Message

From: BC Smith [redacted]
Sent: 3/24/2020 4:56:28 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: 999.315 CCPA Comment

Hello - thanks in advance for your time and consideration.

In **§ 999.315. Requests to Opt-Out, section (a),** as it currently stands, it allows for businesses to comply and have two methods to opt-out plus a way to opt out on their website or mobile app. **There is a loophole here which would make it impossible for an authorized agent to opt-out a consumer. This is because all three opt-out methods provided could involve the individual consumers mobile device.**

For example, as it is currently stands a business could comply with the law and provide the following three methods of opt-out that **require** the individual consumers mobile device as stated above:

1. Turn on the privacy opt-out available from your mobile operating system
2. Download the TrustArc app, provided by industry privacy company TrustArc, and opt-out.
3. Download the COMPANY app and select opt-out.

W309-1

If these all **require** the consumers **personal** mobile device (requiring the consumer themselves to login to their password protected phone) then there is no way for an authorized agent to Request an Opt-Out on the consumers behalf via these three opt-out methods. In fact, the authorized agent would have to use the individual consumers mobile phone to opt-out the consumer. This is problematic and creates a loophole for companies who can now respond to authorized agents with the opt-out methods, while leaving the authorized agent no feasible way to opt-out on behalf of the consumer.

I propose that **§ 999.315. Requests to Opt-Out, section (a),** should state something to the effect of: There must be at least one method of opt-out that does not require the consumers mobile device and this method must be easily accessible and useable by an authorized agent, such as an email address and not a postal address.

Thank you,

Ben

Message

From: Monticollo, Allaire [redacted]
Sent: 3/26/2020 3:44:16 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Jaffe, Dan [redacted]
Subject: ANA Comments on Second Set of Modifications to the Proposed CCPA Regulations
Attachments: ANA Comments on Second Set of Modifications to Proposed CCPA Regulations.pdf

Dear Attorney General Becerra:

Please find attached comments from the Association of National Advertisers (ANA) in response to your request for input on the second set of modifications to the proposed regulations implementing the CCPA.

If you have any questions, please feel free to reach out to Dan Jaffe at [redacted] or by phone at 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

****
This electronic mail transmission may contain confidential or privileged information. If you believe you have received this message in error, please notify the sender by reply transmission and delete the message without copying or disclosing it.
****



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

Second Set of Modifications to the California Consumer Privacy Act Proposed Regulations

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
2020 K Street, NW
Suite 660
Washington, DC 20006
[redacted]

Counsel:
Stu Ingis
Mike Signorelli
Tara Potashnik
Allaire Monticollo
Venable LLP
600 Massachusetts Ave., NW
Washington, DC 20001
[redacted]

March 27, 2020

On behalf of the Association of National Advertisers ("ANA"), we provide the following submission in response to the California Office of the Attorney General's ("CA AG") March 11, 2020 request for public comment on the second set of modifications to the proposed regulations implementing the California Consumer Privacy Act (the "CCPA").[1] While we fully support the goal of creating strong and meaningful privacy protections for Californians, certain provisions in the draft rules could hinder consumer privacy and choice rather than advance it. We therefore urge the CA AG to update the draft rules to better protect California consumers and provide more clarity for businesses, as discussed in more detail in the following comments.

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 provided the California government with input at nearly every stage in the CCPA's development. We have testified in person at legislative and administrative hearings, submitted written comments on the content of the draft regulations, held discussions with government staff, and closely followed the changes to the CCPA through the legislative and regulatory process. While we commend your office's efforts to develop a regulatory scheme that will protect consumers and allow businesses to continue to support and underpin what has been California's vibrant economy, we believe that because of the very limited time for companies to come into compliance with the rulemaking effort before the CA AG's enforcement authority is launched and the virtually unprecedented disruption caused by the current global COVID-19 pandemic it would be appropriate to forbear from enforcement until January 2, 2021. During these extraordinarily turbulent times, we ask that your office provide the business community the ability to focus its resources on addressing the global health and economic challenges facing all of us. W310-1

Below, we provide detailed comment in response to your March 11, 2020 request. We believe certain provisions in the text of the draft modified proposed rules move far beyond the intent and scope of the CCPA and might fall outside of the CA AG's authority to regulate pursuant to the statute. We are also confident that certain specific proposed updates to the draft regulations would improve the legal regime for both consumers and businesses alike.

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. Developing such processes with workforces attempting to work remotely during the pandemic sweeping California and the globe adds yet another unforeseen complexity. Though hardly practical under

[1] California Department of Justice, *Notice of Second Set of Modifications to Text of Proposed Regulations* (Mar. 11, 2020), located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-second-mod-031120.pdf? (hereinafter, "Notice").

the Governor's order for all in the state to stay home, if this regulatory process is to continue during this period, 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 consistently and reliably to consumers.

We and our members strongly support the responsible use of data and the aim of enhancing consumer privacy that is inherent in the CCPA. One example of such a crucial use of data is the call by the government to use data to help combat COVID-19. Nevertheless, the proposed regulations remain significantly unclear in several critical areas of vital importance to both consumers and businesses. We incorporate by reference our previous comments filed with your office, and we highlight here the following key issues:

W310-1 cont.

W310-1 cont.

I. Delay Enforcement Until January 2, 2021
II. Clarify Financial Incentive Terms to Enable the Continued Existence of Loyalty Programs
III. Allow Businesses to Choose to Honor Global Privacy Controls or Offer Another, Equally Effective Method for Consumers to Opt Out of Personal Information Sale
IV. Clarify that Internally-Generated Inferences and Derived Data Are Not Subject to a Consumer Request to Know
V. Provide Flexibility for Offering Opt-Out Mechanisms
VI. Enable Flexibility for Providing the CCPA-Required Notice at Collection to Consumers Through the Telephone and in Person
VII. Clarify That Qualifying Businesses Must Provide Additional Metrics Beginning in 2021

I. Delay Enforcement Until January 2, 2021

With less than four months before CCPA enforcement is scheduled to begin, the regulations implementing the law have not yet been finalized. In the face of this uncertainty, businesses have been forced to implement brand new processes for the CCPA based on incomplete regulatory requirements, and these processes must change with each update to the draft rules. Current events have also placed significant strain on businesses in their earnest efforts to comply with the CCPA and its regulations. The recent outbreak of COVID-19 has brought normal business operations and typical consumer interactions to a halt, as California's governor has instituted a mandatory stay-at-home order, which has paused or dramatically altered day-to-day activities. The health crisis, coupled with the unfinished nature of the draft CCPA rules, has significantly impacted businesses' ability to create processes and procedures to keep up with the continuously evolving proposed regulations. We therefore ask you to forbear from enforcing the CCPA until January 2, 2021.

