety that the posters provide. The company should also:

- Advise retailers or other firms to place the posters in several conspicuous locations in their stores or offices where customers will see them, *e.g*., the area where the product was originally displayed for sale, store entrances, waiting rooms in pediatric clinics, service counters at repair shops.

- Provide sufficient numbers of posters for retailers or others to display them in more than one place in each store or location, and provide a contact for ordering additional posters.

CPSC recommends that posters be 8.5 x 11 inches. This size is the easiest to mail in bulk quantities. Larger sizes may be appropriate for repair and service shops. Also, many retailers, particularly large chains, have specific requirements for posters, including size and some product identification information. To avoid delays and having to reprint, a company producing a recall poster should take care to contact retailers in advance to see if they have any such requirements.

D. Social Media

Firms should notify its customers using all available social media and mobile platforms including firm Facebook, Google+ pages,Twitter accounts, You Tube accounts, Pinterest , Flickr blogs and company blogging networks in an effort to get as broad a notice as possible. Guidelines for such notifications:

- should be on the firm's website's first entry point, such as the home page;
- should include the words "recall" and "safety";
- contains all recall information available in the news release;
- permits persons to request remedy directly from website;
- Facebook, Twitter, Flickr, Pinterest or other social media notification must link to website location that includes recall information available in the news release.

E. Other Forms of Notice

Like news releases and posters, letters, advertisements, bulletins, newsletters, and other communications about a recall need to provide sufficient information and motivation for the reader or listener to identify the product and to take the action you are requesting. They should be written in language targeted to the intended audience.

W291-1
(cont.)

- Letters or other communications should be specific and concise.

- The words "Important Safety Notice" or "Safety Recall" should appear at the top of each notice and cover letter and should also be on the lower left corner of any mailing envelope.

- Notices to retailers and distributors should explain the reason for the recall, including the hazard, and contain all the instructions needed to tell them how to handle their product inventory, as well as instructions for displaying posters or notices, providing information to consumers, and disposing of returned products.

- All letters and other notices to consumers should explain clearly the reason for the recall, including injury or potential injury information, and provide complete instructions.

F. Toll-Free Numbers/URL/E-mail

A company conducting a recall should provide a toll-free (800/888/877/866) telephone number, website URL for consumers to respond to the recall announcement, and email address. Generally, this number and address should be dedicated only to the recall. Historically, the Commission staff has found that most company systems for handling consumer relations or for ordering products, repairs, or accessories are unable to respond effectively to callers about recall announcements, particularly during the first few weeks after the initial announcement. Use of a URL address or e-mail address should be included for every recall.

When establishing a telephone system to handle a recall, be over-generous in estimating consumer response, especially during the first several days/weeks. It is easier to cut back than it is to add more capacity once a recall is announced, and consumers who are unable to get through may not keep trying.

Whether you use an automated system or live operators to answer the calls, prepare scripts and instructions for responding to questions. Operators or taped messages should begin by identifying the firm and product and explaining the reason for the recall. Most consumers who hear about a recall by radio, television, or word of mouth will not remember all the information they initially heard. Again, at its beginning, the message should reinforce the need for listeners to act, particularly if the message is lengthy. CPSC Compliance staff needs to review all scripts before the recall is announced. All automated systems should provide a number for consumers to contact the firm for special problems, *e.g.*, problems completing repairs or installing parts.

Recalling firms should ensure that their call center makes recall response a priority.

W291-1
(cont.)

Firms should also provide a website and e-mail for consumers to register to participate in the recall.

VII. Monitoring Recalled Products

Every recall conducted in coordination with the staff is monitored by both the recalling firm and the Commission. Recalling firms need to understand and prepare for the monitoring since the Consumer Product Safety Improvement Act (CPSIA) makes it unlawful for any person to sell, offer for sale, manufacture for sale, distribute in commerce, or import into the United States any consumer product or substance that is subject to a voluntary corrective action taken by the manufacturer, in consultation with the Commission (CPSA Section 19(a)(2)(B)-(C), 15 U.S.C. Section 2068(a)(B)-(C).

- The law applies to both voluntary recalls by a manufacturer and recalls ordered by the Commission.
- The definition of "manufacturer" includes an importer.
- Any person or firm distributing recalled products in commerce may be liable.
- It is your responsibility to monitor CPSC recalls and ensure that your business complies with the law.

CPSC monitoring of product recalls includes the following:

- Submission of monthly progress reports to the Office of Compliance and Field Operations using a required form so the staff can assess the effectiveness of the firms recall. Information requested includes number of products remedied, number of consumers notified of the recall, and any post recall announcement incidents and injuries.
- Recall verification inspections are conducted to monitor firm implementation of the corrective actions undertaken.
- Retail visits are conducted by CPSC field staff and state investigators to confirm receipt of recall notification and to assure recalled products are quarantined and no longer being sold.
- Requests to dispose or destroy recalled products should be submitted in writing to recalledproductdisposal@cpsc.gov so that CPSC investigator can either witness disposal or make arrangements for other verification of destruction.

Recalling firms need to take every step to assure recalled products are quarantined and segregated from other products throughout the distribution chain. Any third party hired to destroy or dispose of recalled products needs to be monitored by the recalling firm to assure they understand the importance of keeping recalled products separate from other returned products and that they take appropriate steps to assure proper disposal of recalled products. CPSC

staff will witness the safe disposal of recalled products or request written verification of such disposal.

When a firm determines that the corrective action plan has been implemented to the best of the firm's ability and as many products as possible have been removed from the marketplace, it may submit a final progress report requesting that Commission monitoring of the recall be ended. A CPSC field investigator may conduct a close-out recall inspection of the firm upon the firm's request that the file be close. At that time the staff will review the number of notifications made to owners of the product and the number of products returned and/or corrected as well as whether there have been any post recall incidents/injuries or deaths involving the recalled product. As a result of the review of this information, recalling firms should maintain appropriate records to show steps taken to reach owners of the product, the distribution chain, and others. The Compliance staff will evaluate the effectiveness of the firm's corrective action plan. The staff could seek broader corrective action if the plan does not prove effective. When the staff closes its files on the corrective action plan, the firm should continue to implement the recall plan until as many products as possible have been removed from the marketplace. The firm's toll free number should be maintained as well as notice of the recall on the firm's website so consumers can continue to reach the firm in the event they discover a recalled product. Should the firm decide to change or discontinue its toll-free recall number, the firm must immediately notify the Office of Compliance and Field Operations and provide a new recall contact number for the firm. If there are changes to the implementation of the corrective action plan, the firm should also immediately contact the staff. The agreed upon press release announcing the recall is maintained on the Commission's website. Any modifications to the firm's phone number or obligations under the corrective action plan would be posted on the existing press release by way of an update with the date the change was made.

VIII. Developing a Company Policy and Plan to Identify Defective Products and To Undertake a Product Recall

Companies whose products come under the jurisdiction of the CPSC should consider developing an organizational policy and plan of action if a product recall or similar action becomes necessary, whether it involves the CPSC or another government agency. This policy and any related plans should focus on the early detection of product safety problems and prompt response.

A. Designating A Recall Coordinator

Designating a company official or employee to serve as a "recall coordinator" is a significant step that a firm can take to meet its product safety and defect reporting responsibilities. Ideally, this coordinator has full authority to take the steps necessary (including reporting to the Commission) to initiate and

implement all recalls, with the approval and support of the firm's chief executive officer.

The recall coordinator should have the following qualifications and duties:

- Knowledge of the statutory authority and recall procedures of the U.S. Consumer Product Safety Commission;
- Ability and authority to function as the central coordinator within the company for receiving and processing all information regarding the safety of the firm's products. Such information includes, *e.g.*, quality control records, engineering analyses, test results, consumer complaints, warranty returns or claims, lawsuits, and insurance claims.
- Responsibility for keeping the company's chief executive officer informed about reporting requirements and all safety problems or potential problems that could lead to product recalls;
- Responsibility for making decisions about initiating product recalls;
- Authority to involve appropriate departments and offices of the firm in implementing a product recall;
- Responsibility for serving as the company's primary liaison person with CPSC.

B. Role Of The Recall Coordinator

At the outset, the recall coordinator should fully review the company's product line to determine how each product will perform and fail under conditions of proper use and reasonably foreseeable misuse or abuse. Through research and analysis, product safety engineers can identify the safety features that could be incorporated into products that present safety risks to reduce their potential for future injury.

The company should institute a product identification system if one is not now in use. Model designations and date-of-manufacture codes should be used on all products, whether they carry the company's name or are privately labeled for other firms. If a product recall is necessary, this practice allows the company to identify easily all affected products without undertaking a costly recall of the entire production. Similarly, once a specific product has been recalled and corrected, a new model number or other means of identification used on new corrected products allows distributors, retailers, and consumers to distinguish products subject to recall from the new items. Until a production change can be made to incorporate a new model number or date code, some companies have

used sticker labels to differentiate products that have been checked and corrected from recalled products.

W291-1
(cont.)

IX. Records Maintenance

The goal of any product recall is to retrieve, repair, or replace those products already in consumers' hands as well as those in the distribution chain. Maintaining accurate records about the design, production, distribution, and marketing of each product for the duration of its expected life is essential for a company to conduct an effective, economical product recall. Generally, the following records are key both to identifying product defects and conducting recalls:

A. **Records of complaints, warranty returns, insurance claims, and lawsuits.** These types of information often highlight or provide early notice of safety problems that may become widespread in the future.

B. **Production records.** Accurate data should be kept on all production runs—the lot numbers and product codes associated with each run, the volume of units manufactured, component parts or substitutes use, and other pertinent information that will help the company identify defective products or components quickly.

C. **Distribution records.** Data should be maintained as to the location of each product by product line, production run, quantity shipped or sold, dates of delivery, and destinations.

D. **Quality control records.** Documenting the results of quality control testing and evaluation associated with each production run often helps companies identify possible flaws in the design or production of the product. It also aids the firm in charting and sometimes limiting the scope of a corrective action plan.

E. **Product registration cards.** Product registration cards for purchasers of products to fill out and return are an effective tool to identify owners of recalled products. The easier it is for consumers to fill out and return these cards, the greater the likelihood the cards will be returned to the manufacturer. For example, some firms provide pre-addressed, postage-paid registration cards that already have product identification information, *e.g.*, model number, style number, special features, printed on the card. Providing an incentive can also increase the return rate. Incentives can be coupons towards the purchase of other products sold by the firm, free accessory products, or entry in a periodic drawing for a product give away. The information from the cards then needs to be maintained in a readily retrievable database for use in the event a recall becomes necessary.

W291-1
(cont.)

X. Conclusion

Consumers expect firms to stand behind the products they produce and sell. Millions of products have been recalled over the years. Consumers believe they enjoy a safer, better product as a result of a recall conducted responsibly by company. How well a company conducts a timely, reasonable recall of a product can have a strong influence on consumers' attitude about the firm. Successful product recalls in the past have rewarded companies with continuing consumer support and demand for the firms' products.

For additional information about product recalls and reporting, call (301) 504-7520, fax (301) 504-0359, or by email at section15@cpsc.gov or visit the Commission's website at www.cpsc.gov (click on the Business icon).

From: Larry Organ
To: Privacy Regulations
Subject: Written Comments Regarding Proposed Changes CCPA
Date: Monday, February 24, 2020 11:40:22 AM
Importance: High

February 24, 2020

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

Dear Ms. Kim,

Under Definitions 999.301. (d), the proposed language, with changes reads:
"Categories of sources" mean types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers."

For greater clarity, I propose the following change in red below:

"Categories of sources" mean types or groupings of persons or entities from which a business collects personal information about consumers, by name or described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers."

W292-1

Logic: "enough particularity" is vague. By adding "by name or" it leaves no doubt that the law requires greater granularity. For example, "data broker" won't suffice when the specific source is "Exact Data, a Data Broker." If the goal is not to be that specific, the text should be written:

"Categories of sources" mean types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity, without naming the person or entity. They may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers."

Under Definitions 999.301. (e), the proposed language, with changes reads:
"Categories of third parties" mean types or groupings of third parties with whom the business shares personal information., described with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include the consumer directly, advertising

W292-2

networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers."

For greater clarity, I propose the following change in red below:

"Categories of third parties" mean types or groupings of third parties with whom the business shares personal information., described by name or with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers."

Logic: "enough particularity" is vague. By adding "by name or" it leaves no doubt that the law requires greater granularity. For example, "data broker" won't suffice when the specific third party is "Exact Data, a Data Broker." If the goal is not to be that specific, the text should be written:

W292-2 (cont.)

"Categories of third parties" mean types or groupings of third parties with whom the business shares personal information., described with enough particularity to provide consumers with a meaningful understanding of the type of third party, without naming the third party. They may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers."

SUMMARY: Adding "by name or" or "without naming the person or entity/third party" to the paragraphs above, gives covered organizations better direction how to follow the law.

Thank you for your consideration.

Exact Data
Larry Organ
CEO

[redacted]
Exact Data, 33 N. Dearborn Street, Suite 200, Chicago, IL 60602

From:	Robin Slade
To:	Privacy Regulations
Subject:	Comments on Revised Proposed Regulations: CCPA – OAL File 2019-1000-05
Date:	Monday, February 24, 2020 11:14:33 AM
Attachments:	SharedAssessmentsProgram_CCPA2.10.20Comments_24FEB2020.pdf

Dear Ms. Kim,

Please see the attached document, which is being submitted in response to the invitation for written comments on the updated notice of modifications to text of proposed regulations for the California Consumer Privacy Act [OAL File No. 2019-1001-05].

The Shared Assessments Program appreciates the opportunity to submit comments to the California Attorney General as part of the Attorney General's rule making process under the California Consumer Privacy Act (CCPA).
Thank you for your time and consideration. We'd be happy to address any questions you may have.

Best,
Robin

Robin Slade
EVP & COO

SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

[redacted] (c) | [redacted] (o)
[redacted]
www.sharedassessments.org

Save the Date for the 13th Annual Summit – April 29-30, 2020 – Arlington, VA

Certify your third party risk knowledge: The Certified Third Party Risk Professional (CTPRP) Program

SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

Date: February 24, 2020

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

From: Robin Slade, EVP & COO, The Shared Assessments Program
[redacted]

RE: UPDATED NOTICE OF MODIFICATIONS TO TEXT OF PROPOSED REGULATIONS AND ADDITION OF DOCUMENTS AND INFORMATION TO RULEMAKING FILE [OAL File No. 2019-1001-05]

The Shared Assessments Program appreciates the opportunity to submit comments to the California Attorney General as part of the Attorney General's rule making process under the California Consumer Privacy Act (CCPA).

The Shared Assessments Program has been setting the standard in third party risk assessments since 2005. Shared Assessments, which is the trusted source in third party risk assurance, is a member-driven, industry-standard body which defines best practices, develops tools, and conducts pace setting research. Shared Assessments Program members work together to build and disseminate best practices and develop related resources that give all third party risk management stakeholders a faster, more rigorous, more efficient and less costly means of conducting security, privacy and business resiliency control assessments. For more information on Shared Assessments, please visit: http://www.sharedassessments.org.

On behalf of the Shared Assessments Program and its members, thank you for accepting the following comments to the CCPA.

Legend to the comments:

- Shared Assessments' comments and proposed changes are in blue.
  - The Rationale for Clarification is given for proposed alternative language.
  - The Article, sections, and subsections are clearly identified and only those sections are included on which we have comments.
- The original CCPA proposed language is in single underline.
- California's 2/10/2020 CCPA changes are illustrated in red by double underline for proposed additions and by ~~strikeout~~ for proposed deletions.

DEPARTMENT OF JUSTICE Title 11.
Law Division 1. Attorney General Chapter 20. California Consumer Privacy Act Regulations
February 10, 2020

UPDATED NOTICE OF MODIFICATIONS TO TEXT OF PROPOSED REGULATIONS AND ADDITION OF DOCUMENTS AND INFORMATION TO RULEMAKING FILE [OAL File No. 2019-1001-05]

Article 3. Business Practices for Handling Consumer Requests
§ 999.313. Responding to Requests to Know and Requests to Delete – Subsection (c)

Comment and Rationale for Clarification:

- In section **§ 999.314,** the modified text in subsection (e) conveys that there could be instances where the service provider may need to act on behalf of the business in order to respond to the request of the consumer. The criteria listed in **§ 999.313** apply to the business, and not the service provider. To avoid confusion in the roles between parties, it would be important to understand if the parameters apply to the service provider of the business. Or, if it is assumed that such criteria below apply to the service providers when acting on behalf of the business.

(c) Responding to Requests to Know

W293-1

(3) ~~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.~~ In responding to a request to know, a business or a service provider acting on behalf of the business, is not required to search for personal information if all the following conditions are met:

a. The business does not maintain the personal information in a searchable or reasonably accessible format;

b. The business maintains the personal information solely for legal or compliance purposes;

c. The business does not sell the personal information and does not use it for any commercial purpose; and

d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.