COVID-19 has substantially encumbered businesses' ability to operationalize the draft rules implementing the CCPA prior to July 1, 2020. The World Health Organization has proclaimed the virus to be a global pandemic.[2] President Trump has also declared a national state of emergency due to its rapid spread and its potentially deadly effects,[3] and declared California a "major disaster."[4] Governor Gavin Newsom has declared a state-wide order for Californians to shelter in place, ordering them to "stay in their homes unless they are accessing essential services, such as pharmacies, grocery stores and banks."[5] The disruption to daily life and business operations presented by the virus cannot be overstated. W310-1 cont.

On March 20, 2020, in the midst of the spreading COVID-19 pandemic, over sixty-five trade associations, organizations, and companies sent your office a letter asking you to delay the effective date of the rules as well as enforcement until January 2, 2021.[6] We renew that request in these comments, as our members employ millions of individuals who are faced with this unprecedented health emergency. Employees who are responsible for CCPA compliance are being forced to divert resources to provide timely responses to consumer requests given the current state of affairs. The law gives businesses forty-five days to respond, but many of the same employees responsible for responding to requests are now working remotely or not at all or are seeking to support workforces working remotely. Moreover, for many businesses, available resources have been diverted to efforts to respond to COVID-19. Entities are in talks with the

---

[2] World Health Organization, *WHO characterizes COVID-19 as a pandemic* (Mar. 11, 2020), located at https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen.

[3] White House, *Proclamation on Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak* (Mar. 13, 2020) located at https://www.whitehouse.gov/presidential-actions/proclamation-declaring-national-emergency-concerning-novel-coronavirus-disease-covid-19-outbreak/.

[4] Office of Governor Gavin Newsom, *California Secures Presidential Major Disaster Declaration to Support State's COVID-19 Emergency Response* (Mar. 22, 2020), located at https://www.gov.ca.gov/2020/03/22/california-secures-presidential-major-disaster-declaration-to-support-states-covid-19-emergency-response/.

[5] *Californians ordered to shelter in place*, CALMATTERS (Mar. 20, 2020), https://calmatters.org/newsletter/california-coronavirus-homeless/.

[6] *Joint Industry Letter Requesting Temporary Forbearance from CCPA Enforcement* (Mar. 20, 2020), located at https://www.ana.net/getfile/29892.

U.S. government about substantially realigning their daily operations to produce necessary medical equipment and supplies to aid the fight against the virus.[7] Given the unparalleled present situation and the unique realities facing consumers and businesses alike, we urge your office to delay enforcement so businesses can allocate crucial funds, labor, and time to supporting their employees as well as California's and the national response to COVID-19.

Additionally, conduct undertaken now during the emergency should not be the subject of CCPA enforcement actions. Businesses are understandably focused on ensuring the health and safety of their workers and maintaining economic viability in the face of immense challenges. Businesses should not be penalized under the CCPA for current conduct or activities when their attention is rightfully focused on the dire and important matter of managing the novel coronavirus. Relevant authorities in other jurisdictions, such as the United Kingdom Information Commissioner's Office ("UK ICO"), have suspended data protection regulatory actions during the outbreak.[8] The California Attorney General should follow the UK ICO's approach by refraining from using activities undertaken during this exceedingly difficult present period as a hook for enforcement actions.

W310-1 cont.

Developing needed processes to comply with the CCPA necessarily has taken a backseat to the urgent and pressing health crisis. Business efforts to build CCPA compliance mechanisms based on the most up-to-date draft rules have been delayed. Threatening businesses with the prospect of extremely burdensome and resource-intensive litigation in the present catastrophic economic and health emergency will cause increased stress in an already precarious state of affairs. Many businesses who employ millions of Californians are simply trying to keep their doors open without going under during these dire times.[9] Small businesses and startup entities

---

[7] David Shepardson, *GM, Ford in talks with Trump administration on medical equipment production*, REUTERS (Mar. 18, 2020), located at https://www.reuters.com/article/us-health-coronavirus-gm-equipment/gm-ford-in-talks-with-trump-administration-on-medical-equipment-production-idUSKBN2153W5; Jeffery Martin, *Trump Signs Emergency Bill to Make Companies Manufacture Medical Supplies to Fight Coronavirus*, NEWSWEEK (Mar. 18, 2020), located at https://www.newsweek.com/trump-signs-emergency-bill-make-companies-manufacture-medical-supplies-fight-coronavirus-1493142; Jeremy B. White, *Newsom says California enlisting Elon Musk, Tim Cook for coronavirus help*, POLITICO (Mar. 21, 2020), located at https://www.politico.com/states/california/story/2020/03/21/newsom-says-california-enlisting-elon-musk-tim-cook-for-coronavirus-help-1268647; Arjun Kharpal, *US tech CEOs from Tim Cook to Elon Musk pledge to help coronavirus fight with masks and ventilators,* CNBC (Mar. 23, 2020), located at https://www.cnbc.com/2020/03/23/coronavirus-apple-ceo-tim-cook-teslas-elon-musk-pledge-donations.html.

[8] UK ICO, *Data protection and coronavirus: what you need to know*, located at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/covid-19-general-data-protection-advice-for-data-controllers/. In response to a question asking if the regulator would take action against companies for conduct during the pandemic, the UK ICO wrote: "No. We understand that resources, whether they are finances or people, might be diverted away from usual compliance or information governance work. We won't penalise organisations that we know need to prioritise other areas or adapt their usual approach during this extraordinary period."

[9] Roland Li, *Coronavirus closes many Bay Area hotels: 'Worse than 9/11 or 2008'*, SAN FRANCISCO CHRONICLE (Mar. 19, 2020), located at https://www.sfchronicle.com/business/article/Coronavirus-puts-San-Francisco-s-hotels-in-15141953.php?cmpid=gsa-sfgate-result; Ali Wunderman, *How to keep restaurants afloat amidst the coronavirus lockdown,* SFGATE (Mar. 21, 2020), located at https://www.sfgate.com/food/article/restaurants-bars-help-coronavirus-gift-cards-merch-15138978.php.

will be particularly impacted by the economic impacts of the health crisis.[10] A forbearance in enforcement would provide much needed time for businesses to continue to bring their operations into compliance with the regulations once the health emergency is under control.

Although companies have already taken steps to facilitate compliance, the lack of finalized regulations has left our members and thousands of other California businesses uncertain concerning their ultimate obligations. On March 11, 2020, your office released a third iteration of the draft rules, thereby updating the regulatory scheme with new nuances that now need to be built into already-existing compliance strategies.[11] Continuing to change the regulations so close to the law's enforcement date of July 1, 2020 will make it difficult if not impossible for businesses to conform their new procedures to the final rules by July 1, 2020. Furthermore, the rules will not be final until they are approved the California Office of Administrative Law, which adds to the increasingly likely possibility that the draft rules will become effective only a short time before your office could commence enforcement. W310-1 cont.

The CCPA is a first-of-its-kind, complex statute that has imposed entirely new requirements on businesses and has caused them to incur significant costs. The CCPA suggests that the CA AG may begin enforcing the law on July 1, 2020, but your office has discretion to provide a reasonable period of additional time for businesses to understand and implement the final rules before you start bringing enforcement actions. We therefore respectfully ask you to postpone your enforcement efforts until January 2, 2021. This limited deferral will give businesses the time they need to understand and effectively implement the final rules and will help lessen the blow to the economy caused by the coronavirus outbreak.

II. Clarify Financial Incentive Terms to Enable the Continued Existence of Loyalty Programs

Guidance provided on financial incentive terms remains unclear.[12] According to the draft rules, businesses that offer "financial incentives" or "price or service differences" related to the collection, retention, or sale of personal information must ensure that such incentives and differences are "reasonably related to the value of the consumer's data."[13] Additionally, businesses must disclose "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 used" to calculate such value.[14] As articulated in the proposed modified regulations, businesses that do not adequately comply with these requirements may not offer financial W310-2

[10] The economic impact study the CA AG completed on the impacts of the CCPA regulations indicate that small businesses will incur $50,000 in compliance costs in getting ready for the CCPA. In the best of times that would be crippling to cash strapped small business. Given today's realities, it is a death sentence for small businesses owners and its employees. *See* State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* at 10 (August 2019), located at http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/CCPA_Regulations-SRIA-DOF.pdf (hereinafter "*SRIA*").

[11] *See Notice,* supra note 1.

[12] Cal. Code Regs. tit. 11, §§ 999.336, 337 (proposed Mar. 11, 2020).

[13] *Id.* at §§ 999.301(j), (o); 336(b).

[14] *Id.* at § 999.307(b)(5).

incentives or price or service differences to consumers.[15] The unclear nature of these burdensome rules coupled with significant confusion regarding how businesses must operationalize them could force many entities to stop offering loyalty and rewards programs to California consumers altogether. We therefore ask the CA AG to clarify or remove the draft rules' ambiguous financial incentive and price or service difference terms to ensure Californians may continue to receive the benefits of the loyalty and rewards programs they enjoy, value, and expect.

Brands and marketers offer various loyalty and rewards programs to California consumers, such as clothing VIP points programs, tiered ride-sharing programs, grocery rewards, credit card cash back benefits, and myriad others. Consumers have long enjoyed participating in these programs because they receive offers and better deals for the products and services that are most relevant and important to them. Businesses also have benefited from the loyalty, brand trust, and word-of-mouth marketing they accumulate through consumers' participation in these programs. The draft rules could impede or completely eradicate the existence of loyalty and rewards programs in California due to their requirements to tie the "value of the consumer's data" to the financial incentive or price or service difference offered to consumers. It is consequently extremely important for the CA AG to clarify the draft rules' uncertain financial incentive and price or service difference terms so Californians can have the same access to loyalty programs as consumers residing in other states.

W310-2 cont.

The proposed rules offer nearly no information about how a business may show that a price or service difference offered through a loyalty or rewards program is "reasonably related to the value of a consumer's data." Notably, there is no reference in the draft rules to how a business can account for the value it receives in fostering goodwill and consumer loyalty for a brand. This intangible value is difficult if not impossible to quantify, so, showing a direct relationship between a financial incentive and this value in numerical terms might be an unachievable task. Moreover, the value a business attributes to personal information associated with a consumer might vary from situation to situation. Such value might depend, for example, on the particular discount offered at a specific time or in a specific place.

Adding to the confusion is the fact that businesses might offer several different financial incentives or price or service differences to consumers through loyalty and rewards programs at one time. For example, a grocery store might offer consumers discounts through a loyalty card when the consumer signs up for the card with the store. By signing up for the program, consumers might receive discounts on select food items and beverages when they shop. Simultaneously, the very same grocery store might offer consumers a loyalty program that takes the form of a sweepstakes, providing consumers with necessary pieces to complete the game as they make continuous purchases at the store. It is unclear how the grocery store could show that both the loyalty card and the game are "reasonably related to the value of the consumer's data," especially if "the value of the consumer's data" is to remain a constant number. The draft rules are unclear on this point, and they could consequently cause businesses to stop offering loyalty programs in California due to confusion in regard to how to follow the proposed regulations' mandates. Given the vagueness of the terms and requirements, we do not see how the CA AG

[15] *Id.* at § 999.336(b).

could enforce these requirements consistent with constitutional requirements of fair notice and due process. W310-2 cont.

The revised proposed rules also require businesses to provide a "notice of financial incentive" for each incentive or price or service difference offered that discloses an estimate of "the value of the consumer's data" and the method of calculating that value.[16] Requiring a business to make such disclosures could reveal business trade secrets and proprietary information that could jeopardize the business's competitive position in the marketplace. Forcing businesses to reveal their confidential, internal valuations and methods of calculating such value in this way could detrimentally impact competition and risk the exposure of protected business proprietary information. Revealing such data would also provide little to no value to consumers, as the required disclosures would be meaningless from a consumer's point of view. Moreover, consumers would be overwhelmed and inundated with an excessive number of financial incentive notices, as businesses typically offer several incentives to consumers at one time. Consumers would therefore likely not digest or understand meaningful information about business practices by receiving such notices. Finally, compelling the surrender of legally protected, highly proprietary information could raise numerous constitutional problems, ranging from a regulatory taking to dormant Commerce Clause issues given the negative impact on interstate commerce. W310-3

For the foregoing reasons, we urge the CA AG to clarify or remove the unreasonably onerous price or service difference and financial incentive terms in the proposed rules. In particular, we ask the CA AG to remove or clarify the provisions requiring businesses to disclose an estimate of "the value of consumer data," the method of calculating such value, and ensure that financial incentives offered through loyalty and rewards programs are reasonably related to "the value of the consumer's data." We also request that clarification be given to ensure that businesses are not required to disclose internal data, calculations, and inferences. Without such clarification and corrections, these requirements are exceptionally onerous if not impossible for businesses to implement and could result in the end of loyalty programs in California. W310-2 cont. W310-3 cont.