Article 3. Business Practices for Handling Consumer Requests
§ 999.313. Responding to Requests to Know and Requests to Delete – Subsection (d)

Comment and Rationale for Clarification:

W293-2

The storage and retrieval of personal information on archived or backup systems is managed by categories of service providers and subcontractors that are supporting a businesses' operations. The data may be managed independently from the actual system. There may be routine reasons that data is restored for backup systems for disaster recovery, systems testing, business continuity, or change in location of the archive or backup system, without the data shifting to production status for future

use. The current language may create confusion for the business and vendors that manage the archive or backup systems processes.

(d) Responding to Requests to Delete

(3) If a business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system for continued commercial use or ~~next accessed or~~ used for a sale, disclosure, or commercial purpose.

W293-2 (cont.)

Article 3. Business Practices for Handling Consumer Requests
§ 999.314. Service Providers – Subsections (a)-(e)

Comment and Rationale for Clarification:

Subsection (a) language has created confusion as to the type of third party relationships that would be deemed a service provider providing services to an organization that is not a business, but per the definition in CCPA, a Service Provider processing information on behalf of a business. If the intent of (a) is to define a set of entities that collect data directly from consumers, or differentiate entities that provide services to non-profits, for example, that should be clarified.

W293-3

Regarding subsection (b), there are industry practices for the protocols of detecting data security incidents, which all require a level of investigation, which is missing from the clarification. In order to perform detect functions, there are related processes.

W293-4

With the addition of (e) the Service provider may be acting upon the direction of the business to fulfill the requests; however, the business has the direct consumer relationship and so is accountable for the process and mechanisms to verify the consumer request.

W293-5

(a) ~~To the extent that a person or entity~~ A business that provides services to a person or organization that is not a business, and that would otherwise meet the requirements and obligations of a "service provider" under ~~Civil Code section 1798.140(v)~~ the CCPA and these regulations, ~~that person or entity~~ that business shall be deemed a service provider for purposes of the CCPA and these regulations.

W293-3 (cont.)

(b) To the extent that a business directs a ~~person or entity~~ second business to collect personal information directly from a consumer on the first business's behalf, and the second business would otherwise meet ~~all other~~ the requirements and obligations of a "service provider" under the CCPA and these regulations ~~Civil Code section 1798.140(v), that person or entity~~ the second business shall be deemed a service provider of the first business for purposes of the CCPA and these regulations.

(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.~~ A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except:

W293-4 (cont.)

(1) To perform the services specified in the written contract with the business that provided the personal information;

(2) To retain and employ another service provider as a subcontractor, where the subcontractor meets the requirements for a service provider under the CCPA and these regulations;

(3) For internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source;

(4) To detect and investigate data security incidents, or protect against fraudulent or illegal activity; or

(5) For the purposes enumerated in Civil Code section 1798.145, subsections (a)(1) through (a)(4).

W293-4 (cont.)

(d) A service provider shall not sell data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business. ~~If a service provider receives a request to know or a request to delete from a consumer regarding personal information that the service provider collects, maintains, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial. The service provider shall also inform the consumer that it should submit the request directly to the business on whose behalf the service provider processes the information and, when feasible, provide the consumer with contact information for that business.~~

(e) If a service provider receives a request to know or a request to delete from a consumer, the service provider shall either act on behalf of the business in responding to the request, after verification by the business, or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider.

W293-5 (cont.)

Article 3. Business Practices for Handling Consumer Requests
§ 999.317. Training; Record-Keeping Subsections (b) & (e)

Comment and Rationale for Clarification:

The service provider may be responding to the consumer request, and it is unclear what record-keeping obligations extend to the service provider. In the case of (e) an organization may undergo audits or inspections of record management programs or compliance to CCPA by external auditors engaged by the organization. "Any" third party could be conveyed as too broad a category.

W293-6

W293-7

(b) A business shall maintain records of consumer requests made pursuant to the CCPA and how the business or its' service provider responded to said requests for at least 24 months. The business or its' service provider shall implement and maintain reasonable security procedures and practices in maintaining these records.

W293-6 (cont.)

(e) Information maintained for record-keeping purposes shall not be used for any other commercial purpose except as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and these regulations. Information maintained for record-keeping purposes shall not be shared with any third party for marketing or commercial purposes.

W293-7 (cont.)

From:	Aloni Cohen
To:	Privacy Regulations
Subject:	Comments on Proposed Regulations
Date:	Monday, February 24, 2020 7:45:55 AM
Attachments:	Feb-2020-CCPA-Comments.pdf Dec 2019 CCPA Comments.pdf

To whom it may concern,

Please find attached a letter regarding the Attorney General's proposed regulations, dated 24 Feburary 2020. Also attached is an earlier letter from 4 December 2019 which is referenced in the February 2020 letter.

Sincerely,
Aloni Cohen, PhD

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

Aloni Cohen, PhD

February 24, 2019

The February 2020 draft CCPA regulations put forth a misguided interpretation of the definition of "personal information" (Section 999.302). The regulation's definition makes for bad policy and ignores the CCPA's intent.

The problem in short

Suppose a free adult video site logs every video watched along with the associated IP address. It stores no other session or user information. Under the most obvious reading of Section 999.302 of the new draft CCPA regulations, the log would not constitute personal information. The site could, for example, tweet out every IP+video record publicly. Clearly, this is not the intent of CCPA.

"Personal information" in statute and draft regulations

W294-1

CCPA governs the use of “personal information.” Under the statute's definition, personal information definitely includes information that “could reasonably be linked” with a particular household. For reference, the statute's definition reads:

> 1798.140(o)(1): “Personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

The newest draft regulations includes new “Guidance Regarding the Interpretation of CCPA Definitions", which reads:

> 999.302(a) Whether information is “personal information,” as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that “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.” For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or

household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be "personal information."

Problems with 999.302

1. 999.302 distinguishes between what a specific business can do with data and what can be done with data more generally. The original definition demands protection of information if it can be reasonably linked with a particular household by anybody. In contrast, the draft regulation only requires protection of information if it can be reasonably linked by the business. It suggests that to free personal information from CCPA protection, a business doesn't have to make the information less identifiable, but to handicap its own identification capabilities. This is something industry critics of CCPA (who want to weaken the law) have been begging for. Their argument is that you can't expect every mom-and-pop data company to be able to figure out what elite computer scientists can do with data. That argument makes some sense, and it's clear that a lot is riding on the meaning of "reasonable" in CCPA's definition of personal information.

However, this distinction yields a nonsensical policy. For example, CCPA makes it illegal for a business to publicly tweet its users' personal information. But if the business can't reasonably link it to a household, then it's not personal information. And if it's not personal information, CCPA doesn't apply---they can tweet away. What should matter from a policy perspective is what the recipients of that information---anybody on the internet---can do with it.

2. 999.302 illustrates its point with the worst possible example: IP addresses. A typical household's IP address (say, on a family desktop) stays the same for months or years at time. During that period, every webpage they visit sees the IP. If anything "could reasonably be linked to a specific household," it's an IP address. But the draft regulation makes clear that it's possible for IP addresses to not be personal information. If the business doesn't keep around other information needed to link the IP address to the household, then the data is free from CCPA. W294-1 (cont.)

3. Personal information no longer includes all information that could reasonably be linked with a particular household. It only includes information that is "maintained in a manner that could be reasonably linked" with a particular household. Compare with the statute's language. The new definition regulations focus the definition of personal data on the form of the data: how it's maintained. It sidelines the power of the data: what can be done with it. For a data privacy regulation, this is backwards: the power of data, not its form, is what matters.

I made a related point in the earlier comments to the Attorney General. Those comments are dated December 4, 2019 and included as an attachment to this message. They focused on some subtleties in the law's definition of "probabilistic identifiers" and suggested specific language for regulations. The new draft regulations enshrine the worst interpretation of the ambiguous definition of probabilistic identifier as the main definition for personal information.

4. 999.302 misquotes the statute. The regulation changes “could reasonably be linked” to “could be reasonably linked.”

Recommendations

Remove 999.302 from the regulations. The statute does not distinguish between the capabilities of the business who controls the information and the potential recipients of the information. The regulations should not either. My comments dated December 4, 2019 suggested specific regulatory language for "probabilistic identifiers." They are attached to this message and may prove useful in crafting language for "personal information." W294-1 (cont.)

If some version of 999.302 must remain, change the example from an IP address to a cryptographically secure hash of a user's email address. This example fits the spirit of the regulation's change: it's information that if maintained in a certain way would allow a business to identify a user, but which can conceivably be maintained in a way to prevent the business (or anybody else) from doing so.

From: Lorrie Cranor
To: Privacy Regulations
Cc: Stacey Schesser
Subject: comments on revised proposed regulations
Date: Monday, February 24, 2020 6:49:34 AM
Attachments: CCPA Toggle Study Report.pdf

User Testing of the Proposed CCPA Do-Not-Sell Icon

February 24, 2020

Lorrie Faith Cranor, Director of CyLab Security and Privacy Institute, Bosch Distinguished Professor in Security and Privacy Technologies, FORE Systems Professor of Computer Science and of Engineering & Public Policy, Carnegie Mellon University ([redacted])

Hana Habib, PhD Candidate, School of Computer Science, Carnegie Mellon University ([redacted])

Yixin Zou, PhD Candidate, School of Information, University of Michigan ([redacted])

Alessandro Acquisti, Professor of Information Technology & Public Policy, Carnegie Mellon University ([redacted])

Joel Reidenberg, Stanley D. and Nikki Waxberg Chair and Professor of Law, Fordham University School of Law ([redacted])

Norman Sadeh, Professor of Computer Science and Co-Director Privacy Engineering Program, Carnegie Mellon University ([redacted])

Florian Schaub, Assistant Professor in the School of Information at the University of Michigan ([redacted])

CyLab Carnegie Mellon University Security and Privacy Institute

SCHOOL OF INFORMATION UNIVERSITY OF MICHIGAN

USABLE PRIVACY.ORG

CLIP Center on Law and Information Policy AT FORDHAM LAW SCHOOL

1. Overview

In a previous report to the California Attorney General's office (OAG) [1], we reported on a series of design sessions and online experiments we conducted to test the effectiveness of various approaches for communicating the presence of Do-Not-Sell choices. Our report provided recommendations, supported by empirical data, on what icons (buttons or logos) and text taglines most effectively signal the presence of an opt-out choice related to the sale of personal information. This choice is required to be made available to California consumers under the California Consumer Privacy Act. In our report we recommended the use of a blue *stylized toggle* icon paired with current CCPA taglines ("Do Not Sell My Personal Information" or "Do Not Sell My Info"):

 **Do Not Sell My Personal Information**

The choice of this icon reflected multiple design considerations: (1) Our *stylized toggle* used both a checkmark and an X to visually convey the availability of yes/no options. (2) We slanted the dividing line in the icon to prevent the icon from being confused with a real toggle control. (3) We recommended the color blue since blue is a neutral color that does not convey a particular state, unlike green or red. The user testing results reported in our previous report [1] show that this particular icon paired with the CCPA taglines indeed effectively communicates the presence of a choice, particularly one related to the sale of personal information, without substantial misconceptions. W295-1

The OAG's February 10, 2020 Revised Proposed Regulations [2] include a proposed opt-out button (§ 999.306.f) that is similar to, but not exactly like, the blue icon we had recommended [1]:

When we saw the OAG's proposed opt-out button, which we refer to as *CalAG toggle*, we were concerned that it might suffer from some usability problems:

1. The *CalAG toggle* icon could be confused with an actual toggle switch. In fact, the *CalAG toggle* icon's design appears to be closely modelled after an actual toggle switch as can be found in settings dialogs, for instance, in Apple's IOS mobile operating system.[1] In contrast, our proposed icon was a stylized representation of a toggle using both a checkmark and X, as well as a slanted line to divide them.

[1] See the Apple Developer Human Interface Guidelines: https://developer.apple.com/design/human-interface-guidelines/ios/controls/switches/

2. The *CalAG toggle* icon's close resemblance of a toggle switch in combination with the use of the color red may be misinterpreted as an indication of an off-state, i.e., a consumer may misinterpret the *CalAG toggle* icon as an indication that they have already opted-out of the sale of their personal information.
3. If the *CalAG toggle* icon is misinterpreted as a toggle switch in an off-state, a consumer might inaccurately assume that clicking the icon would reverse their opt-out and allow the company to sell their data, which is the opposite of the icon's intended function.

However, without testing, it is difficult to know how an icon will be perceived by users. Therefore, we conducted a follow-up online experiment to test for differences in interpretation between our proposed *stylized toggle* icon and the *CalAG toggle* icon. In addition, we created and tested a slightly modified version of the *CalAG toggle* icon, referred to as *CalAG-X toggle,* in which we increased the size of the X to give it a more visually balanced appearance next to the circle. We further tested each icon in a blue variant and in a red variant in order to determine the effects of both icon design and color on the icon's interpretation. For our experiment, we recruited 398 participants who were each randomly assigned to be shown one of the six toggle icons, all placed next to the "Do Not Sell My Personal Information" tagline.

Based on the findings from this follow-up study, we make the following recommendations:

W295-1 (cont.)

The CCPA opt-out button should use the *stylized toggle* in our earlier proposal because that toggle, when placed next to the "Do Not Sell My Personal Information" tagline, more effectively conveys the concept of do-not-sell without creating problematic misconceptions compared to the *CalAG toggle*. Our results show that the *stylized toggle* consistently and significantly outperformed the *CalAG toggle* and *CalAG-X toggle* in creating the expectation of making do-not-sell choices or confirming a do-not-sell request on the landing page. Importantly, the *stylized toggle* also significantly reduced the misconception that the icon with an actual control switch for the website's do-not-sell setting.

We recommend that the opt-out icon be colored blue instead of red. Our results suggest that whether the icon is blue or red has little or no impact on users' interpretations and expectations. In most cases, we found no significant differences between the red and blue *stylized toggle* icons. For cases with differences, the red version better conveyed choices related to the sale of personal information. However, it also increased the odds of the toggle being perceived as an actual control toggle switch that would change the setting of the website to "Do Not Sell My Personal Information," possibly because red, as a color generally associated with a negative state, conveyed the message that the setting "Do Not Sell My Personal Information" is currently off. We recommend the blue icon, which can represent a more neutral option that may be less likely to be misinterpreted as representing a user's current opt-out setting.

2. Methodology

After reading the proposed revision of CCPA [2], we were concerned about the possibility that the *CalAG toggle*, by using a circle instead of a checkmark and by removing the slanted dividing line, creates a close resemblance to the iOS toggle switch (see Figure 1) and might be misinterpreted as being an actual and direct control over whether or not the user wants their personal information to be sold. The fact that red is usually associated with a negative state further complicates the issue due to the existence of a double negative in conjunction with the "Do Not Sell My Personal Information" tagline — the user could interpret it as "my data is currently being sold" (because red is understood as the setting "Do Not Sell My Personal Information" is off), or "my data is currently not being sold" (because red indicates something is prohibited, and in this case could be interpreted as meaning the sale of personal information). We conducted an online experiment to examine whether the change of toggle style and color of the *CalAG toggle* might lead to different interpretations and expectations related to the sale of personal information compared to the findings in our earlier studies [1].

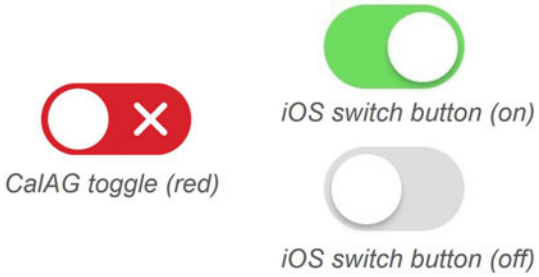


Figure 1: A comparison of the proposed CalAG opt-out button and the iOS toggle switch button.

W295-1
(cont.)

2.1 Study Design

To capture the potential interaction effects between icon style and color, we implemented a fully-factorial experimental design which included two color conditions and three style conditions. The resulting six conditions are shown in Figure 2. We tested blue versus red color to examine the potential impact of the color's indication of state: red is generally conceived as negative or something being prohibited, whereas blue is a neutral color. In addition to our proposed toggle icon (*stylized toggle*) and the toggle icon proposed by the California AG office in the revised CCPA regulation (*CalAG toggle*), we created a third condition for the toggle style, denoted as *CalAG-X toggle*, which fixes some aesthetical design details of the *CalAG toggle.* Specifically, we increased the size of the "X" to make it look visually equivalent to the circle. This creates a more harmonious look without substantially altering the design concept.

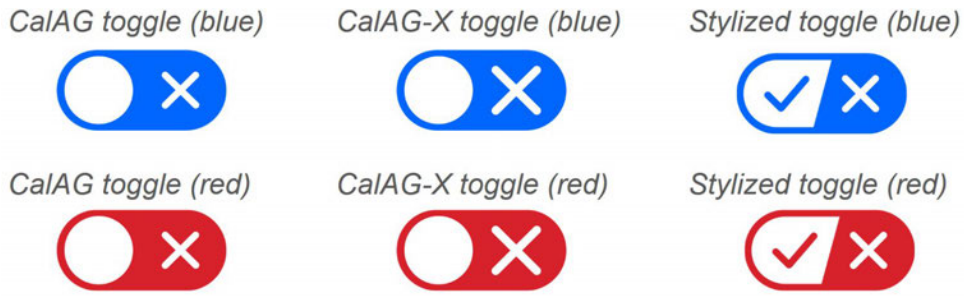


Figure 2: Icons tested in this study.