III. Allow Businesses to Choose to Honor Global Privacy Controls *or* Offer Another, Equally Effective Method for Consumers to Opt Out of Personal Information Sale

According to the draft rules, a business that collects personal information from consumers online must "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 to opt out of sales.[17] This requirement raises constitutional concerns, as it is wholly divorced from the text of the CCPA itself, is an arbitrary and capricious exercise of the CA AG's authority to issue regulations according to law, and impinges on constitutionally protected speech under the First Amendment to the United States Constitution and Article I, Section 2(a) to the California Constitution. The requirement will also impede consumer choice and the digital economy by casting a single, default opt-out signal to all entities in the online marketplace instead of enabling consumers to W310-4

[16] *Id.* at § 999.307(b)(5).
[17] *Id.* at § 999.315(d).

make individualized, business by business selections about which entities may and may not sell personal information as the law requires. The requirement consequently violates both constitutional rights as well as consumers' rights to exercise robust and specific choices in the marketplace.

Instead of instituting a blanket requirement for businesses to honor browser signals and privacy controls, we ask the CA AG to clarify that businesses *may* honor global privacy controls *or* offer consumers another, equally effective method of opting out of personal information sale. This clarification would avoid the constitutional concerns inherent in the requirement and would better enable businesses to abide by consumers' expressed choices. It would also prevent intermediaries from setting default signals that do not align with consumer preferences.

A. The Draft Rules' Browser Mandate Exceeds the CA AG's Authority and Raises Serious Constitutional Concerns

The draft rules have instituted an entirely new requirement for businesses to honor browser signals and global privacy controls that is nowhere present in the text of the CCPA. This requirement is arbitrary and capricious, exceeds the scope of the CCPA, falls outside of the CA AG's authority to issue regulations as set forth in Section 1798.185 of the law, and impedes free speech as protected by the First Amendment to the United States Constitution and Article I, Section 2(a) to the California Constitution.[18] Businesses have had no meaningful opportunity to anticipate or prepare for this brand-new obligation, and it represents a broadly applicable rule that does not advance the state's interest in protecting consumer privacy. We therefore request that this requirement be removed from the regulations or that your office alternatively adopt a less restrictive means to effectuating consumer choice.

W310-4 cont.

1. The Browser Mandate Contradicts the Text of the CCPA and Therefore Exceeds the CA AG's Authority

In passing the CCPA, the California Legislature purposefully did not include a mandate to respect default signals set by browsers that send a single opt-out signal to the entire Internet ecosystem. The CA AG's proposed regulation requiring businesses to respect global privacy controls set through browsers effectively turns the CCPA's opt-out regime into an opt-in regime. The present text of the draft rules empowers browsers and other intermediaries to set such signals by default, allowing for opt-out signals to be sent to businesses even if they do not align with consumers' actual preferences or desires. Upon the receipt of such a default global opt-out signal through a browser, businesses will be forced to contact consumers directly to ascertain whether such consumers would like to opt-in to sales of personal information. This structure thwarts legislative intent by converting the opt-out right in the CCPA into an opt-in system.

The Legislature specifically created a right for consumers to opt out of personal information sales, enabling consumers to submit granular choices directly to businesses rather

[18] As Professor Grodin has commented, "California may have broader protection for commercial speech than the First Amendment provides, at least as to compelled speech." Joseph R. Grodin, *Freedom of Expression under the California Constitution*, 6 *California Legal History* 214 (2011), available at http://repository.uchastings.edu/faculty_scholarship/1067.

than requiring a single online signal to trump all other signals set in the marketplace.[19] It was not the goal of the Legislature to force consumers to opt in to every business's sale of personal information associated with them. Under California administrative law, when an agency is delegated rulemaking power, rules promulgated pursuant to that power must be "within the lawmaking authority delegated by the Legislature," and must be "reasonably necessary to implement the purposes" of the delegating statute.[20] More than five years ago, when it amended the California Online Privacy Protection Act, the California Legislature considered global privacy controls and elected to refrain from enshrining them into law.[21] The CCPA similarly took the approach of refraining from requiring businesses to honor global browser settings or privacy controls. The CA AG was empowered by statute only to "adopt regulations to further the purposes of [the CCPA]."[22] Thus, as the CCPA does not authorize or contemplate an opt-in regime, the CA AG lacks statutory authority to promulgate the browser mandate.

W310-4 cont.

By imposing a *de facto* opt-in regime that the California Legislature has previously rejected and again declined to adopt in the CCPA, the draft regulation would usurp legislative authority and violate the separation of powers required by the California Constitution.[23] Transforming the legislative directive for an opt-out system to an opt-in system is not within the scope of the delegated legislative authority, nor is it reasonably necessary to implement the CCPA, nor is it a reasonable interpretation of the CCPA's terms.[24] It therefore violates multiple aspects of the separation-of-powers doctrine.[25]

2. The CA AG's Economic Impact Analysis Neglected to Consider the Unique Impacts of the Browser Mandate

W310-5

The CA AG failed to comply with California's Administrative Procedure Act ("APA") when it neglected to consider the unique economic costs associated with the browser mandate at the initial proposal stage. Agencies are required by law to consider the economic impacts of proposed regulations prior to submission.[26] The CA AG's economic impact assessment did not separately consider the effective opt-in regime created by the browser mandate, which will prevent regulated businesses from selling data from a class of consumers who have not expressed specific data-sharing preferences.[27] It also did not consider the costs consumers could incur from default opt-out signals expressed through browsers without their express permission or buy-in.

---

[19] Cal. Civ. Code § 1798.120.

[20] *Western States Petroleum Assn. v. Bd. of Equalization*, 304 P.3d 188, 415 (Cal. 2013) (quoting *Yamaha Corp. of America v. State Bd. Of Equalization*, 960 P.2d 1031 (Cal. 1998)).

[21] *See Assembly Committee on Business, Professions and Consumer Protection*, Hearing Report on AB 370 (Apr. 16, 2013), located at https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201320140AB370# ("According to the California Attorney General's Office, 'AB 370 is a transparency proposal – not a Do Not Track proposal. When a privacy policy discloses whether or not an operator honors a Do Not Track signal from a browser, individuals may make informed decisions about their use of the site or service.'")

[22] Cal. Civ. Code § 1798.185.

[23] Cal. Const. Article III, Section 3 ("The powers of state government are legislative, executive, and judicial. Persons charged with the exercise of one power may not exercise either of the others except as permitted by this Constitution.").

[24] *See Yamaha Corp. v. State Bd. of Equalization*, 19 Cal. 4th 1, 6 (1998).

[25] *See id.*

[26] Cal. Gov. Code § 11346.3(a)(2).

[27] *SRIA*, supra note 10.

Thus, the impact analysis erroneously counted as a benefit what should have been counted as a cost—loss of value to consumers when opt-out signals are cast without their permission, and lost revenue for businesses that otherwise would have been able to sell personal information about parties who do not oppose the sale of personal information and thus derive no benefit from this prohibition. A substantial failure to comply with the APA is grounds for a regulation's invalidation,[28] and California courts have invalidated regulations in cases where an agency's economic impact analysis was "materially deficient."[29] We therefore urge the CA AG to either reexamine the economic impacts of the browser mandate or remove it from the final regulation.

W310-5 cont.

3. The Browser Mandate Violates the First Amendment

By turning the opt-out regime into an opt-in regime through the requirement to honor global privacy controls set through browsers, the CA AG's proposal violates the First Amendment to the United States Constitution, as applied to California through the Fourteenth Amendment, and Section 2(a) to the Declaration of Rights within the California Constitution (Article I). The dissemination of data collected by a business is constitutionally protected commercial speech.[30] In order for a regulation restricting commercial speech to pass constitutional muster, (1) the state must assert a substantial interest in restricting this speech, (2) the regulation must directly advance that interest, and (3) the regulation must be narrowly tailored to serve that interest.[31] There is a substantial state interest in the protection of consumer privacy in business relationships.[32] But, this proposal neither directly advances a substantial governmental interest, nor is it narrowly tailored to advance such an interest. Therefore, it violates the First Amendment and Art. 1, Sec. 2(a).

W310-4 cont.

Regulations that provide only "'ineffective or remote support for the government's purpose'" do not satisfy the constitutional protections afforded to commercial speech.[33] As is further explained below, forcing businesses to defer to global privacy controls is less effective and less direct than the opt-out methods employed by the rest of the CA AG's regulations. The comprehensive opt-out system devised by the CA AG and the California Legislature directly addresses a consumer's relationship with an individual business, allowing consumers to express their privacy preferences in the context of their unique relationships with individual entities. The global privacy controls proposal, on the other hand, requires businesses to infer nuanced attitudes toward data disclosure from a one-size-fits-all device setting. Thus, if the State's interest is in preventing the spread of specific data that a consumer wishes to withhold, the global privacy controls proposal falls short—it provides no indication that a consumer desires to withhold information particular to a specific business relationship, instead forcing businesses to infer

---

[28] *Western States Petroleum Assn. v. Bd. of Equalization*, 304 P.3d 188, 203 (Cal. 2013).
[29] *See, e.g., John R. Lawson Rock & Oil, Inc. v. State Air Resources Bd.*, 20 Cal. App. 5th 77 (Cal. App. 5th 2018).
[30] *See Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001); *Boetler v. Advance Magazine Publishers Inc.*, 210 F. Supp. 3d 579, 597 (S.D.N.Y. 2016).
[31] *Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001).
[32] *Verizon Northwest, Inc. v. Showalter*, 282 F. Supp. 2d 1187, 1192 (W.D. Wash.).
[33] *Id.* (quoting *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980)).

disclosure preferences from a remote and indirect signal which might not accurately reflect a consumer's attitude towards the data at issue in a given transaction.

Moreover, the proposal is not narrowly tailored to serve the state's interest; it needlessly restricts the commercial speech of regulated businesses without bolstering the effectiveness of the existing opt-out framework. In order to be narrowly tailored, a regulation must not be disproportionately burdensome and must "signify a careful calculation of the costs and benefits associated with the burden on speech imposed."[34] The existing opt-out regime provides businesses with precise information about the informed preferences of individual consumers. The global privacy controls rule, though serving no additional purpose not already served by the opt-out rules, has the potential to restrict speech by requiring businesses to defer to potentially inaccurate information about a consumer's individual preferences. Section 999.315(d)(2) of the CA AG's proposed regulation provides that, if global privacy controls conflict with the individual user preferences logged into a business's privacy settings, a business must defer to the global privacy controls by default or must seek out separate approval from the consumer. Thus, businesses are required by default to defer to a general and imprecise expression of user preference at the expense of specifically expressed preferences, and businesses must bear the cost of clearing up these indeterminacies. The standard opt-out regime is both more precise and less burdensome, as it allows businesses to assess the specific preferences of users in the context of each unique consumer relationship and restricts commercial speech only inasmuch as that speech is known to interfere with consumer preferences. W310-4 cont.

The global privacy controls rule does nothing to enhance the existing opt-out regime, while needlessly restricting speech. Thus, the global privacy controls rule unconstitutionally imposes burdens on commercial speech without offsetting those burdens with benefits.

B. The Browser Mandate Hinders Consumer Choice and Allows Intermediaries to Block Consumer Preferences

As we have explained in prior submissions, the unprecedented requirement to honor global privacy settings and browser controls does not further the purposes of the CCPA. Instead, it threatens to impede consumers' ability to make choices about specific entities that can and cannot sell personal information. Because global privacy controls cast a single opt-out signal to every business across the entire Internet ecosystem, the ability to make granular choices that the California Legislature meant to confer on consumers would be rendered nonexistent.

Additionally, such a requirement would be poised for intermediary tampering, as businesses would have no way to verify whether a signal is a genuine consumer-set preference. In the March 11, 2020 second set of modifications to the draft rules, the CA AG removed the requirement for consumers to "affirmatively select" such browser signals or privacy controls to clearly indicate a choice to opt out.[35] The CA AG also removed a provision stating that "[t]he privacy control… shall not be designated with any pre-selected settings."[36] The result of striking these important terms is that intermediaries will be able to set *default* opt-out signals through W310-6

[34] *Id.* at 1194.
[35] *Compare* Cal. Code Regs. tit. 11, § 999.315(d)(1) (proposed Feb. 10, 2020) *with* Cal. Code Regs. tit. 11, § 999.315(d)(1) (proposed Mar. 11, 2020).
[36] *Id.*

browsers that may have absolutely no connection to a consumer's actual preferences. The proposed regulations therefore take choice away from consumers by inserting the choice of intermediaries in place of those consumers. In departing so far from the legislative intent, the requirement would be arbitrary and capricious.