2.2 Evaluation Method

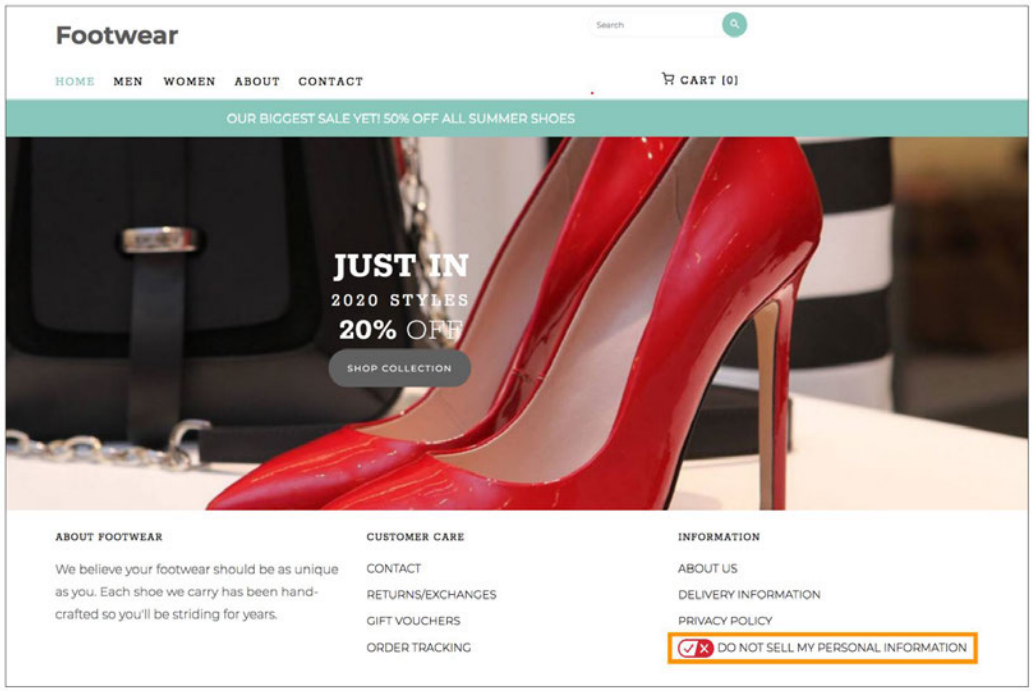
Similarly to our previous study [1], we conducted a between-subjects online study in which we showed participants one of the six icons at random, next to the CCPA tagline "Do Not Sell My Personal Information." Participants were shown a screenshot of a fictitious shoe retailer website called "Footwear," with the opt-out icon and tagline placed in the footer under the link to the website's privacy policy, to mimic the scenario of how users are likely to see a CCPA opt-out in the real world (see Figure 3). To ensure participants were able to read the text link within the survey, we highlighted the icon and tagline with an orange box and displayed a close-up of just the icon and tagline portion of the website.

After seeing the screenshot, we asked participants follow-up questions to explore which combinations of the icon style and color best conveyed the presence of a do-not-sell opt-out. The set of questions participants answered was similar to those asked in our previous testing [1] with minor modifications.[2] Participants were first asked to describe their expectations of what they thought would happen if they would click on the symbol and link shown in the orange box on the webpage. Additionally, we derived eight specific scenarios about people's possible expectations based on participants' open-ended responses in our previous studies. Three of these scenarios were accurate expectations related to do-not-sell, i.e., after clicking the user would be taken to a page where they could choose whether or not the website can sell their personal information, confirm that they do not want their personal information to be sold, or read more information about how the website uses and shares their personal information. Two scenarios were incorrect, reflecting expectations in which the toggle is perceived as an actual control, i.e., after clicking, the toggle would switch to the opposite direction and change the setting on the website from "Do Not Sell My Personal Information" to "Sell My Personal Information" or the other way around. Three scenarios were incorrect expectations related to other misconceptions, namely clicking the icon would cause the website to send unwanted emails, result in seeing ads about privacy or security products, or result in exposure to phishing or malware risks. For each scenario, we asked participants to indicate whether it is "definitely

W295-1 (cont.)

[2] The full set of survey questions for this study are included in Appendix A.

not," "probably not," "not sure," "probably," or "definitely" going to happen. As with our previous testing [1], participants were asked about their familiarity with CCPA and to provide their demographic information.



Close up of highlighted area:

What do you think would happen if you clicked on the symbol and link in the highlighted area on this web page?

W295-1 (cont.)

Figure 3: Screenshot of what participants assigned to the condition "stylized toggle in red" saw within the survey platform Qualtrics.

2.3 Participant Profile

We launched the study in mid-February 2020, recruiting 398[3] participants through Amazon Mechanical Turk. Participants were required to be residents of the United States over the age of 18 and have a 95% or higher approval rate on Mechanical Turk to be eligible to take the survey. As with our previous study populations, the demographic information we collected indicated that our sample was fairly diverse, but not U.S.-census representative. Our participants were evenly distributed between men and women, but skewed younger and more educated than the general U.S. population. Participants reported being residents of 44 different states plus Washington D.C., with 15.1% reporting residence in California. Our study population was also fairly tech savvy, with 27.9% reporting that they have an education in, or work in, the field of computer science, computer engineering or IT. 29 (7.3%) participants reported that they were aware of a law in the U.S. that required companies to provide a "do not sell" option, and 19 (4.8%) participants explicitly mentioned the CCPA or California when asked to name or describe the law.

2.4 Data Analysis

To categorize all open-ended responses provided by participants, we followed the same qualitative data analysis approach used in our previous studies [1].[4] To explore which toggle icon paired with the CCPA tagline conveyed the most correct expectations related to do-not-sell and the least misconceptions, we ran binomial regression models on the coded open-ended responses as well as on the quantitative data related to the eight expectation scenarios, after binning the five-point rating scale into a binary variable of expected (including "definitely" and "probably") versus unexpected (including "not sure," "probably not," and "definitely not"). Participants' age, gender, education and technical expertise were also included in the regression model as control variables.

W295-1 (cont.)

3. Results

Next, we discuss our findings. Based on these results we conclude that the *stylized toggle* effectively conveyed correct expectations related to do-not-sell and generated significantly fewer misconceptions compared to the *CalAG toggle* and the *CalAG-X toggle*. The switch between different toggle styles had a much bigger impact on participants' interpretations than whether the toggle was blue or red.

[3] We initially recruited 421 participants, but had to remove 23 responses from our analysis since these responses included nonsensical text to all open-ended questions in the survey. This is a common data cleaning practice.

[4] The codebook used for this study is included in Appendix B.

3.1 Open-ended Responses for Stylized Toggle More Frequently Mention Correct Expectations

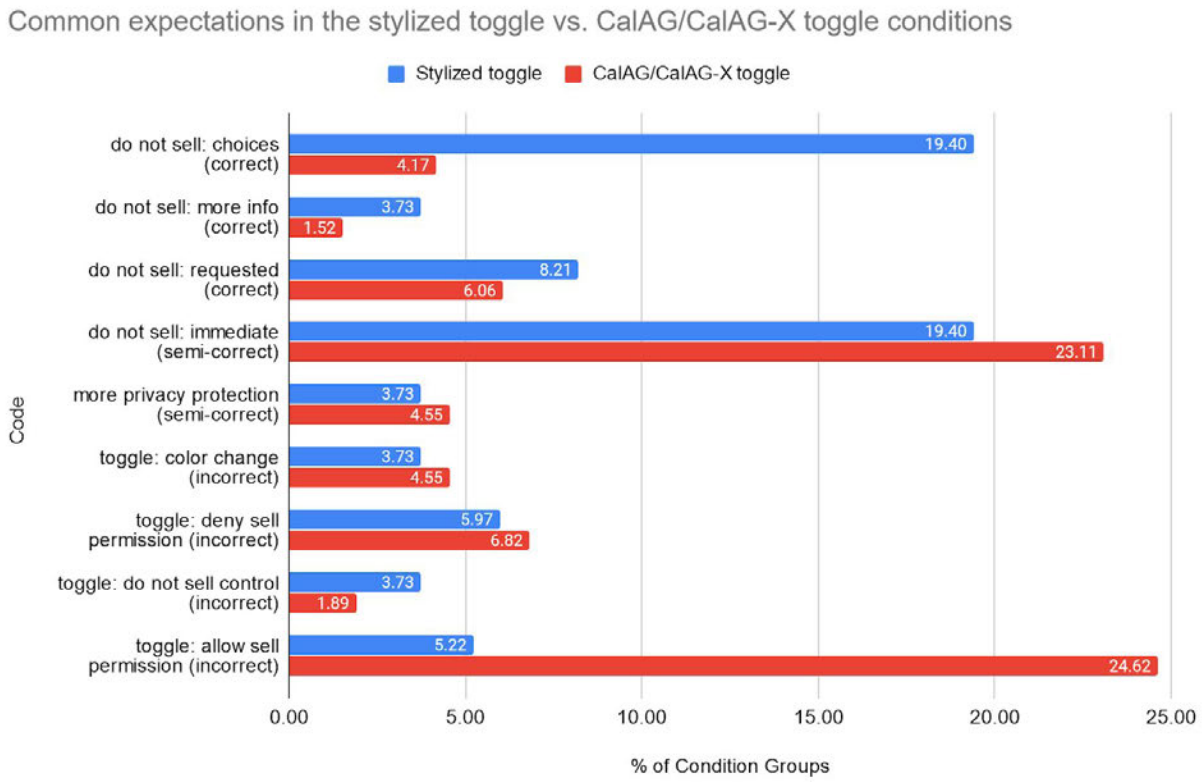


Figure 4: The proportion of participants in the two stylized toggle conditions (N=134) vs. in the four CalAG/CalAG-X toggle conditions (N=264) for common expectations after clicking the icon accompanied by "Do Not Sell My Personal Information," based on open-ended responses.

W295-1 (cont.)

We examined participants' open-ended responses to "what do you think would happen if you clicked on the symbol and link in the highlighted area on this web page?" **and observed different patterns between the *stylized toggle* conditions and the *CalAG/CalAG-X toggle* conditions** (see Figure 4). We discuss potential effects of color later on.

The most frequent expectation from participants who saw the *stylized toggle* (26, 19.40%) was that clicking the icon would lead them to a page where they could make choices related to the sale of personal information, which is the correct and desired interpretation of the icon. This correct expectation, however, was mentioned much less frequently in the CalAG/CalAG-X toggle conditions (11, 4.17%). In contrast, the **most frequent expectation from participants who saw the *CalAG/CalAG-X toggle* (65, 24.62%) was that the icon was an actual toggle**

switch that is currently set to "Do Not Sell My Personal Information" and that by clicking the icon they would allow permission to sell their personal information. The prevalence of this expectation is problematic and concerning, considering that people who have this notion might avoid clicking on the icon and/or the link text for fear of the loss of privacy, thus missing the chance of finding relevant information and choices related to do-not-sell available to them after clicking the icon. This misconception was only mentioned by 7 (5.22%) participants who saw the *stylized toggle*.

Relatedly, another erroneous expectation is that the website currently sells the user's personal information and the toggle, perceived as a functioning button, would deny the permission to continue doing so. This expectation was mentioned less frequently, by only 8 (5.97%) participants in the *stylized toggle* conditions and 18 (6.82%) participants in the *CalAG/CalAG-X toggle* conditions. This misconception is less problematic as it is less likely to cause people to avoid clicking on the icon and/or link text.

3.2 The Stylized Toggle Better Conveys the Concept of Do-Not-Sell

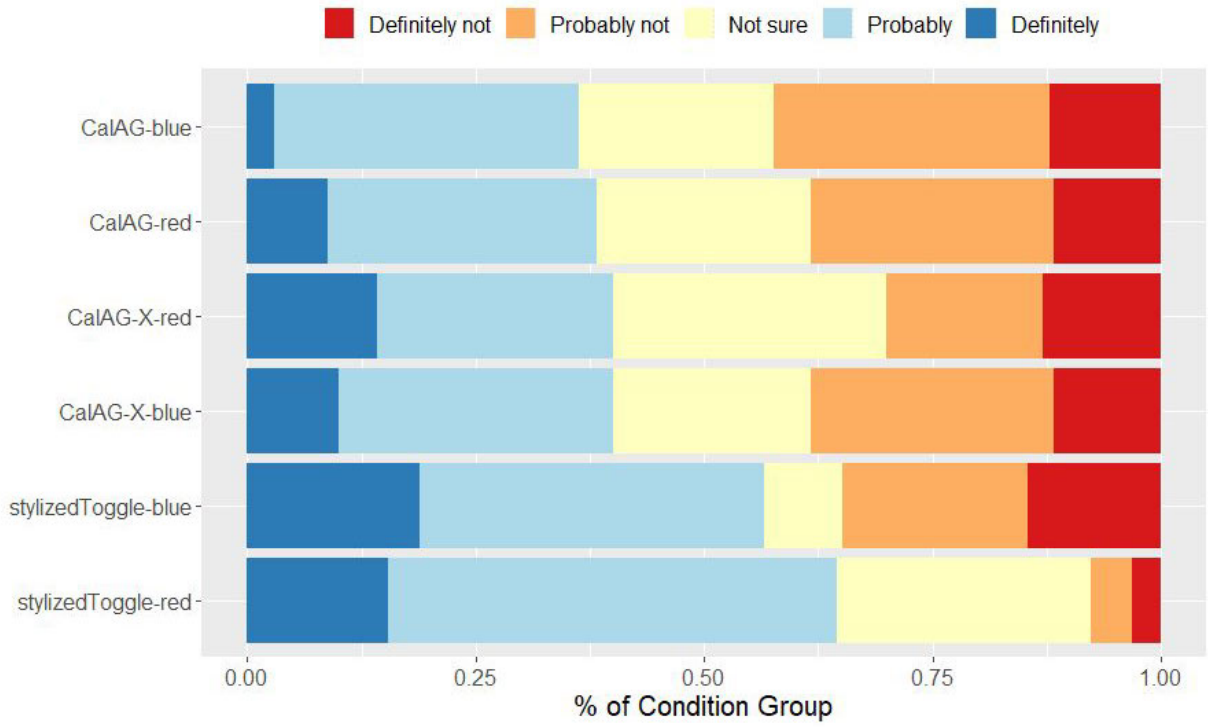


Figure 5: Distribution of participants' responses across conditions to the scenario "It [the symbol/link] will take me to a page where I can choose whether or not the website can sell my personal information."

W295-1 (cont.)

Our observation in Section 3.1 that *the stylized toggle* best conveyed the expectation of choices related to the sale of personal information was further corroborated by our analysis of multiple-choice question responses. As shown in Figure 5, when asked whether the symbol/link would take them to a page for opting out of the sale of personal information, the *stylized toggle* appeared in the top two conditions with the most positive responses ("definitely" and "probably"). **The *stylized toggle* significantly increased the odds of expecting choices related to do-not-sell on the landing page compared to the *CalAG toggle* (OR=2.89, p<0.001) and the *CalAG-X toggle* (OR=2.42, p=0.001)**. Looking at differences between the six conditions, our proposed icon design (*stylized toggle-blue*) conveyed the expectation of making do-not-sell related choices significantly better than the *CalAG toggle* in both colors (OR=2.42, p=0.02 for blue; OR=2.48, p=0.02 for red).

A similar distribution of responses emerged for the scenario of expecting to confirm a do-not-sell request on the landing page that appears after clicking the icon ("It will take me to a page where I can confirm that I do not want my personal information to be sold by the website"), with the two *stylized toggle* conditions having the highest percentage of positive responses. Similarly, **the *stylized toggle* significantly increased the odds of expecting a do-not-sell request confirmation on the landing page compared to the *CalAG toggle* (OR=2.24, p=0.004) and the *CalAG-X toggle* (OR=1.86, p=0.03)**. Our proposed design performed significantly better than the *CalAG toggle* in red (OR=3.88, p<0.001) and the *CalAG toggle* in blue (OR=2.45, p=0.02) in conveying this expectation.

For the scenario of expecting more information about the company's practices related to do-not-sell ("It will take me to a page with more information about how the website uses and shares my personal information"), the two *stylized toggle* conditions still had the highest percentage of expected responses, but the advantage over other conditions was no longer substantial. Neither toggle style, color, nor their combination made a significant impact on the expected/unexpected responses to this scenario.

W295-1 (cont.)