W310-6 cont.

C. The Draft Rules Offer No Clarity Regarding How Conflicting Privacy Controls or Signals Should Be Managed

It also is unclear in the most recent draft how default browser signals should interact with a consumer's previously expressed desire to allow a business to sell personal information. If, for example, a consumer has enabled an individual business to sell personal information, a browser's subsequent institution of a default global opt out would cut directly against the choice the consumer expressed directly to the business. Any subsequently instituted default global privacy control would effectively block the particularized choice that the consumer set with the individual business. The requirement to honor browser signals and global privacy controls would allow intermediaries to interfere with consumers' individual choices by using cookies, plugins, JavaScript and other technologies to set a single signal to the marketplace. Consumer preferences cannot be respected if such interference is permitted. As a result, the obligation to honor browser signals and global privacy controls coupled with intermediaries' capability to set such controls by default has the potential to obstruct consumers' expressed choices.

W310-4 cont.

Additionally, the browser signal requirement advantages consumer-facing businesses over others in the marketplace and entrenches incumbents who regularly interface with consumers. Third party entities, for example, might not have a direct touchpoint with consumers through which they could ascertain whether a consumer intends to opt in or opt out of personal information sale. Moreover, it is not clear how, or at what frequency, companies would be able to communicate with consumers in regard to default privacy settings. Businesses would be forced to ask consumers to opt in to the sale of personal information every time the consumer interacts with that business. However, the CCPA limits a business's ability to seek "opt-in" consent to once every twelve months.[37] The lack of clarity on this issue will impede the expression of consumers' actual choices and will hinder their ability to express preferences in the marketplace.

D. The CA AG Should Amend its Approach To Browser Settings So It Is Less Restrictive and So It Passes Constitutional Muster

Instead of requiring businesses to honor browser settings and global privacy controls, the CA AG should update the draft rules to allow 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 is a better approach that will enable consumers to express individualized choices about specific entities' use of data. This approach would also avoid the constitutional concerns inherent in the browser signal requirement. There is no privacy-enhancing reason to require businesses to respect user-enabled privacy controls over choice provided by a business. Updating the draft

[37] Cal. Civ. Code § 1798.135(a)(5).

rules to give businesses the ability to respect such controls or offer another, equally effective opt-out mechanism would allow consumers to make granular opt-out choices instead of concentrating control and power in the hands of intermediaries such as browsers.

IV. Clarify that Internally-Generated Inferences and Derived Data Are Not Subject to a Consumer Request to Know

In the course of developing the draft rules, the CA AG helpfully aligned the regulations with the text of the CCPA by clarifying that a "request to know" means a consumer request that a business disclose personal information that it has *collected* about the consumer, including the specific pieces of personal information *collected* about the consumer.[38] The draft rules do not, however, state whether internally-generated data, such as inferences and derived data, must be returned in response to a consumer request to know. We ask the CA AG to issue additional updates to the draft rules to clarify that internally-generated inferences and derived data need not be returned in response to a consumer request to access specific pieces of personal information because such data is not collected.

For most businesses, providing access to personal information is both an important and costly aspect of complying with the CCPA. Providing access presents challenges because many businesses do not maintain information about an individual in a centralized way, so complying with access requests often involves a manual process of searching through various storage locations to build a centralized collection of data that can be provided to a consumer. Additionally, in today's day and age, nearly every entity processes information about individuals in some manner and generates internal data, like internal inferences, that would be both time-consuming to collect and of little privacy value to consumers. Against this backdrop, it is critical that businesses have clarity around what data should be disclosed under CCPA. The draft rules should require a business to return to the consumer the specific pieces of personal information it has collected about the consumer, but not the personal information it independently generated or derived from such data. This approach reflects a logical reading of the law and aligns with consumer expectations as to the types of data that could be "collected" from and sold about them. W310-7

This interpretation also protects the intellectual property of businesses in their inferences and provides clear guidance that allows them to practically provide information about consumers that is readily understandable. Significantly, a broader interpretation that would require the disclosure of inferences or decisions made tied to a consumer would in many cases infringe on the intellectual property of businesses. Companies compete on providing consumers with the best consumer experience, including through pricing, customer support, product offering scope, and many other factors. In the digital age, consumer experience is driven by trade secrets regarding computing and efficiencies. The CCPA specifically recognizes and enumerates that information that amounts to intellectual property or a business's trade secrets should be exempt from the law. The statute instructs your office to "establish… any exceptions necessary to comply with state or federal law, including but not limited to those relating to trade secrets and intellectual property rights."[39]

---

[38] Cal. Civ. Code § 1798.110(a)(1); *see also* Cal. Code Regs. tit. 11, § 999.301(q) (proposed Mar. 11, 2020).
[39] Cal. Civ. Code § 1798.185(a)(3).

Pursuant to Section 1798.110 of the CCPA and the draft regulations, a consumer may request that a business disclose to them personal information that the business has collected about the consumer.[40] The final rules should clarify that the duty to disclose information that a business collects does not apply to *internally-generated* data such that business are not required to disclose such data in response to a consumer access request for specific pieces of personal information. Such information was not "collected" consistent with the law's definition of the term. However, this is distinguishable from instances where a business receives or buys inferred data from another entity. In such cases the business *has* collected this data and would be subject to a verified consumer access request.[41] Additionally, if a business sells its proprietary inferences to a third party or discloses such inferences for a business purpose, the business would disclose that it has sold and/or disclosed the category of "inferences" pursuant to the CCPA requirement to provide the categories of personal information that the business sold and disclosed about the consumer for a business purpose.[42] This reading of the CCPA is supported by the text of the law itself as well as your office's recent revisions to the regulations implementing the CCPA.

Compelled disclosure of proprietary information would have significant legal consequences. Not only would it exceed the scope of the legislative delegation (and thus implicate separation of powers), it also could constitute a regulatory taking prohibited by the Fourteenth Amendment to the U.S. Constitution and Article 1, Sections 1, 7(a). 15, and 19(a) to the California Constitution. Inasmuch as it would have substantial effects on interstate commerce, it also could violate the dormant Commerce Clause, Article 1, Section 8 to the U.S. Constitution.

W310-7 cont.

The CCPA appropriately limited the scope of the access obligations to "collected" data to avoid imposing undue burden on California businesses and ensure the data provided to consumers is meaningful and intelligible. If the CCPA were to require businesses to return *all* generated data, including inferences in response to a consumer access request, consumers would be burdened by the delivery of excessively detailed and potentially incomprehensible information, including internally-generated inferences—basic computing connections, like validating a name, that businesses must undertake in order to sustain day-to-day operations. Businesses ultimately would have difficulty or impossibility in complying. A business's provision of this data to a consumer would hinder the consumer's ability to access meaningful information about the information collected from or about the consumer, thereby thwarting the aim of the CCPA to provide consumers with enhanced transparency. For these reasons, ANA urges the CA AG to update the draft rules to clarify that a business should return to a consumer the specific pieces of personal information it has *collected* about the consumer, but not the personal information it independently generated, inferred, or derived from such data.

V. Provide Flexibility for Offering Opt-Out Mechanisms

[40] *Id.* at § 1798.110(a)(5).
[41] *Id.*
[42] *Id.* at §§ 1798.115(a)(2)-(3).

In the March 11, 2020 updates to the draft rules, the CA AG modified the proposed regulations to state that a business shall not utilize an opt-out method "that is designed with the purpose or *has the* substantial effect of subverting or impairing a consumer's decision to opt-out." We respectfully ask the CA AG to restore the previous language in this requirement. Reverting to the prior language will better provide businesses with flexibility for offering opt-out mechanisms to consumers and will reduce the likelihood that businesses could be punished for effects of opt-out mechanisms they do not intend or reasonably expect.

Prohibiting businesses from using opt-out methods that have the substantial effect of impairing a consumer's decision to opt out will disincentivize businesses from creating innovative methods for consumers to opt out of personal information sale. This language provides no leeway for businesses to design new opt-out mechanisms that could make opt-outs easier or substantially less burdensome for consumers to submit. Moreover, businesses will not know which opt-out mechanisms would have the effect of impairing a consumer's decision to opt out until those mechanisms are appropriately vetted. Businesses should be prohibited from designing methods that have the *purpose* of subverting a consumer's decision to opt out, but they should not be held accountable for potential effects they did not reasonably anticipate or set out to achieve. As a result, we ask the CA AG to restore the previous language in the draft rules that prohibited businesses from designing opt-out mechanisms with the purpose of subverting or impairing a consumer's request to opt out. This change will give businesses needed flexibility to develop new and useful opt-out mechanisms and help ensure that they are not penalized for results they did not intend. W310-8

VI. Enable Flexibility for Providing the CCPA-Required Notice at Collection to Consumers Through the Telephone and in Person

The second set of modifications to 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.[43] 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. W310-9

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.

[43] Cal. Code Regs. tit. 11, § 999.305(a)(3)(d) (proposed Mar. 11, 2020).

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. W310-9 cont.

VII. Clarify That Qualifying Businesses Must Provide Additional Metrics Beginning in 2021

According to the draft rules, "[a] business that knows or reasonably should know that it, 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," must make certain disclosures regarding the number of CCPA requests received and answered annually.[44] The proposed regulations would require qualifying businesses to make such disclosures online "by July 1 of every calendar year."[45] Given the fact that the draft rules are still not final as well as the quickly shrinking period of time before July 1, 2020, we ask the CA AG to update the draft regulations so applicable businesses must make such disclosures "by July 1 of every calendar year *beginning in 2021*." W310-10

Should the requirement to provide such disclosures by "July 1 of every calendar year" remain in the text of the draft rules, the regulations could be read to require businesses to provide such disclosures by July 1, 2020. As a result, qualifying businesses would have to scramble to gather the mandated metrics within a few short weeks after the requirement to make such disclosures becomes effective. If the CCPA regulations become final in April or later, there will be very little time to compile such information. Additionally, the numbers that businesses may be able to provide by July 1, 2020 will not reflect annualized information because the CCPA went into effect just six months prior. We respectfully request that the CA AG add clarifying language stating that applicable businesses must provide the disclosures "by July 1 of every calendar year beginning in July 2021" so that businesses will have enough time to compile accurate information and so the numbers reflect annual figures rather than figures for the prior six-month period.

* * *

Thank you for the opportunity to submit comments on the second set of modifications to the proposed regulations implementing the CCPA. Please do not hesitate to contact us with any questions you may have regarding this submission.

---

[44] *Id.* at § 999.317(g)(1).
[45] *Id.* at § 999.317(g)(2).

Message

From: [redacted]
on behalf of Katie Kennedy [redacted]
Sent: 3/27/2020 4:39:34 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Apple Inc Comments to the California Department of Justice re CCPA
Attachments: Apple Inc Comments to California Department of Jusice re CCPA Regulations March 2020.pdf

To Whom It May Concern:

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

Thank you,

Katie

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

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

Apple believes that privacy is a fundamental human right, and we greatly appreciate the extensive work that the Attorney General's office has put towards drafting regulations to implement the California Consumer Privacy Act. The regulations will play a critical role in protecting consumer privacy, and we thank the Attorney General's office for its ongoing commitment to drafting clear guidance that implements robust protections for consumers.

We agree with many provisions of the draft regulations and respectfully offer comments on two issues where the Attorney General has the power to make revisions that would further protect consumers, clarify unnecessary ambiguities in the text, and encourage the development of privacy-protective and consumer-friendly practices.

First, the most recent revisions to the definitions of "financial incentive" and "price or service difference" appear to have drastically expanded the scope of those terms, and, may have resulted in the transformation of nearly any program or service that involves the collection or retention of personal information into a "financial incentive." We believe that applying the financial incentive obligations to any program or offering that involves the collection and retention of personal information will result in a flood of notices to consumers, consent fatigue, and confusion over what is truly a request for certain processing of personal information in exchange for compensation. W311-1 W311-2

Second, while Apple supports the use of the various agent request verification methods set out in the regulations, we urge the Attorney General to clarify that businesses may innovate in this space and develop their own robust procedures for verifying the authenticity of CCPA requests made by authorized agents. As a company that strives to provide the highest protections for consumers' information, we see the continually evolving strategies that bad actors use in an attempt to gain unauthorized access to personal information. Given that bad actors will develop increasingly sophisticated methods for submitting fraudulent agent requests, it is important for businesses to have the Attorney General's support as they develop new mechanisms to identify and deny fraudulent agent requests and stay a step ahead of bad actors. W311-3 W311-4

We thank you for this opportunity to provide comments on these regulations.

The Attorney General should revise the definitions of "financial incentive" and "price or service difference" to ensure that they provide meaningful data privacy transparency and control to California residents. W311-1 cont. W311-2 cont.