Furthermore, our analysis on the coded open-ended responses shows that **the *stylized toggle* was more effective than the *CalAG/CalAG-X toggle* at conveying the concept of do-not-sell accurately, without creating the impression that the toggle is an actual privacy control switch**. We created a binary variable to denote whether the response was a correct expectation specifically related to do-not-sell, namely when it mentioned choices or more information related to the sale of personal information, making a do-not-sell request (sometimes with doubts of its effectiveness), confirming a do-not-sell request, or the website immediately stopping the sale of the user's data. We then ran a regression model on this binary variable. **The *stylized toggle* significantly increased the odds of conveying the do-not-sell concept accurately compared to the *CalAG toggle* (OR=2.21, p=0.004) and the *CalAG-X toggle* (OR=2.23, p=0.004)**. Looking at differences between the six conditions, our proposed design significantly increased the odds of conveying the do-not-sell concept accurately compared to the CalAG's proposed design *CalAG toggle-red*, OR=2.32, p=0.03.

3.3 The Stylized Toggle Caused Fewer Misconceptions

We binned participants' open-ended responses regarding their expectations of what would happen if they clicked on the icon into two categories, correct and incorrect, where incorrect means the responses exhibited misconceptions. Examples of misconceptions range from perceiving the toggle icon as an actual switch, to negative scenarios (e.g., triggering unwanted emails, introducing phishing/malware risks, seeing ads of privacy products, and less privacy protection) and the expectation that nothing would happen. We ran a regression model on the correct/incorrect variable. **Both the *CalAG toggle* and the *CalAG-X toggle* significantly increased the odds of misconceptions compared to the *stylized toggle*** (OR=2.78, p<0.001; OR=2.63, p=0.001). In addition, the red *CalAG-X toggle*, the blue *CalAG toggle,* and the red *CalAG toggle* all significantly increased the odds of misconceptions compared to the *stylized toggle* (OR=3.00, p=0.006; OR=2.34, p=0.04; OR=2.37, p=0.04).

We then took a closer look at responses that mentioned the toggle being an actual button. Specifically, we code open-ended responses as toggle-specific misconceptions if they mentioned clicking would result in the toggle changing color or position, the toggle being a control for do-not-sell settings (e.g., "How I opt in/out or it would change between red and green depending on if I wanted to allow it."), or specified the direction of change as from "Do Not Sell My Personal Information" to "Sell My Personal Information" or the other way around. Our regression model on this binary variable shows that **both the *CalAG toggle* and the *CalAG-X toggle* significantly increased the odds of toggle-specific misconceptions compared to the *stylized toggle*** (OR=2.98, p<0.001; OR=2.45, p=0.004). Looking at individual conditions, the *CalAG toggle* in blue or red, and the *CalAG-X toggle* in red all significantly increased the odds of toggle-specific misconceptions compared to our stylized toggle design (OR=3.02, p=0.01; OR=3.17, p=0.008; OR=3.83, p=0.002).

W295-1 (cont.)

The analysis of likert responses results in the same overall conclusion that the *stylized toggle* conveyed fewer toggle-specific misconceptions, but the differences were less pronounced. As shown in Figure 6, for the expectation that clicking would immediately grant permission to sell personal information, i.e., the icon is perceived to be an actual toggle switch, the *CalAG toggle* exhibited significantly higher odds compared to the *stylized toggle* (OR=1.79, p=0.04), but the difference between the stylized toggle and the *CalAG-X toggle* was not significant. No significant differences were found between individual conditions for this scenario either.

For the expectation that clicking would deny permission to sell personal information, no significant impact was found from the use of different styles or colors. However, as shown in Figure 7, there were interaction effects between the style and color: compared to our blue *stylized toggle* design, the *stylized toggle* in red, the *CalAG-X toggle* in blue, and the *CalAG toggle* in blue all significantly increased the odds of the toggle being perceived as an actual toggle switch that, after clicking, denies the permission to sell consumer data (OR=2.92, p=0.006; OR=2.89, p=0.008; OR=2.18, p=0.04).

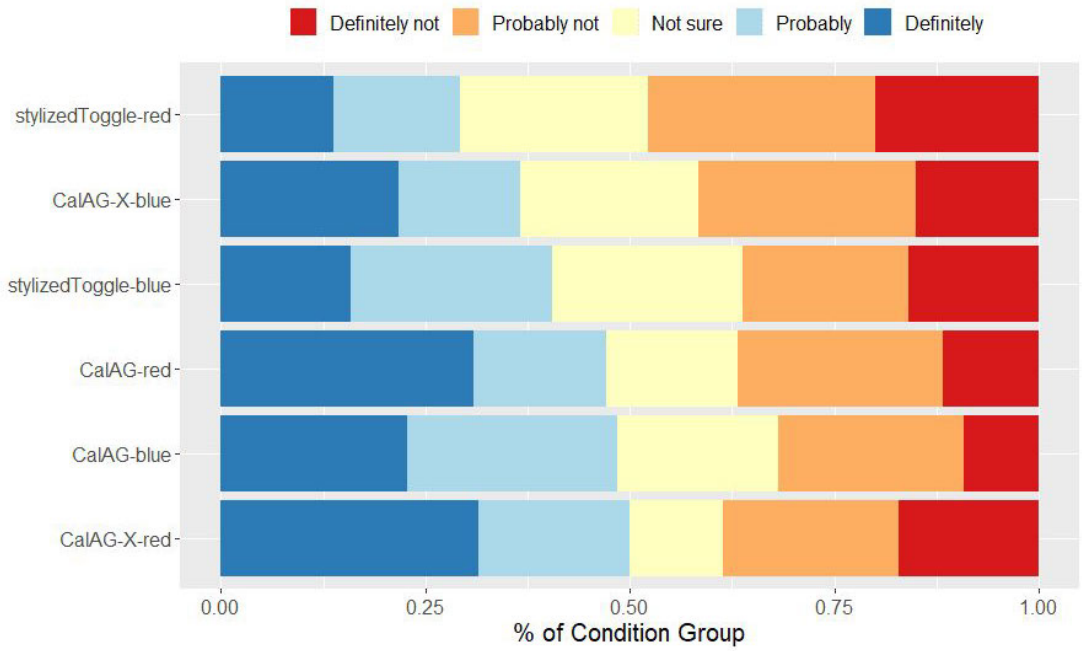


Figure 6: Distribution of participants' responses across conditions to the scenario "It [the symbol/link] will immediately change the setting on this website from "Do Not Sell My Personal Information" to "Sell My Personal Information."

W295-1 (cont.)

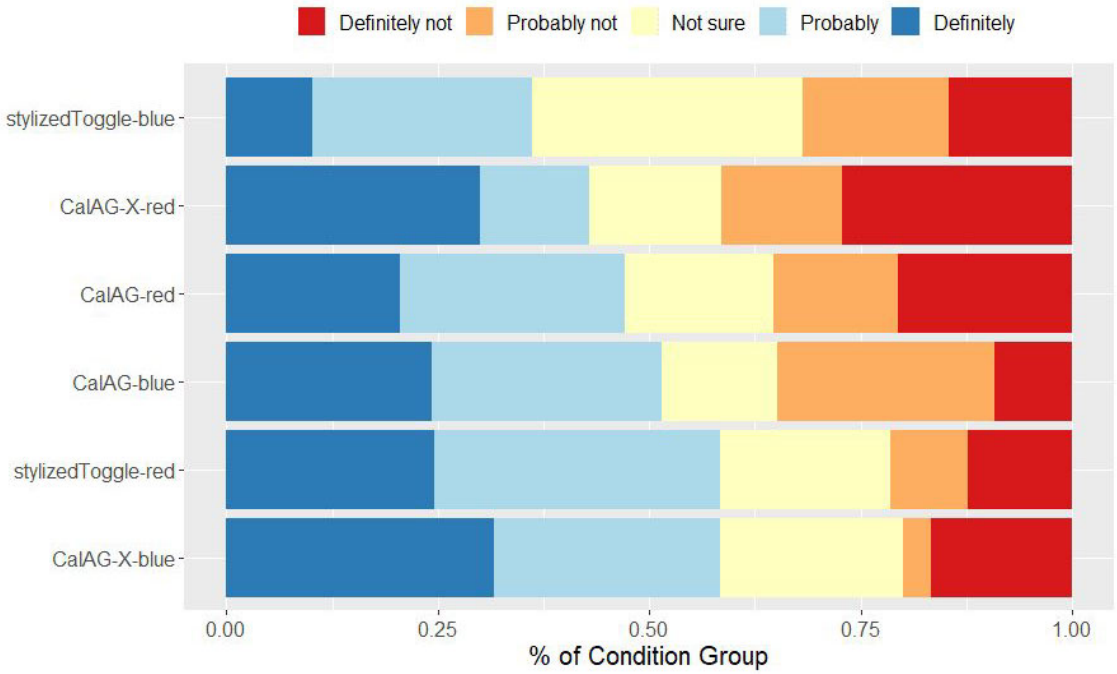


Figure 7: Distribution of participants' responses across conditions to the scenario "It [the symbol/link] will immediately change the setting on this website from "Sell My Personal Information" to "Do Not Sell My Personal Information."

3.4 Blue Color for Stylized Toggle Reduces Misconceptions

Based on the analysis above, we reach the conclusion that the *stylized toggle* is preferable to the *CalAG/CalAG-X toggle*, as the stylized toggle more effectively conveyed the concept of do-not-sell and generated fewer misconceptions. However, whether the icon is blue or red does not appear to have a significant impact on the dependent variable in any of the regression models we ran.

The only significant difference we found between the red and blue *stylized toggle* in the tests discussed above is that the ***stylized toggle* in red significantly increased the odds of the toggle being perceived as an actual toggle switch that, after clicking, denies the permission to sell consumer data**, as shown in Figure 7.

To further understand the impact of color on the interpretation of the *stylized toggle*, we ran pairwise chi-square tests between the red and blue variants of this icon on likert-scale responses to the eight scenarios, as well as coded open-ended responses regarding expectations. To discern potential subtle differences we used all five points of the scale instead of binning into the expected/unexpected categories. We found that the ***stylized toggle* in red performed significantly better than the blue version in suggesting do-not-sell choices on the landing page** (p=0.004, Cramer's V=0.36). No significant differences between the red and blue *stylized toggles* were found in any of the other seven tests.

W295-1 (cont.)

We conclude that there are tradeoffs to be made when deciding whether to present the *stylized toggle* icon in blue or red. While red is indeed more effective at conveying the presence of choices related to do-not-sell, it also increases the odds of the toggle being perceived as an actual control toggle switch that, after clicking, would change the setting of the website to "Do Not Sell My Personal Information." This is probably because participants interpreted red as an indication that the setting "Do Not Sell My Personal Information" is currently turned off. **To reduce the potential for misinterpreting the toggle as conveying the user's current opt-out setting we recommend presenting the icon in blue.**

References

1. L.F. Cranor, H. Habib, Y. zou, A. Acquisti, J. Reidenberg, N. Sadeh, F. Schaub. Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA. February 4, 2020. https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-cranor.pdf

2. Revised Proposed Regulations, modified February 10, 2020. Office of the California Attorney General. https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf

Appendix A: Survey Questions

Open-ended Expectations

Please answer the following questions with regards to the symbol and link in the rectangular highlighted area near the bottom of the web page displayed. Make sure not to reveal any private or personally identifiable information about yourself or others in your responses to any open-ended questions.

[Display the screenshot of the web page that participants were randomly assigned to]

Close up of highlighted area:

[Display the highlighted area]

1. What do you think would happen if you clicked on the symbol and link in the highlighted area on this web page? *[Open-ended response.]*

Tagline Elements

2. What do you think “sell” refers to in this link? *[Open-ended response]*

3. What do you think “information” refers to in this link? *[Open-ended response]*

Scenario Expectations

[Display the highlighted area]

4. Which of the following do you think could happen if you clicked this symbol and link on a web page? *[For each statement below, participants were asked to choose from a 5-point likert scale “Definitely” “Probably” “Not sure” “Probably not” and “Definitely not.” Statements were presented in randomized order.]*

- It will immediately change the setting on this website from "Do Not Sell My Personal Information" to "Sell My Personal Information."
- It will immediately change the setting on this website from "Sell My Personal Information" to "Do Not Sell My Personal Information."
- It will take me to a page where I can choose whether or not the website can sell my personal information.

- It will take me to a page where I can confirm that I do not want my personal information to be sold by the website.
- It will take me to a page with more information about how the website uses and shares my personal information.
- It will cause the website to send me unwanted emails.
- It will take me to a page with ads about privacy and security products.
- It will take me to a page that steals my information or has a virus or malware.

Demographics and Background

5. Are you aware of any laws in the United States that require companies to provide a “do not sell my personal information” option?
- No
- Yes (please name or describe them): ___

6. What is your age?
- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65-74
- 75-84
- 85 or older
- Prefer not to answer

7. What is your gender?
- Female
- Male
- Non-binary
- Prefer to self-describe: ___
- Prefer not to answer

8. What is the highest level of education you have completed?
- Less than high school
- High school degree or equivalent
- Some college, no degree
- Associate’s degree, occupational
- Associate’s degree, academic
- Bachelor’s degree
- Master’s degree
- Professional degree
- Doctoral degree
- Prefer not to answer

9. What was your total household income before taxes during the past 12 months?
   - Under $15,000
   - $15,000 to $24,999
   - $25,000 to $34,999
   - $35,000 to $49,999
   - $50,000 to $74,999
   - $75,000 to $99,999
   - $100,000 to $149,999
   - $150,000 or above
   - Prefer not to answer

10. In which state do you currently reside? *[Open-ended response]*

11. Which of the following best describes your educational background or job field?
   - I have an education in, or work in, the field of computer science, computer engineering or IT.
   - I do not have an education in, or work in, the field of computer science, computer engineering or IT.
   - Prefer not to answer

12. Which of the following best describes your primary occupation?
   - Administrative Support (e.g., secretary, assistant)
   - Art, Writing, or Journalism (e.g., author, reporter, sculptor)
   - Business, Management, or Financial (e.g., manager, accountant, banker)
   - Education or Science (e.g., teacher, professor, scientist)
   - Legal (e.g., lawyer, paralegal)
   - Medical (e.g., doctor, nurse, dentist)
   - Computer Engineering or IT Professional (e.g., programmer, IT consultant)
   - Engineer in other field (e.g., civil or bio engineer)
   - Service (e.g., retail clark, server)
   - Skilled Labor (e.g., electrician, plumber, carpenter)
   - Unemployed
   - Retired
   - College student
   - Graduate student
   - Mechanical Turk worker
   - Other: ___
   - Prefer not to answer

13. If you have any feedback on the survey, please leave it here. *[Open-ended response]*

Appendix B: Codebook

Open-ended expectations (for responses to “Which of the following do you think could happen if you clicked this symbol and link on a web page?”)

Code	Definition	Example
choices: opt out	Either generic opt out of "something" or opt out of things other than do not sell, such as data collection or email subscription list.	"I would probably go to one of those forms that lists all the information-gathering the site makes, and which ones I can opt out of."
do not sell: choices	Specific mentioning that consumers will have the option to choose whether or what types of data can or cannot be sold to third-parties by the site.	"It would give you the option to not have your personal information given, shared, or sold to someone else."
do not sell: confirmation	The link will lead to a page that double checks whether or not the participant wants their information not to be sold to others.	"You would be taken to a page to confirm you wish your personal information not to be shared."
do not sell: doubted	The user expects that the website will not sell their personal information but meanwhile expresses reservation that the site might not follow this rule.	"I would hope that it would mean the company wouldn't sell my personal information. Not sure if that would actually happen or not."
do not sell: immediate	The user assumes that the company will not sell their personal data.	"My data will not be sold."
do not sell: more info	The link leads to more info on how to make use of the "do not sell" choice or how the company does not sell consumer information to third parties.	"It would tell me how to choose not to share my information."
do not sell: requested	The link will take the user to a page where they can require the company to not sell their personal data, but they do not explicitly expect the request to be honored.	"I will be shown a page that allows me to opt out of allowing companies to sell my private information, similar to opting out of junk mail."
less privacy protection	The participant indicates that clicking the icon/link would lead to less privacy protection or another negative outcome but doesn't specify that it's because their data would now be sold.	"Your personal information will be available and spread on the internet."

more info: collected data	The link will lead to more info on what types of data (or specific data) the site has collected about the user.	"It would pull up information that the company has collected about me, possibly my demographics and what they think my shoe preferences are based on what pages I've spent time looking at."
more info: data practices	The link will lead to more info on how the site collects, uses, and shares user data, a more granular description of privacy policy.	"A page where you understand how your info will be used."
more info: generic	The general feeling that they would see more information.	"It would take me to a page with more info."
more info: products/services	The link will lead to info on the products and services sold on this website, including promotions and discounts.	"I think it would lead me to a page with more information about how to purchase these shoes."
more privacy protection	The user will enjoy a higher level of privacy protection that does not relate to do not sell, such as less tracking and use of cookies, removing existing collected data, or providing an incognito version of the site.	"It could provide privacy for me."
new page	The link will direct the user to a new page/site, open a new tab/window, without giving any further context of what's included in the page.	"It opens a web page."
not sure	The user is not sure what to expect.	"I don't know."
nothing	The user expects nothing would happen if they clicked, or is skeptical that there's actually a privacy choice present, or complains that the "toggle" is not working	"Nothing really, They would still track me."
personalization	The site will ask for more information that creates a better personalization experience or for targeted ads, e.g., recommending more relevant shoes.	"I assume it takes you to a page where you can supply personal information that will influence what the site shows you, perhaps sending you emails regarding products you might be interested in based on the information you've provided."

privacy choices: data processing	The user expects to see choices related to how the company uses collected data. However, if the response mentions choices related to how the company *share* data with others we assume the sharing involves transactions, hence code it as "do not sell: choices."	"I think a drop-down menu will open and you can choose how your private information is handled if you are using the website."
privacy choices: generic	The user expects to be led to general privacy/cookie settings.	"You should be able to set your privacy options, meaning, how your info is used, how you are contacted."
privacy policy	The link leads to a privacy policy. We use this code when participants mention the word "privacy policy" explicitly.	"I would be taken to another page full of text with their privacy policy that i most likely won't read or understand if i did read it."
spamming	The link leads to settings that would bring the user annoying messages such as unwanted emails.	"Your IP address and information would go to other sources and then you would receive a bunch of emails from other sources."
toggle: color change	The user expects the color or the motion of the icon to change, but does not specify anything else related to the configuration of do-not-sell.	"It would turn green."
toggle: do not sell control	The user expects that the toggle is a control for whether or not they want their personal data to be sold, but did not specify the direction as sell —> not sell or not sell —> sell.	"I would toggle back and forth from ‘do not sell’ to ‘it's okay to sell.’"
toggle: deny sell permission	The user expects clicking will toggle the setting such that the website won't be able to sell your data.	"I think it would activate the button and let the business know that I didn't want to share my personal information."
toggle: allow sell permission	The user expects clicking will toggle the setting such that the website can now sell your data.	"Right now it is clicked ‘off’ so if you click it ‘on’ they will be free to sell your personal information."

Mapping of Expectation Codes for Regressions

Code	Conveys the ability to opt-out of selling personal info (yes/no)	Conveys misconceptions (yes/no)	Conveys icon as an actual toggle switch (yes/no)
choices: opt out	no	no	no
do not sell: choices	yes	no	no
do not sell: confirmation	yes	no	no
do not sell: doubted	yes	no	no
do not sell: immediate	yes	no	no
do not sell: more info	yes	no	no
do not sell: requested	yes	no	no
less privacy protection	no	yes	no
more info: collected data	no	no	no
more info: data practices	no	no	no
more info: generic	no	no	no
more info: products/services	no	yes	no
more privacy protection	no	no	no
new page	no	no	no
not sure	no	no	no
nothing	no	yes	no
personalization	no	yes	no
privacy choices: data processing	no	no	no
privacy choices: generic	no	no	no
privacy policy	no	no	no
spamming	no	yes	no
toggle: color change	no	yes	yes
toggle: do not sell control	yes	yes	yes
toggle: deny sell permission	yes	yes	yes
toggle: allow sell permission	yes	yes	yes

From: Lydia De La Torre
To: Privacy Regulations
Subject: Comments to CCPA Proposed Rules
Date: Saturday, February 22, 2020 12:43:58 PM
Attachments: CCPA Comments to Rules.pdf

Please find attached my comments to the proposed rules.

Kind regards,

Lydia F. de la Torre
Adjunct Professor
Santa Clara Law School
Data Protection Law Blog: Golden Data
Twitter: @dltsays

Lydia F. de la Torre
500 El Camino Real
Santa Clara, CA
[redacted]

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

February 22, 2020

Comments regarding proposed changes to § 999.315 (c) (Requests to Opt-Out) of the California Consumer Privacy Act (CCPA) regulations

Although I am an attorney and I have worked in data privacy most of my career, I am filing these comments as a consumer and as a California resident.

The comments relate to the addition of the following language to § 999.315 (c) (Requests to Opt-Out)

> *"(1) Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to the opt-out of the sale of personal information.* ***The privacy control shall require that the consumer affirmatively select their choice to opt-out and shall not be designed with any pre-selected settings. "***

W296-1

The requirement for a consumer to *"affirmatively select their choice to opt-out"* and for controls to *"not be designed with any pre-selected settings"* disregards the fact that choosing a specific product or brand can itself be an affirmative choice to select privacy protective features.

I personally choose to use products that include default and pre-selected privacy features precisely because they are designed with privacy in mind. For example, I use a browser and a search engine that limit online tracking and a mobile operating system developed by an organization that brands itself as privacy protective. Many other consumers do as well. We should not be expected to take additional steps to ensure our desire for privacy is respected, nor should our preferences be negated on the theory that we choose the product without awareness of the fact that it included privacy protective defaults.

In addition, the proposed language undermines the principles of Privacy by Design (PbD) (as expressed in the seven 'foundational principles' developed by the Information and Privacy Commissioner of Ontario in 2013[1]) and arguably goes against prior guidelines provided by the California Attorney General Office[2] and the Federal Trade Commission[3].

W296-1 (cont.)

Therefore, I respectfully request that the last sentence of § 999.315 (c) (1) *("The privacy control shall require that the consumer affirmatively select their choice to opt-out and shall not be designed with any pre-selected settings.")* be eliminated in the final version of the rules.

Thank you for your consideration of my request,

Lydia F. de la Torre

[1] See, Operationalizing privacy by design: a guide to implementing strong privacy practices (Dec. 2012) a paper by Ann Cavoukian at https://collections.ola.org/mon/2012/320221.pdf

[2] See, for example, Privacy on the Go: Recommendations for the Mobile Ecosystem (CA AG, Jan 2013)

[3] See, for example, Mobile Privacy Disclosures FTC Staff Report | February 2013 # Building Trust Through Transparency (FTC Staff Report, Feb. 2013)

KIMBERLYN R. HEARNS
[redacted]

LISA B. KIM, PRIVACY REGULATIONS COORDINATOR
CALIFORNIA OFFICE OF THE ATTORNEY GENERAL
300 SOUTH SPRING STREET, FIRST FLOOR
LOS ANGELES, CALIFORNIA 90013

FEBRUARY 17, 2020

RE: OAL FILE No. 2019-1001-05
"PROPOSED CHANGES ... TO THE RULEMAKING FILE"

DEAR MS. KIM,

I'm MAKING THE FOLLOWING PROPOSALS

UNDER ARTICLE 3 "... HANDLING CONSUMER REQUESTS"
999.312(a) A BUSINESS THAT OPERATES EXCLUSIVELY ONLINE AND HAS A DIRECT RELATIONSHIP WITH A CONSUMER FROM WHOM IT COLLECTS PERSONAL INFORMATION SHALL PROVIDE AN EMAIL ADDRESS AND A PHYSICAL MAILING ADDRESS FOR SUBMITTING REQUESTS TO KNOW AND SERVICE OF CIVIL PROCESS.

W297-1

999.312(c) ADD:
"... A BUSINESS SHALL NOT LIMIT A CONSUMER'S OPTIONS TO A TABLET OR COMPUTER PORTAL THAT ALLOWS THE CONSUMER TO COMPLETE AND SUBMIT AN ONLINE FORM NOR THE BUSINESS'S TOLL-FREE NUMBER NOR EMAIL ADDRESS"

W297-2

(COVER)

999.313 (c)(1) INSERT:

"... IF A CONSUMER REQUESTS A MAILED QUESTIONNAIRE IN LIEU OF A PHONE INTERVIEW OR EMAIL QUESTIONNAIRE, THE BUSINESS MUST COMPLY WITHIN 10 BUSINESS DAYS OF NOTIFICATION..."

W297-3

999.313 (11)(d)(2)a AND 999.313 (11)(d)(3) REVAMP:

HOW IS A CONSUMER'S INFORMATION AND DATA PERMANENTLY AND COMPLETELY ERASED ON A BUSINESS' EXISTING SYSTEMS IF THERE ARE EXCEPTIONS FOR ARCHIVED OR BACK-UP SYSTEMS? IT'S A LOOPHOLE AND SUBJECT TO RAMPANT EXPLOITATION.

W297-4

SECTION (11)(d)(3) SHOULD BE STRUCK IN ITS ENTIRETY.
SECTION (11)(d)(2)a CHANGE TO:

"PERMANENTLY AND COMPLETELY ERASING THE PERSONAL INFORMATION ON ALL SYSTEMS."

999.315(b): CHANGE AND ADD

W297-5

SEE MY PRIOR RECOMMENDATIONS FOR 999.312(c) AND ADD THAT LANGUAGE.

999.317 (g): CHANGE TO:

"... THE PERSONAL INFORMATION OF 3,000,000 OR MORE CONSUMERS IN A CALENDAR YEAR, FISCAL YEAR, AND/OR BUDGET YEAR..."

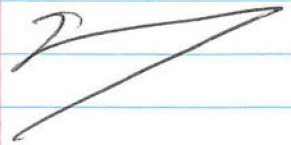
W297-6

BUMPING THE NUMBER UP TO 10,000,000 EVISCERATES THE RULE AND WOULD APPLY ONLY TO THE LARGEST FIRMS. A PRIVACY RULE AND LAW NEEDS TEETH

FURTHERMORE, IF THE RULE IS ALLOWED TO REMAIN AT 10,000,000 CUSTOMERS AND/OR CONSUMERS IT WOULD VIRTUALLY EXEMPT ALL BIOMETRIC FIRMS, ATTRIBUTION FIRMS, DATA ANALYTICS FIRMS; FACIAL IMAGING, RECOGNITION AND IMAGE MATCHING FIRMS AND INSURERS. WHOLE INDUSTRIES WOULD BE EXEMPTED! MORE BUSINESSES THAT SPECIALIZE IN INTELLIGENCE GATHERING, COVERT OPERATIONS, DATA HARVESTING, AND UNTRACEABLE EQUIPMENT INTERFERENCE (i.e "HACKING AND CRACKING") WOULD ALSO BE LEGALLY EXEMPT. A SEPARATE SET OF RULES ARE NEEDED FOR THIS GROUP - TO INCLUDE LICENSING AND PROPRIETARY METHODS. W297-6 (cont.)

THANK YOU FOR YOUR TIME AND CONSIDERATION IN THIS MATTER.

SINCERELY,



From: [redacted]
Sent: Monday, February 17, 2020 8:06 AM
To: Privacy Regulations
Subject: "Household" in the Definition of Personal Information in the CCPA

Categories: Written Comment

Ph.D., D.Sc., dr. hab., att. Mariusz Krzysztofek

Privacy Regulations Coordinator
Office of the Attorney General
State of California Department of Justice

Dear Coordinator,

Let me submit the attached comments for the proposed adoption of Section § 999.301(k) and for Section 1798.140 (o)(1) of the California Consumer Privacy Act (CCPA).

Sincerely
Mariusz Krzysztofek

Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the policy or position of any company or institution.

W298-1

"Household" as people who reside at the same address

In October of 2019, the Attorney General's office issued draft regulations which defined "household" as a "person or group of people occupying a single dwelling" (this definition is similar to the one proposed by the United States Census Bureau, https://urldefense.proofpoint.com/v2/url?u=https-3A__www.census.gov_programs-2Dsurveys_cps_technical-2Ddocumentation_subject-2Ddefinitions.html&d=DwIDaQ&c=uASjV29gZuJt5_5J5CPRuQ&r=kXcUIWCJFJC3Y7A6WPl5oNx0wEUzL_7MxjOspe9bxxI&m=qaaZFX48DsJo0hmPTNwNA_44M3FKo8bmU2wVHM_ezi0&s=RTriw-kBHLKSZrkXk7x7bl5cmeT4OPid0NpejGQHcAc&e=).
On February 7, the Attorney General's office issued a second, revised draft of the CCPA which defined "household" as a "person or a group of people" not - as before – only "occupying a single dwelling", but still
"who: (1) reside at the same address, but also (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier."
The scope of the concept of "household" has therefore been limited compared to the previous one. A family or even students who for example set up four profiles to share a single TV account, and who also reside at the same address, constitute a household.

HOWEVER, THIS DEFINITION DOES NOT INDICATE HOW AN INDIVIDUAL WITHIN A HOUSEHOLD DIFFERS FROM A CONSUMER IN THE DEFINITION OF PERSONAL INFORMATION. SINCE EVEN A PERSON LIVING ALONE IN A HOUSING UNIT IS COUNTED AS A HOUSEHOLD, HOW DOES THIS INDIVIDUAL DIFFER FROM THAT HOUSEHOLD IN THE CONTEXT OF THE DEFINITION OF PERSONAL INFORMATION? Some personal information clearly identifies both directly consumer and household, e.g. a postal address. W298-1 (cont.)
In other words, people who constitute a household are in the same time consumers as defined in the CCPA (California residents). Therefore the above definition of household as defined by the Attorney General's office (and the United States Census Bureau), although official and common sense, since households anyway are made up of consumers, which means California residents, does not bring any additional explanation to the interpretation of the scope of the definition of personal data in the CCPA.
Therefore, one may consider whether adding "household" as a data subject alongside "consumer" increases the level of protection of personal information if, in any case, the Attorney General's guidance § 999.318(b) indicate „all consumers of the household".

Consumer (data subject) rights

In October of 2019, the Attorney General's office issued draft regulations which provided guidance (§ 999.318) for how to fulfill requests to access or delete "household information." However, the regulations do not indicate how the definition of household is to be applied to other areas of the law (e.g. notice or data breach provisions, like how a household whose personal information is subject to a breach, such as unauthorized access and exfiltration, or disclosure W298-2 as a result of the business's violation of the duty to implement and maintain reasonable security procedures, may be notified of noncompliance by a business). Furthermore, the guidance § 999.318 do not indicate e.g. how to distinguish whether a request relates to household or consumer information when this information is e.g. postal address which applies to both. For example, can one consumer of the household request for the deletion of his or her personal information which is also the household personal information of other consumers?

Conclusion

Since even a person living alone in a housing unit is counted as a household, it is not indicated how an individual within a household differs from a consumer in the definition of personal information. In other words, people who constitute a household are in the same time consumers as defined in the CCPA (California residents), so "household" in the CCPA duplicates the meaning of "consumer" in the definition of personal information. W298-1 (cont.)
The definitions of "personal information" enshrined in the CCPA and in the GDPR, as well as in data protection laws adopted in some other countries, such as Argentina, Canada, Israel, Japan, New Zealand, Switzerland, Uruguay, South Korea, Brazil, Ghana, Singapore, United Arab Emirates, and South Africa, are largely convergent. HOWEVER, THE DEFINITION IN THE CCPA DIFFERS FROM THE GDPR AND ABOVE PRIVACY LAWS AS IN THE CCPA IDENTIFIABLE INFORMATION CONCERNS NOT ONLY INDIVIDUALS BUT ALSO "HOUSEHOLDS". SO, I DO NOT THINK THAT REMOVING "HOUSEHOLD" AND LEAVING ONLY "CONSUMER" WOULD REDUCE THE LEVEL OF PROTECTION OF PERSONAL INFORMATION.

I THINK BOTH GUIDANCE OF THE CCPA ISSUED BY THE ATTORNEY GENERAL'S OFFICE ACTUALLY SHOW THAT AT THE END OF THE DAY, THE HOUSEHOLD NEEDS TO BE TIED TO A CONSUMER IN ORDER TO VALIDATE THE REQUEST, FOR EXAMPLE IN THE GUIDANCE § 999.318 IT IS EXPLICITLY SAID „ALL CONSUMERS OF THE HOUSEHOLD".

THEREFORE, IN MY OPINION AN INTERPRETATION WORTHY OF RECOMMENDATION MAY BE THAT THE PHRASE "HOUSEHOLD" COULD BE DELETED IN FUTURE AMENDMENTS.

About the Author

Mariusz Krzysztofek, Ph.D., D.Sc., dr. hab., att., Professor of Law,

Director, DPO, Privacy Counsel at a global nutrition company based in Los Angeles. Authored six books and dozens of articles on personal data protection. His recent book is: “GDPR: General Data Protection Regulation (EU) 2016/679: Post Reform Personal Data Protection in the European Union”, Kluwer Law International BV, 2019. He has been an expert for the Ministry of Justice and the Ministry of Digital Affairs of Poland, and on business TV channels. He is a member of the program council of the quarterly ‘Information in Public Administration’, C.H.Beck.
A professor within a postgraduate study at SGH Warsaw School of Economics, honored as "Exemplary Lecturer of 2011, 2012, 2013, 2014, 2016, 2018 and of 20 years of the Warsaw Institute of Banking, awarded a medal for educational activity for banks by the Polish Bank Association (2008). A scholar at Georgetown University and University of Wisconsin – La Crosse, 1998.

LinkedIn:
https://urldefense.proofpoint.com/v2/url?u=https-3A__www.linkedin.com_in_ph-2Dd-2Ddr-2Dhab-2Dmariusz-2Dkrzysztofek-2D309b05a_&d=DwIDaQ&c=uASjV29gZuJt5_5J5CPRuQ&r=kXcUIWCJFJC3Y7A6WPl5oNx0wEUzL_7MxjOspe9bxxI&m=qaaZFX48DsJo0hmPTNwNA_44M3FKo8bmU2wVHM_ezi0&s=scRWM80OnfbB8WvgUXcMeoMXRLr5VZBC3EPzyFelcZw&e=

From: MISTRAL Jean Pierre
To: Privacy Regulations
Subject: Comments
Date: Friday, February 14, 2020 6:05:37 AM

UPDATED NOTICE OF MODIFICATIONS TO TEXT OF PROPOSED REGULATIONS

Changes are highlighted in yellow for proposed additions:

1- § 999.302. Guidance Regarding the Interpretation of CCPA Definitions (a) Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "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." For example, if a business or its service provider collects the IP addresses of visitors to its website but does not intentionally link the IP address to any particular consumer or household, and could not on its own or via its service provider reasonably link the IP address with a particular consumer or household, then the IP address would not be "personal information." W299-1

2- Updated Regulations § 999.314(c)(3)

For internal use by the service provider to build or improve on its own or through a third party the quality of its own services (for instance through the use of artificial intelligence and machine learning), provided that the use does not include building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source. W299-2

Thanks for considering these proposed additions.

Best regards,

Jean-Pierre MISTRAL
Director Data Privacy
Phone# [redacted]
Fax# +1 512 257 3881
Cell# [redacted]
Gemalto, Inc., Arboretum Plaza II 9442 Capital
of Texas Hwy North Suite 100 Austin, TX (USA) 78759

From: zzc735735
To: Privacy Regulations; [redacted]
Subject: California Consumer Privacy Act
Date: Thursday, February 13, 2020 3:39:18 PM

Sent via email: Lisa B. Kim, Privacy Regulations Coordinator California Office of the Attorney General

Dear Attorney General Becerra,

I am submitting this comment to the Department of Justice, Privacy Regulations Coordinator, for review of the California Consumer Privacy Act (CCPA) to add protection to senior, disabled and consumers that do not have online internet access (email) to comply with existing CCPA policy. As discussed below, these are serious concerns for this large community throughout California.

A large California organization recently published, for their members, the steps to "***Manage Your Privacy Rights***" under the CCPA. Unfortunately, this organization requires member(s) to have an internet email account in order to avail themselves of this important privacy management process. When told that an email account does not exist, the company indicated that the "CCPA law requires an email" address. Although, no email account is required to join for membership in this organization, it appears that in order to manage privacy policy at this organization does, in fact, require an email address for its members. W300-1

The organization mentioned above is the **Auto Club of Southern California (AAA)**. In the recent member magazine called *Westways* (California), the CCPA policy is noted and takes up a full page with information on how a member can manage their privacy. While most of the instructions are online accessed, they do include a telephone number that a member can call for help in managing their privacy.

Unfortunately, when you call this telephone number, the representative clearly states that they will need an email address from the member to continue the call. In essence, if a member does not have the internet and email address, AAA will not allow a member to manage their privacy, per CCPA.

Many California residents do not have an online (internet) email addresses due to many reasons. If, however, the CCPA law requires access only through the internet and email address, this ruling will bar many Californians from managing their privacy.

If AAA is, in fact, correct as to the need for an email address, a large portion of the California population will be unable to manage their privacy under current CCPA law.

Conclusion: It is hoped that AAA misunderstood the CCPA rules and that, indeed, the law does allows participation for ALL California residents regardless if they have the internet (email address) or not. We seek your opinion on this important public matter.

Sincerely,

Ken

[redacted]
Subject: RE: Additional comment on proposed CCPA regulatory changes
Date: Wednesday, February 12, 2020 4:02:25 AM

I wish to amend the additional comment I submitted the other day to substitute the version shown below The amended portion is indicated in **blue boldface** for ease of identification. (The color and styling has no other effect; it is simply intended to indicate how this revised version differs from the version submitted on Feb. 11.)

[redacted]

[redacted]
Sent: Tuesday, February 11, 2020 3:27 AM
To: 'PrivacyRegulations@DOJ.CA.GOV' <PrivacyRegulations@DOJ.CA.GOV>
Subject: Additional comment on proposed CCPA regulatory changes

The following is an additional comment on the proposed revisions to the CCPA regulations. The portion of this message between dashed lines below is okay to publish in connection with the rulemaking; I ask that my contact info and other personal information be excluded from such publication.

While the proposed change for the required response periods from calendar days to business days is a step in the right direction, the response intervals are still excessively, dangerously short.

Requiring response within 10 to 15 days may be trivial for corporations or larger companies, but it represents a significant burden for sole proprietorships and small businesses with only a handful of employees. What happens if the owner of a sole proprietorship or micro-business is in the hospital, out of the office on a business trip, or (perish forbid) wants to take a vacation or go away for the holidays? These regulations essentially chain sole proprietors to their desks or their computers.

W301-1

While it may be possible to provide some initial response while on the road, dealing with identity verification steps while away from the office may be difficult or impossible: Not everyone stores their business records in the cloud, and doing so significantly increases the risk of data breaches. Assigning legally fraught tasks like responding to privacy requests to temps or part-time employees while the business is otherwise closed or traveling seems imprudent and risky. As a result, a small business owner who wants to, for example, close the office over the Christmas and New Year holiday or attend a business convention in another state may be on very thin ice if the business receives a significant number of requests during that period -- particularly opt-out requests, which under these regulations demand almost immediate action beyond simply reply to a request.

This is another example of how the CCPA and these regulations are structured so as to

disproportionately burden small businesses and give a significant structural edge to big businesses with large staffs and their own compliance or legal departments. The effect for small business is to make it dangerous to ever step away for more than a few days without risking immediately being out of compliance, with essentially no recourse even in emergencies. That's both unreasonable and unfair.

It also significantly increases the risk of harm. Requiring quick responses promotes hasty action, which increases the chances of errors, such as failure to properly verify a requestor or incomplete response to a request. It also increases the harm that may be caused by volumes of abusive or fraudulent requests, something this system already invites.

Privileging corporations over small businesses in this way does not benefit consumer privacy, or will it benefit the California economy. Ten to 15 business days is an unreasonably short timeframe. At least 30 days would be much more appropriate.

W301-1 (cont.)

An additional means by which OAG could partially mitigate the burdensome impact for small businesses would be to add guidance specifying that the required response times shall be measured in business days from the date a request is CONSTRUCTIVELY received. For example, a request delivered via postal mail on a Saturday to a business that is closed on weekends will not be constructively received until the next day on which the business is open, so any stipulated timeframes for response would begin from that day. Similarly, a request sent to a sole proprietor who is in the hospital will probably not be constructively received until that proprietor is discharged.

Adding guidance to this effect would reduce the implicit expectation that small businesses and sole proprietors subject to the CCPA be available 24/7, 365 days a year. That would have the additional benefit of reducing the potentially discriminatory impact of these required response timeframes. For example, WITHOUT such guidance, a Jewish-owned business that receives requests while the business is closed in observation of Rosh Hashanah and Yom Kippur will always have fewer days to respond than a business that does not observe those holidays. Creating such systemic legal disadvantages based on religious or cultural observance seem unreasonable within the bounds of the California Constitution and the state's nondiscrimination laws.

[end of comment]

From: Griselda Perez
To: Privacy Regulations
Subject: CCPA Comment to Proposed Regulations
Date: Tuesday, February 11, 2020 7:00:24 PM

Hello,

We believe Section 999.307 of the proposed regulations (discussing notices of financial incentive) paired with the definition of financial incentive in Section 999.301, is unclear on whether a retailer who periodically mails out promotions or discount codes to its customer lists (similar to grocery mailers that might have cut-out coupons), must provide the notice described under section 999.307 when a consumer requests to have their personal information deleted (Note that this is different than a loyalty program whereby someone might receive a discount or offer as a benefit). Since these promotional offers/discounts are not provided as a benefit nor compensation under a loyalty program, we do not believe these are covered under the financial incentive definition. We suggest adding in verbiage to make clear that these sort of periodic promotional offers/discounts do not fall under the definition of "financial incentive."

W302-1

Best,

Griselda Perez
Associate General Counsel
direct line: [redacted]

LUCKY BRAND
LOS ANGELES
540 South Santa Fe Ave. | Los Angeles, CA 90013

Blog.LuckyBrand.com
Facebook.com/LuckyBrand

From:	Odom, Jennifer
To:	Privacy Regulations
Subject:	Comments on Modifications to Text of Proposed Regulations to Implement the California Consumer Privacy Act
Date:	Tuesday, February 11, 2020 8:17:44 AM
Attachments:	image001.png image002.png image003.png image004.png image005.png CCPA Rule Comment Letter (Feb 2020).pdf

Please find ICI's letter Re. Comments on Modifications to Text of Proposed Regulations to Implement the California Consumer Privacy Act.

Jennifer M. Odom

Assistant to Tami Salmon, Jane Heinrichs, and Sarah Bessin | Investment Company Institute

P: [redacted] | **F:** 202-326-5839 | [redacted] | www.ici.org

1401 H Street, NW, Washington, DC 20005

INVESTMENT COMPANY INSTITUTE

1401 H Street, NW, Washington, DC 20005-2148, USA
202/326-5800 www.ici.org

February 11, 2020

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

Sent via email to PrivacyRegulations@doj.ca.gov

Re: Comments on Modifications to Text of Proposed Regulations to Implement the California Consumer Privacy Act

Dear Ms. Kim:

The Investment Company Institute[1] appreciates the opportunity to comment on the regulations the Department of Justice has proposed to implement Title 1.81.5, the California Consumer Privacy Act (CCPA). According to the Department's current *Updated Notice of Modifications to Text of Proposed Regulations and Addition of Documents and Information to Rulemaking File,* the Department seeks comment on changes made to regulations it previously published in October 2019 to implement the CCPA. As discussed in more detail below, the Institute recommends that the Department further modify these regulations to ensure that the provisions of Section 999.305, Notice at Collection of Personal Information, are consistent with Title 1.81.5 as revised during the 2019 session of the California General Assembly.

W303-1

[1] The Investment Company Institute (ICI) is the leading association representing regulated funds globally, including mutual funds, exchange-traded funds (ETFs), closed-end funds, and unit investment trusts (UITs) in the United States, and similar funds offered to investors in jurisdictions worldwide. ICI seeks to encourage adherence to high ethical standards, promote public understanding, and otherwise advance the interests of funds, their shareholders, directors, and advisers.

EMPLOYEE INFORMATION

During the 2019 session of the California General Assembly, Subsection 1798.145(h) was added to Title 1.81.5. According to Paragraph (1) of this new provision, the entirely of Title 1.81.5 "shall not apply" to:

> (1) Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.

The one exception Section 1798.145(h) provides to this total carve out from Title 1.81.5 can be found in Paragraph (h)(3). It states that "this subdivision shall not apply to subdivision (b) of Section 1798.100(b) or 1798.150."[2] As a result, with respect to employee-related information governed by Subsection 1798.145(h), aside from the provision authorizing a consumer to bring a civil action for a breach, the *only* provision of Title 1.81.5 that would apply to such information is Subsection 1798.100(b).[3] W303-1 (cont.)

Section 1798.100(b) of the CCPA requires a business that collects a consumer's personal information to inform consumers as to (1) the categories of personal information to be collected and (2) the purposes for which the information will be used. This disclosure must occur at or before the point when such information is collected. Section 1798.100(b) further prohibits any business from collecting additional categories of information or using collected information for purposes not disclosed unless the employer first provides the employee (consumer) notice of such collection or use. In other words, Section 1798.145(h) limits the disclosure an employer must provide to its employees or job applicants under Title 1.81.5 to the "categories of personal information to be collected" and "the purpose for which" the information will be used as required by Section 1798.100(b).

---

[2] As you know, Section 1798.150 authorizes a consumer to bring a civil action in the event of a breach involving non-encrypted information.

[3] *Cf.* the exception in Section 1798.145(n) which is not as broad sweeping. That exception only excepts businesses from having to comply with specific sections -- *.i.e.,* Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.135 – of Title 1.81.5.

PROPOSED REGULATION 999.305, NOTICE AT COLLECTION OF PERSONAL INFORMATION

Section 999.305(e) is the only provision in the Department's regulations that appears to address a business's collection of "employment-related information." This provision, however, does not appear to be consistent with the total carve out of Title 1.81.5 provided by Section 1798.145(h) of the CCPA. Instead, Section 999.305(e) requires a business collecting employment-related information from a consumer to comply *with the entirety of Section 999.305 except* for two provisions in it relating to the "notice at collection of employment-related information." These two provisions relieve the employer of having to provide to an employee or job applicant a "do not sell" link and a link or web address to the business's privacy policy.[4]

And yet, as noted above, pursuant to Section 1798.145(h)(3), the *only* requirement in the CCPA that the Department may impose on an employer in connection with its employees or job applicants is a duty to "inform [such consumers] as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used." Period. Because Section 999.305(e) of the Department's regulations impose duties beyond the clear and unambiguous language of Section 1798.145(h) of the CCPA – including a duty to provide additional information such as the privacy notice required by Section 1798.130 of the CCPA and Regulation 999.308 – this provision in the regulations appears to exceed the Department's lawful authority under the CCPA. W303-1 (cont.)

To ensure that Section 999.305 of the Department's regulations is consistent with Title 1.81.5 and, in particular, Section 1798.145(h) of the CCPA, we recommend that the Department revise Section 999.305(e) of the regulations as follows:

(e) With respect to employment-related information, a ~~A~~ business ~~collecting employment-related information~~ shall only be required to comply with the provisions of section 999.305(a) and (b)(1) and (b)(2), ~~except with regard to the following:~~

~~(1) The notice at collection of employment-related information does not need to include the link or web address to the link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info".~~

~~(2) The notice at collection of employment-related information may include a link to, or paper copy of, a business's privacy policies for job applicants, employees, or contractors in lieu of a link or web address to the business's privacy policy for consumers.~~

[4] With respect to the business's privacy policy, Regulation 999.305(e)(2) permits the business to provide a paper copy of its privacy policy in lieu of a link or web address to access such policy.

We believe this revision will clarify that Section 999.305 is not intended to impose on an employer relying on the carve out from Title 1.81.5 in Section 1798.145(h) of the CCPA a duty to provide its employees information beyond that expressly required in Section 1798.100(b) of the CCPA. W303-1 (cont.)

◆ ◆ ◆ ◆

The Institute appreciates the Department's consideration of our comments. If you have any questions about them, please do not hesitate to reach out to the undersigned by phone ([redacted]) or email ([redacted]).

Regards,

Tamara K. Salmon
Associate General Counsel

[redacted]

To: [redacted]
Subject: Privacy Regulations
Date: Comment on proposed CCPA regulatory changes
Friday, February 7, 2020 9:49:09 PM

The following is my comment on the proposed revisions to the CCPA regulations. The portion of this message between dashed lines below is okay to publish in connection with the rulemaking; I ask that my contact and other information be excluded from such publication.

I am heartened to see the addition of § 999.302, Guidance Regarding the Interpretation of CCPA Definitions, which is a welcome step toward addressing the absurdly overreaching nature of the statutory definitions. W304-1

§ 999.305 (a)(4), regarding collection of information from mobile devices, is a well-intentioned, badly framed attempt to deal with a common problem. As a consumer, I am very concerned about the data collection practices of mobile apps, and take various efforts to limit that collection. As a business owner, I am dismayed by the broadness of the phrase "for a purpose that the consumer would not reasonably expect," which, despite the admirable clarity of the example presented, is so broad as to be potentially meaningless.

Consider, for example, the fact that the type of mobile device used is typically revealed in a web browser's user agent information, and that many websites and online services use that information (usually automatically) to tailor their content to better suit the technical limitations of that specific device. There is nothing at all nefarious about such use; it would be very difficult or impossible *not* to collect that data in the context of a user agent; and the normal function of the service might be badly disrupted by the lack of that data. However, does the average consumer "reasonably expect" that? Probably not, unless they are unusually well-versed in web technology. The same is true for business owners, who may sensibly respond to the broadness of this regulation by adding a series of annoying "just-in-time" popup notices to every user interaction, which dilutes the intended purpose of the regulation to meaningless boilerplate that the putative average consumer will simply ignore. This does not seem the desired effect. W304-2

§ 999.312 (a) as revised provides some important incremental relief for online small businesses, but retaining the requirement for a toll-free number for other businesses is impractical, onerous, and unreasonable while providing little utility to consumers. Operating a toll-free number is very costly, that cost can be driven up substantially by malicious activity (frequent prank or robocalls can increase the cost by an order of magnitude), and few consumers under 50 years of age desire (much less prefer) to engage in complex customer service interactions by telephone. Requests made by phone are more difficult to verify, more difficult to audit, and more difficult to properly record, as well as introducing significant opportunities for both error and abuse. While some businesses may prefer to deal by telephone, and may already have existing toll-free numbers that can be used for this purpose, making it a regulatory requirement remains frankly ridiculous and it should be struck. W304-3

§ 999.313: The proposed revision to section (c)(3) is ALMOST a good idea. It attempts to address a problem I raised in my earlier comments on the proposed regulations, which is W304-4 (cont.)

that the absurd broadness of the statutory definitions create insuperable problems for businesses that maintain, for example, archives of published information such as magazines, journals, or newspapers.

For instance, an archive of old magazines may contain various personal information, such as letters to the editor submitted by a particular consumer, but it is probably not "in a searchable or reasonably accessible format," and a business could so describe it to a consumer. However, such information could probably not be said to be maintained "solely for legal or compliance purposes" (a curious framing, since the compliance value of information that cannot be accessed or searched is at best questionable), and whether its use is not "for any commercial purpose" is arguable. In fact, I struggle to envision a scenario in which ALL of the listed conditions of the proposed regulations would be met. Therefore, by requiring that "all the following conditions" be met, the proposed regulation therefore renders itself largely useless and immaterial. W304-4 (cont.)

§ 999.315: Subsection (d) remains a dangerous, badly worded, technically illiterate provision that risks creating a series of unintended consequences. I suspect from the proposed subparagraphs (1) and (2) that the intent of these regulations is to allow businesses to offer settings or extensions that automate the opt-out process. However, the wording of the regulation suggests that online businesses are required to treat ANY browser privacy plugin or device setting as a valid opt-out request, which is absurd. I remind OAG that no industry consensus has ever emerged regarding the treatment of "Do Not Track" browser settings, to the extent that those settings have almost no effect (indeed, some privacy experts recommend that consumers disable those settings to reduce the information transmitted to third parties online). Although I am not a web developer, I can envision at least half a dozen ways a browser addon might "communicate" an opt-out request, and the prospect of designing a website that could not only recognize them all, but respond to them as the law requires is enough to make me cry. W304-5

If the Attorney General desires to create such an onerous technical requirement, which I do not consider prudent or appropriate, it needs to be accompanied by a clear set of open technical standards subject to their own public review and comment process, not buried in poorly worded regulations. If that is not the intent, and if the object of this section is to set certain regulations pertaining to businesses that develop or use specific addons for this purpose (e.g., the browser addon Google offers to allow consumers to globally opt out of Google Analytics), the text needs to say so more clearly.

Regarding Subsection (h), I am dismayed that this provision still asserts that "A request to opt-out need not be a verifiable customer request." I warned in previous comments that the lack of a verification requirement for opt-out requests, combined with the ridiculous over-broadness of the CCPA definitions of "sale" and the regulations' confusing and onerous expectations for compliance (including the problems with 999.315(d) noted above and the farce that is the entire § 999.336, noted below), is an invitation to harassment and abuse. It provides endless opportunities for malicious actors to create liability for businesses and inconvenience for consumers. W304-6

For example, a prankster or malicious individual could read through posted customer comments on a business's website and then submit bogus opt-out requests in the name of every single customer who posted a comment, badly disrupting the business's relationship with its established customers. The business would have little recourse and few permitted

options for determining whether the requests were fraudulent or not.

That same issue also makes it particularly dangerous for online businesses to offer a web form for consumers to submit requests. Any web form attracts spam of varying levels of sophistication. The framing of this subsection effectively obligates businesses to respond to EVERY submission, even ones that are obviously spam or that include malware or other malicious content. That's completely unreasonable and increases the risk of a business being hacked or having its data compromised. W304-6 (cont.)

§ 999.317(e): This subsection's proposed addendum, "Information maintained for record-keeping purposes shall not be shared with any third party," will have an assortment of unpleasant consequences. First, it effectively forbids businesses from using ANY service providers for data storage or records retention: That means, among other things, no backups to cloud storage and no malware scans that involve third-party scanning tools. Second, the proposed amendment would prohibit small businesses from engaging consultants -- even duly contracted ones with NDAs -- to audit the business's records or advise on compliance procedures, or even seeking legal guidance about such matters! That is ridiculous, and will make significantly it harder for businesses to manage their own compliance efforts. For small businesses, getting good help is hard enough; the proposed regulations effectively prohibit it. W304-7

§ 999.336: The framing of this entire section is farcical and begs the question of what "opting out" actually means. The illustrative examples in subsection (d) describe scenarios where businesses are asked not to make commercial use of customers' information (which, I remind the OAG, the CCPA defines absurdly broadly to include a broad range of uses that the average person or common law would not regard as a "sale") -- and then required by regulation to continue doing so on the grounds that not doing so would be discriminatory! I remain unsure how a business can be expected to delete a customer's information and/or cease to make commercial use of it and then be able, much less required, to maintain an ongoing business relationship with that customer.

Consider Example 4: The example asserts that the bookseller's failure to provide coupons is discriminatory, but if the consumer has opted out and demanded deletion of their information, how could the consumer use the coupons? The bookseller must collect personal information from the purchaser to complete a book purchase -- payment information, shipping information, and (for every online retailer I have ever seen or used) an email address to send receipts, shipping updates, and/or fulfilment information. I cannot even fathom how an online retailer could process any transaction or purchase without that information. So, while the email address might not be necessary to provide the coupons, it is almost certainly necessary for the consumer to USE the coupons, which by any sane standard should be "reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business." It is disturbing that the "illustrative examples" proposed evidence such a lack of common sense. W304-8

This entire section is camel-through-the-eye-of-the-needle stuff, and I am certain that every retailer who deals with customers in California is baffled as to what these regulations even expect, much less how to comply.

In sum, the proposed changes include a few positive amendments, some ill-conceived ones, and several that are quite dangerous.

I remain disturbed by the overall impracticality of the regulations, the over-broadness of the definitions, and the invitation to abuse that they represent. As a consumer, I find it hard to see how many of these provisions will benefit me, particularly relative to how onerous they are and how cumbersome they make it for small businesses to comply. These regulations have the effect of providing significant structural advantages to large tech companies like Facebook and Google, which have demonstrated the least good faith in their collection and use of consumer information, which seems to me exactly the opposite of the desired effect. The amendments suggest that OAG does not recognize and/or is not concerned about that substantial risk.

W304-8
(cont.)

[The comment ends here.]

From: Liang Ni
To: Privacy Regulations
Subject: FW: CCPA follow-up questions
Date: Friday, February 7, 2020 4:54:09 PM
Attachments: image001.png

Dear Privacy Regulations Coordinator at CA AG's Office,

We would like clarification on the following language in the proposed CCPA regulation:

1. Under § 999.313(c)(4) of the proposed regulation, "A business shall not disclose in response to a request to know 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, or unique biometric data generated from measurements or technical analysis of human characteristics."

   Questions: We understand that we cannot disclose the above information in our response to a request to know, but can we use these information to verify the requestor's identify?

W305-1

2. Under § 999.326 (a), when a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require that the consumer do the following:

   (1) Provide the authorized agent written and signed permission to do so;
   (2) Verify their own identity directly with the business.
   (3) Directly confirm with the business that they provided the authorized agent permission to submit the request.

   Questions:

   - Are we required to take one or all of the actions above?
   - For (2) Verify their own identity directly with the business, does "their own identity" mean the agent's or consumer's identity? What is "the business"? It is the consumer who is giving the authorization or the business the agent is working for (if any)? What specific questions we should ask to conduct this verification? In summary, we would like to know how to perform this verification in real life situations.

W305-2

W305-3

Thank you for your guidance.

Liang Ni

State Bank of India
(California)

Liang Ni
SVP, Chief Compliance and Risk Officer
& CRA Officer
State Bank of India (California)
Head Office
707 Wilshire Boulevard, Suite 2900
Los Angeles, CA 90017 USA
Tel: [redacted]
Email [redacted]
Web: www.sbical.com
Member FDIC

From: John Davis <[redacted]>
Sent: Thursday, January 23, 2020 11:26 AM
To: Raul Perez <[redacted]>
Cc: Robert Olsen <[redacted]>; Liang Ni <[redacted]>
Subject: RE: CCPA Notice at Collection

Hi Raul:

This responds to State Bank of India's ("Bank") question regarding the regulations that have been proposed ("Prop. Reg.") under the California Consumer Privacy Act (CCPA).

Facts: The Bank is considering entering into a marketing arrangement with a vendor, S&P Global ("S&P"). S&P would provide the Bank with data that includes consumer's personal information (PI) for the purpose of marketing the Bank's business products to these consumers. By "business" products we assume you mean products that are for business or commercial, as opposed to classically "consumer" (personal, family or household), purposes. Despite that the individuals whose information you would receive from S&P would meet the definition of a "consumer" under the CCPA which means almost any individual resident of California.

Issue: The Bank had a question with regard to its obligation to provide a Notice at Collection (NAC) to such consumers. Specifically, the Bank sought advice as to whether the exception from providing an NAC under Prop. Reg. .305(d) is available for all businesses (but limited to situations where they do not collect PI directly from consumers) or alternatively only for those businesses that never collect information directly from consumers. You were not asking about S&P's own obligations under the CCPA.

Short Answer:

We tend to think that the exception should be read narrowly as applying to those businesses which never, or at least whose general practice is to not to, collect information directly from consumers, such as a data broker. Thus while S&P itself may be covered by the exception, the Bank probably is not.

Analysis:

Prop. Reg. .305(d) provides that:

> *"A business that does not collect information directly from consumers does not need to provide a notice at collection to the consumer, …"* (§ 999.305(d)).

The regulation itself does not further clarify whether this exception applies to all businesses or only those that primarily do not collect information directly from consumers. Therefore, it is not perfectly clear whether it was intended to apply in any situation where a business does not collect information directly from a consumer or instead to those businesses that never collect PI directly from consumers or at least not as part of their standard practice.

We first note that Prop. Reg. .305(d) does more than create an exception. It goes on to impose some significant burdens which in turn shed light on who the exception was intended to cover. In full Prop. Reg. .305(d) provides as follows:

(a) 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. Confirm that the source provided a notice at collection to the consumer in accordance with subsections (a) and (b) [which would include a "Do Not Sell" link]; and
    b. Obtain signed attestations from the source describing how the source gave the notice at collection and including an example of the notice. Attestations shall be retained by the business for at least two years and made available to the consumer upon request.

Our point is that rather than creating a complete exemption to the requirement to give an NAC Prop. Reg. .305(d) only pushes the NAC obligation upstream to the party which originally collected the information. This sheds some light on the purpose of the exception and thus on its intended scope, which is that exception was intended for data brokers who never collect information directly from consumers. (Note, by the way, that the data broker must verify that the NAC was given by the source of the information, not the ultimate recipient. In other words, the data broker cannot push the responsibility downstream to the ultimate recipient of the PI (which would be the Bank in its arrangement with S&P) but rather must push it upstream to the original source.)

The reading suggested above is further supported by the supplemental information the Attorney General issued with the proposed regulations. In the Initial Statement of Reasons

(ISOR) to Prop. Reg. .305(d), the AG states that this exception, "addresses businesses, such as data brokers, that do not collect personal information directly from consumers." The AG further describes the types of businesses the exemption addresses as those that, "collect personal information primarily in order to sell it."

This seems to suggest that the exception was intended to address businesses which either never, or at least that primarily do not, collect information directly from consumers and primarily for the purpose of selling it to others, such as data brokers. It does not seem that a business that does primarily collect information directly from consumers, such as a retail bank, may rely on this exception to avoid providing an NAC in situations where it happens to collect information indirectly from consumers, such as through a data broker. In other words, it seems this exception may not be available to the Bank because we assume the Bank regularly collects personal information directly from consumers.

(Ironically, while the .305(d) exception is likely not available to the Bank itself it may be available to S&P which we think of as a data broker. We bring this up because in addition to the compliance issues the Bank is facing directly, as discussed below, the Bank should seek reasonable assurances from S&P as to S&P's own compliance with the CCPA, and Prop. Reg. .305(d) in particular, as part of the Bank's vendor management protocols.)

We would note that given the utter lack of clarity surrounding this law, an alternative reading of Prop. Reg. .305(d), as with other parts of the CCPA and the proposed regulations, is not entirely unreasonable. However, we have serious doubts that a court or regulator would broadly interpret this provision so as to apply in any situation where an otherwise covered business collects personal information but not directly from the consumer.

As such, based on the above and without further guidance to rely on, we tend to think that the exception should be read narrowly as applying to those businesses whose general practice is to not collect information directly from consumers, such as a data broker. Therefore, it would appear that the Bank would still be subject to the NAC obligation when it collects PI from S&P.

This opens a can of worms. It might mean that the Bank would need to arrange for the subject consumers to receive the Bank's NAC before it collects any PI from S&P. This could be logistically challenging. It seems that S&P or another upstream source of the information would need to give the Bank's NAC to subject consumers before it releases the consumers' PI to the Bank. There may be other solutions but we suggest you discuss it with S&P and then re-contact us.

In addition, the Bank should also consider that the B2B Exemption expressly does not apply to the CCPA's opt-out provisions in Section 1798.120. Section 1798.145(n)(1). The requirement to provide an opt-out triggers upon the "sale" of PI and the CCPA employs an extremely broad definition of sale (which is subject to certain exceptions). Section 1798.140(t)(1). The definition seems broad enough to cover almost any commercial transfer of information, not only traditional sales for cash. As such, the purchase of marketing information from S&P may constitute the sale of PI triggering the opt-out requirements. While the obligation to provide an opt-out notice is imposed on the entity that is selling the information (i.e. potentially S&P) and not the purchaser, each consumer whose PI is being transferred may have the right to opt-out of their PI being disclosed as part of this transaction. As such, even if the information the Bank receives from S&P is otherwise exempt under the B2B Exemption, the Bank will want to consider how this transaction may intersect with the

consumer's right to opt-out under Section 1798.120.

We trust the above information was helpful. If you have any questions regarding the above or anything else please do not hesitate to ask.

John M. Davis, Associate | Aldrich & Bonnefin, PLC
18500 Von Karman Avenue, Suite 300, Irvine, California 92612
T. [redacted] | F. (949) 474-0617 | [redacted]

From: John Davis
Sent: Monday, January 13, 2020 12:44 PM
To: Raul Perez <[redacted]>
Cc: Robert Olsen <[redacted]>; Liang Ni <[redacted]>
Subject: RE: CCPA Notice at Collection

Hi Raul:

Hope you had a good new year as well. You raise a good question which does not admit an easy answer. I will start looking into this and expect to have a response to you by mid next week (due to current backlog).

If you have other questions on this or anything else please do not hesitate to contact me. Have a great rest of the day.

John M. Davis, Associate | Aldrich & Bonnefin, PLC
18500 Von Karman Avenue, Suite 300, Irvine, California 92612
T. [redacted] | F. (949) 474-0617 | [redacted]

This e-mail and any accompanying documents contain information from the law firm of Aldrich & Bonnefin, PLC and are confidential and legally privileged. The information is intended only for the sole use of the recipient named in this e-mail. If you are not the intended recipient please contact administrator@ABLawyers.com, and delete all copies of it from your system. Please note that the sender accepts no responsibility for viruses and it is your responsibility to scan this e-mail and attachments (if any). No contracts may be concluded on behalf of the sender by means of electronic communications unless expressly stated to the contrary.

From: Raul Perez [redacted]>
Sent: Monday, January 13, 2020 11:35 AM
To: John Davis [redacted]>
Cc: Robert Olsen <[redacted]>; Liang Ni [redacted]>
Subject: CCPA Notice at Collection

Hi John –

I hope the New Year is treating you well.

The Bank is seeking advice as it relates to *§ 999.305(d)* under the CCPA.

> *§ 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, …*

The Bank would like to onboard a new vendor, S&P Global, which would provide the Bank with data that includes consumer's personal information for the goal to market and sale the Bank's business products. The Bank's concern is the delivery of the required *Notice at Collection Disclosure (NAC)* to these consumers who are not our customers before the collection of such PI.

However, in reading the above noted section (*§ 999.305(d)*), it may seem that the Bank might be exempt from having to deliver the NAC to these consumers whose personal information was collected by S&P Global and not the Bank directly?

Or, in terms of general practices and operations, because the Bank is indeed a "*business that collects information directly from consumers*", that section does not apply and is only applicable to a "*business that does not collect information directly from consumers*"? In other words, can the Bank, who is a business that collects directly from a consumer, be exempted from providing a NAC to consumer's whose personal information was derived from a third-party?

Thank you for your time and the Bank understands their may be an associated fee.

Warm Regards,

State Bank of India (California)

Raul Perez
Compliance & CRA Analyst
State Bank of India (California)
Head Office
707 Wilshire Boulevard, Suite 2900
Los Angeles, CA 90017 USA
Tel: [redacted]
Email: [redacted]
Web: www.sbical.com

Member FDIC

From: Tara Aaron-Stelluto
To: Privacy Regulations
Subject: Comment on the Revised Rules for CCPA
Date: Friday, February 7, 2020 3:31:02 PM

To the Attorney General's Office for the State of California:

The proposed modification to Section 999.306(f) of the California Consumer Protection Act Regulations allowing for companies subject to CCPA to place an "on/off toggle" (the "Toggle") next to the "Do Not Sell My Personal Information" link (the "Link") is extremely poor design. The Toggle next to the Link, which is a negative statement, requires consumers to understand whether they should be making a double negative statement ("No, Do Not Sell My Personal Information"), or a positive statement ("Yes, Do Not Sell My Information") in order to effectuate their wishes. I understand that the Toggle is optional, but it should instead be banned. The Toggle creates extreme confusion that complicates compliance for companies and puts them at risk of violating the CCPA when they do not comply with the wishes that a user thinks he or she has expressed, since both parties are at risking of misunderstanding the commands expressed.

W306-1

A hyperlink should be the exclusive requirement, and furthermore, the Regulations should further effectuate the requirement in the CCPA that the Link be "conspicuous," by regulating placement and font size on a website of a company that is required to include such a Link.

Respectfully submitted,
Tara Aaron, CIPP/US / E

Tara M. Aaron, CIPP/US, CIPP/E
Aaron | Sanders PLLC
605 Berry Road
Suite A
Nashville, TN 37204

[redacted] • O [redacted] • F 615•250•9807 • M [redacted]
www.aaronsanderslaw.com • [redacted] • [redacted]

--

From: Field Garthwaite
To: Privacy Regulations
Subject: Proposed CCPA Legislation
Date: Friday, February 7, 2020 3:22:15 PM

Your proposed CCPA legislation does not go far enough to ramp up penalties for companies generating >$1B or >$10B annually from digital transactions, nor does it properly exonerate startup and smaller companies who are forced to adopt policies but lack the ability to invest in solutions. Thus the legislation will inadvertently hurt small businesses and innovative startups in ways regulators have not properly though through. Smaller companies lack the legal team and scaled user base that Google, Facebook and Amazon have which makes compliance and opt-in substantially easier. By not properly forcing companies with substantially higher online digital transaction volume to go through higher scrutiny and provide more transparency to the users and to the market, CCPA will largely not impact the businesses it is intending to regulate and will negatively affect thousands of businesses due to a lack of thoroughness with regards to these issues. W307-1

I highly value the work the California Department of Justice is doing to enact this measure. Thank you for taking a moment to consider these comments and in your work protecting consumers in our state.

- Field Garthwaite

From: Sara DePaul
To: Privacy Regulations
Cc: Christopher Mohr; Carl Schonander; Sharon Burk; Jeff Joseph; Sara Kloek
Subject: SIIA Comments to Modifications to the Proposed CCPA Regulations
Date: Wednesday, February 26, 2020 12:24:34 PM
Attachments: image001.png
SIIA Comments re CCPA Regs Feb 2020 FNL FLD.pdf

On behalf of the Software & Information Industry Association (SIIA), I submit our written comments on the Attorney Genera's updated notice of modifications to the text of the proposed CCPA regulations. If you have any questions or concerns, please contact me at your convenience.

With kind regards,
Sara

Sara DePaul
Senior Director, Technology Policy
SIIA - The Software & Information Industry Association
1090 Vermont Ave NW, Sixth Floor, Washington, DC 20005
202-789-4471 Office / [redacted] Mobile / [redacted] Twitter
siia net/policy

SIIA Accelerating Innovation in Technology, Data & Media

1090 Vermont Ave NW Sixth Floor
Washington DC 20005-4905
www.siia.net

February 25, 2020

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

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

The Software & Information Industry Association (SIIA) appreciates the opportunity to submit additional comments on the modifications to proposed regulations implementing the California Consumer Privacy Act (CCPA). These comments, like our prior submission, highlight the constitutional defects raised by the CCPA and, by extension, any implementing regulation.[1] We also identify discrete compliance issues raised by the proposed text in several provisions.

SIIA is the principal trade association for the software and digital content industry. We provide global services in government relations, business development, corporate education, and intellectual property protection to the leading companies that are setting the pace for the digital age. With over 800 members spread over eight specialized divisions, SIIA provides a voice for its membership on the importance of information to promote a competitive, fair, and innovative digital economy. Our members include software publishers, financial trading and investment services, specialized and B2B publishers, and education technology service providers.

We submit these comments to reiterate our concern that the CCPA, and the implementing regulation, will be vulnerable to a First Amendment challenge unless the Attorney General uses the authority granted by Cal Civ. Code 1798.185(a)(3) to cure the unconstitutional regulation of information in the public domain. In addition, our comments identify several proposed provisions that could benefit from edits to avoid unintentional compliance outcomes. The identified provisions are not an exhaustive list, but represent key concerns based on SIIA's members.

W308-1

[1] SIIA Comments on the Proposed Text of the CCPA Regulations (Dec. 6, 2019), available at https://www.siia.net/Portals/0/pdf/Policy/Privacy%20and%20Data%20Security/SIIA%20Comments%20re%20CCPA%20regs%206%20DEC%20FNL%20%20FILED.pdf?ver=2019-12-06-172925-923.

I. The Attorney General Should Cure the CCPA's First Amendment Defects

We appreciate the Attorney General's partial response to the constitutional concerns we previously raised. First, we were glad to see Section 999.305(d), which would have required attestations before disseminating public domain information, stricken from the draft regulations. As we noted in our comments, the draft language raised a number of significant First Amendment and policy concerns by imposing impossible compliance obstacles that would render the publication of information unlawful even when the CCPA would otherwise permit its dissemination. The Attorney General's decision to strike this provision was correct as a matter of law and policy.

Second, we thank the Attorney General for curing a similar problem with the definition of "categories of sources" to exclude the reference to public records. As our comments flagged, the capture of public records by this definition was in contravention of AB 874, which amended the CCPA to entirely exclude public records information from its regulatory scope. Moreover, it raised significant First Amendment concerns because it regulated the public domain without advancing a compelling interest or tailoring the regulation to meet that interest. Again, the decision to strike this reference is the right choice as a matter of law and policy.

Although we welcome these revisions, they are insufficient to address the statute's core First Amendment problems. The statute defines "personal information" to exclude "publicly available information."[2] The CCPA, however, limits "publicly available information" to "information that is lawfully available from federal, state, or local government records." It does not exclude a second and considerably larger category of public domain information, which is information that is widely available in private hands. This second category of public domain information includes professional contact details, credential and licensing details, biographical data, and other information drawn from registries, directories, websites, and news and social medial channels.

W308-1 (cont.)

The broad and untailored regulation of this second category of the public domain raises significant constitutional and policy concerns. As a constitutional matter, the CCPA's regulation of the non-governmentally sourced public domain impedes protected speech without advancing a compelling government interest or

[2] The CCPA's treatment of publicly available information has been a concern of SIIA's through this entire legislative process, and we have documented the statute's constitutional defects in several filings. For additional resources, please refer to our December 6, 2019 written comments (*see* fn. 1, *supra*), which cites to a memorandum from our outside counsel, our December 26, 2019 letter to the Attorney General, and the Senate and Assembly's Bill Analyses for AB 874 (which was enacted in response to the concerns outlined in our outside counsel memo).

engaging in the tailoring to meet that interest as required by the First Amendment. *See IMS Health v. Sorrell*, 564 U.S. 552 (2011); *Bartnicki v. Vopper*, 532 U.S. 514 (2001). Moreover, the CCPA discriminates among speakers and on the basis of speech content, which separately violates the First Amendment.

W308-1 (cont.)

As a policy matter, the regulation of the non-government public domain will result in poor policy outcomes, including the suppression of information for use in law enforcement investigations, investigative journalism, identity verification, scientific and medical research, corporate due diligence, and finding missing persons. SIIA's members provide the tools necessary to achieve these socially valuable uses. The value of these tools depends on their completeness and accuracy, and consists in large part of information that is publicly available from both governmental and non-governmental sources. If the CCPA and its implementing regulation do not exclude the non-governmental public domain from their scope, these socially valuable uses will be impeded through efforts to obfuscate the ability to collect, disseminate, and publish information in the public domain.

W308-2

To cure these constitutional and policy flaws, SIIA again urges the Attorney General to use his authority in Section 1798.185(a)(3) to promulgate a regulation that makes the CCPA constitutional. This can be done by expressly excluding public domain information that is widely available from non-governmental sources from the regulation's scope.

W308-1 & W308-2 (cont.)

II. The Regulations Should be Amended to Define "Data Broker" and Clarify When Non-Data Broker Third Parties Must Provide Notices. *See* Sections 999.301(d)-(e); 999.304; 999.305(a)(7) and (d).

The modifications add references to "data brokers" in the definitions for "categories of sources" and "categories of third parties." *See* Section 999.301(d) and (e). The proposed modifications, however, do not incorporate a corresponding definition for "data broker" to explain the use of the term in .301(d) and (e). This is in contrast to Section 999.305, which also refers to "data broker," but expressly ties the use of the term in that provision to the data broker registry law (*see* Cal Civ. Code 1798.99.80 *et seq.*), which in turn defines a "data broker." To cure any resulting regulatory ambiguity, we respectfully urge the Attorney General to promulgate a regulation that adopts the definition of "data broker" from Cal Civ. Code 1798.99.80(d).[3]

W308-3

Relatedly, we note that the modification to Section 999.305(d) to address "data brokers" leaves continued ambiguity regarding the obligations of non-data brokers that collect information indirectly from consumers with respect to the

[3] We note that the "data broker" definition in Section 1798.99.80 is ambiguous on its own with respect to which businesses qualify as data brokers.

notices required at the time of collection. As we noted above, Section 999.305(d) applies only to businesses that register as data brokers in compliance with Cal Civ. Code 1798.99.80. That law defines a "data broker" to exclude several categories of businesses to the extent they are covered by another sectoral federal privacy law (i.e. consumer reporting agencies, financial institutions, and insurance companies). Thus, an entity like a consumer reporting agency, will not be subject to the proposed modifications in Section 999.305(d).

W308-3 (cont.)

To cure this, the Attorney General should amend the modifications at Sections 999.304 and 999.305(a)(7) and (d) to clearly state that businesses that are not data brokers and that do not collect information directly from consumers are not required to provide a notice at the time of collection to the consumer. Doing so will permit businesses that are excluded from the "data broker" definition to continue to engage in data collection while bound by existing federal sectoral privacy laws.

III. Affirmative Authorization Should Not Be Defined to Require a Two-Step Verification Process. *See* Sections 999.301(a); 999.316(a).

In our prior comments, we objected to the CCPA's proposal to require a two-step process for consumers 13 years and older to opt-in to the sale of their personal information. As we noted then, and reiterate now, the de facto double opt-in fails to meaningfully advance consumer choice. Indeed, it risks unduly interfering with consumer choice by calling into question the informed decision the consumer already made with respect to their request to opt-in. Consumers should be free to exercise their choices without barriers designed to signal that such choice is wrong or risky. Moreover, consumers should be able to exercise a meaningful and intentional opt-in without a barrage of repeat notifications that realistically only interrupt the consumer's online experience and risk notification fatigue.

W308-4

The baseline definition for "affirmative authorization" accomplishes what is the appropriate and necessary consent for consumers 13 years and older who request to opt-in to the sale of their information. By the terms of the proposed definition, that authorization "means an action that demonstrates the ***intentional decision*** by the consumer to opt-in to the sale of personal information." The strength of this provision lies in its requirement of a demonstrated intentional decision to opt-in, which can and should be accomplished in one notice. **To accomplish this, we urge the Attorney General to modify the definition at Section 999.301(a) to strike the two-step requirement. Then, to fully capture the spirit of this change, the Attorney General should also modify Section 999.316(a) to remove the requirement for a second step in the opt-in process.**[4]

[4] We also note that if the Attorney General does not take our suggested modification for Section 999.301(a), then a modification of Section 999.316(a) is absolutely necessary. As

W308-5

IV. Data Does Not Have an Independent Value and the Regulations Should Not Require a Misleading Disclosure of a Value that Cannot be Quantified. *See* Sections 999.307(b)(5); 999.337).

We recommend that the Attorney General revise the proposed modifications to remove any requirement for businesses that offer financial incentives to provide estimates of the value of the consumer's data. **To accomplish this, we suggest the Attorney General strike subsections (a) and (b) of 999.307(b)(5) and strike Section 999.337 entirely. The revised Section 999.307(b)(5) would read: "An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data."**

The purpose of our recommendation is to avoid value disclosures that are impossible to calculate. As a general matter, data does not have independent value. Its value, if any, is subjective, in flux, and depends on the context in which it is collected and processed. Because of data's lack of a clear and objective value, even academics are flummoxed when estimating its value, often arriving at wildly different estimates for the same services. W308-6

One of the fundamental misunderstandings in the debate over the value of data is the assumption that its usefulness to advertising corresponds to its value. It is not possible, however, to derive a value estimate from data solely by looking at ad revenue. With respect to ad-supported and free online services, the consumer value rests in the experience, which is made possible by the data that supports the ad model. Consumers do not exchange their data for the experience. Rather, the experience is made possible by the data. The data, in turn, enables the ads so that the service can provide its core service – the personalized content. The business model isn't compensated by consumer's data, but rather through the selling of ads. The data may influence the delivery of the ads, but it does not drive the value of the ad sales, which are influenced by external metrics relating to delivery, views, and clicks.

---

currently drafted, Section 999.316(a) sets out the requirements for a "request to opt-in" as requiring two steps: (1) a clear "request to opt-in" and (2) a separate confirmation of the consumer's choice to opt-in. The problem, however, is that "request to opt-in" is a defined term. As defined in Section 999.301(t) it means "the ***affirmative authorization*** that the business may sell personal information about the consumer. . ." "Affirmative authorization," as we discuss above is currently defined to mean a two-step process for obtaining consent and then confirming that consent. The explicit inclusion of a two-step process in Section 999.316(a), therefore, is superfluous because by its terms it incorporates the "affirmative authorization" requirement of a two-step process. If the Attoreny General keeps both provisions as currently proposed, then Section 999.316(a) could be interpreted to actually require a three step process for an opt-in: First, the request to opt-in and the two-step process it requires by its very terms; and secondly, the .316(a) confirmation of the request to opt-in. W308-5 (cont.)

V. Businesses that Operate Online Should Not Be Required to Maintain Toll-Free Numbers for Receiving Requests to Know. *See* Section 999.312(a).

We are concerned that the proposed modification to Section 999.312(a) would require businesses that do not have a direct relationship with consumers to maintain a toll-free telephone number for receiving requests to know even if the business operates online. The requirement to maintain a toll-free telephone number is expensive and burdensome, and it is not clear how mandating its upkeep and availability materially improves a consumer's ability to submit a request to know to an online business with which she does not have a direct relationship. **We respectfully request that the Attorney General modify the proposed text to permit online businesses that do not have direct relationships with consumers to provide two or more designated methods, which can include a toll-free number, an interactive webform, a designated email address, or a form submitted via the mail.**

W308-7

VI. Businesses Should Not be Burdened With Obligations to Respond to Unverified Requests to Know. *See* Section 999.313(c)(1) and (3).

Both the initial proposal and the current modifications contemplate obligations for businesses with respect to *unverified* requests to know in Section 999.313(c)(1). This is inconsistent and contrary to the CCPA, which expressly contemplates the discarding of unverified requests precisely because they are unverified. *See* Section 1798.105. As a practical matter, the CCPA's direction that business can and should discard unverified requests operates for the protection of the consumer, which Section 999.313(c)(1) undermines. **To address this, we suggest the Attorney General strike the last sentence of Section 999.313(c)(1)**.

W308-8

We are also concerned that the modifications to the proposed text include the deletion of Section 999.313(c)(3), which would have prohibited a business from providing a consumer with specific pieces of personal information when the disclosure created a substantial, articulable, and unreasonable security risk. The modifications replace this text with a four-part test. We are concerned, however, that this new test is too restrictive, overly burdensome, and completely fails to address the key security concerns addressed by the original language.

The security standard originally set forth in Section 999.313(c)(3) was high. A business could not merely identify a potential security risk and withhold the information when responding to a request to know. To be a valid withholding, the business had to be able to show that the disclosure would create a "substantial, articulable, and unreasonable risk to the security of [the] personal information, the consumer's account with the business, or the security of the business's systems or networks." When this standard is met, a business should not be compelled to turnover personal information in response to a request to know.

W308-9

We respectfully urge the Attorney General to amend the modification to re-insert the original Section 999.313(c)(3). With respect to the four-part test, we urge the Attorney General to largely retain it, but draw a clearer line by making any of the enumerated conditions sufficient on their own to limit access rights in a manner that balances individual privacy and operational burdens. We suggest the following language:

W308-9 (cont.)

In responding to a request to know, a business is not required to search for or provide personal information ~~if all~~ that meets any of the following conditions ~~are met~~, provided the business describes to the consumer the categories of records that may contain personal information that it did not provide because it meets one of the conditions state ~~above~~ below

(a) The business does not maintain the personal information in a searchable or reasonably accessible format;
(b) The business maintains the personal information solely for legal or compliance purposes;
(c) The business does not sell the personal information and does not use it for any commercial purpose
(d) ~~The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above~~. The business does not associate the personal information with a consumer in the ordinary course of business; or
(e) The personal information was not collected from the consumer or a third party, but was instead derived internally by the business.

W308-10

VII. Conclusion

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

Respectfully submitted,

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