Apple supports the Attorney General's effort to clarify the meaning of the financial incentive provisions of the CCPA. However, we are concerned that recent revisions to the proposed regulation's definitions of "financial incentive" and "price or service difference" will undermine the intended purpose of these provisions and ultimately harm California residents. Significantly

Apple
One Apple Park Way
Cupertino, CA 95014



expanding the application of these terms beyond their intended scope, as currently proposed, would create confusion by blurring the lines between actual financial incentive programs (e.g., programs where a business offers a benefit in exchange for the consumer allowing the sale of their personal information) and programs and services that simply require the collection of necessary personal information for operational purposes in order to deliver a service requested by a user. Therefore, we encourage the Attorney General to revise further the definitions for "financial incentive" and "price or service difference," as discussed below.

W311-1 cont. W311-2 cont.

For context, the key changes that expanded the proposed scope of "financial incentive" are (1) the replacement of "as compensation, for" with "related to," and (2) the replacement of "disclosure, deletion" with "collection, retention."

W311-1 cont.

> Section 999.301(j) (j) (g) "Financial incentive" means a program, benefit, or other offering, including payments to consumers, related to ~~as compensation, for~~ the collection, retention ~~disclosure, deletion~~, or sale of personal information.

Similarly, the changes that have expanded the scope of "price or service difference" are (1) the addition of "related to," and (2) the replacement of "disclosure, deletion" with "collection, retention."

W311-2 cont.

> Section 999.301(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 collection, retention, ~~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 collection, retention, ~~disclosure, deletion,~~ or sale of personal information, including the denial of goods or services to the consumer.

If the current proposed "financial incentive" and "price or service difference" definitions are not revised further, any program or offering that is "related to" the "collection" or "retention" of personal information would seem to qualify as a "financial incentive." The current definitions could be read to encompass nearly any program or offering that involves the collection of any amount of personal information, including programs or services built with privacy very much in mind and for which businesses need to collect personal information to operate the service, but do not seek to otherwise derive value from it. For example, a business may offer an email-based service and require that consumers provide their name as part of the registration process. Even if the business uses the registered user's personal information solely for the purpose of providing the service, such a program could arguably qualify as a "financial incentive" under the current proposed definition. As another example, a small app developer could be viewed as offering a "financial incentive" because it offers a benefit (i.e., the services) to consumers that is "related to" the collection of personal information (i.e., the consumer's name, shipping information, and billing information), even though the personal information is used solely for billing and shipping purposes.

W311-1 cont. W311-2 cont.

Additionally, these hypothetical services might also involve a "price or service difference" given that a consumer who declines to provide their name would be denied the service because the business cannot maintain an account for the person without having a name to associate with the account. Such a denial could be viewed as being "related to" the "collection" of personal information.

The overbroad proposed definitions of "financial incentive" and "price or service difference" would ultimately reduce transparency, contrary to the consumer interests that the CCPA's financial incentive provisions were intended to protect. For example, because the CCPA requires that consumers provide opt-in consent to participate in a financial incentive program, if the overbroad definitions prevail, consumers will be flooded with notices describing financial incentives and requests for their opt-in consent to participate in any service or program that involves a business's collection or retention of their personal information. If consumers come to view nearly all programs and collections of personal information as "financial incentives" that require opt-in consent, they may develop consent fatigue and be less likely to scrutinize true financial incentives or exercise their right to withdraw consent to such programs.

W311-1 cont.
W311-2 cont.

Given the problems posed by the recent revisions to the "financial incentive" and "price or service difference" terms, we urge the Attorney General to revise these definitions further in a way that aligns them with the text and history of the CCPA and ensures that the financial incentive obligations remain focused on providing meaningful transparency and control to consumers.

Example Revisions

"Financial incentive" means a program, benefit, or other offering, including payments to consumers, ~~related to~~ that is provided as compensation in exchange for the collection, retention, or sale of personal information. For clarity, a business's provision of a good or service that reasonably requires the collection or retention of personal information to provide the good or service to the consumer shall not by itself be sufficient to qualify as a financial incentive.

W311-1 cont.

"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 collection, retention, 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 collection, retention, or sale of personal information, including the denial of goods or services to the consumer. This term does not include price or service differences that are caused in whole or in part by a consumer's decision to not allow the collection or retention of personal information that is reasonably required for the provision of a good or service to a consumer.

W311-2 cont.



The Attorney General should confirm that businesses are allowed to rely on other reasonable methods for confirming the authenticity of agent authorizations.

We support the Attorney General's decision to provide businesses with a number of different methods for confirming the authenticity of CCPA requests from agents. However, given the rapid pace of technological change, we encourage the Attorney General to clarify and confirm that businesses have the flexibility to establish their own reasonable procedures for verifying and confirming the authenticity of requests from agents.

Under section 999.326(a), a business that receives an access or deletion request from an agent is allowed to require the consumer to take one or more of three different steps to confirm that the consumer has actually authorized the request: (1) require the consumer provide signed permission to the agent; (2) require the consumer to verify their identity directly with the business; and (3) require the consumer to directly confirm with the business that they authorized the agent to submit the request. Additionally, section 999.326(c) grants a business the ability to deny an agent's access or deletion request if the agent does not submit proof of authorization to act for the consumer. Similarly, section 999.315(g) allows a business to deny an agent's opt-out request if the agent does not submit proof of authorization to act for the consumer.

W311-3 cont.
W311-4 cont.

While these procedures can provide reasonable assurance of an agent's authorization in some circumstances, the regulations should also protect consumers by supporting the ability of businesses to develop new and potentially more secure methods for verifying the authenticity of agent requests. For example, some businesses may develop the capability to analyze metadata associated with an agent's request and determine if it is likely being made by a known bad actor. In such cases, the regulations should not prevent a business from using that technology and denying the fraudulent request, even if the bad actor is able to pass some of the other authentication mechanisms that are permitted under the current text of the regulations (e.g., the bad actor may have hacked the consumer's email account and therefore be able to respond to an email from the business requesting confirmation of the agent's authorization).

To ensure that businesses are able to continue to develop and implement innovative new ways to secure consumer data and protect it from fraudulent CCPA requests, we urge the Attorney General to revise the regulations to confirm that businesses are empowered to rely on other reasonable methods for verifying the authenticity of agent requests.

Example Revisions

Section 999.315
(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 signed by the consumer. A business may deny a request from an authorized agent if (1) the agent ~~that~~ does not submit proof that they have been authorized by the consumer to act on the consumer's behalf, or (2) the business is unable to establish a reasonable, good-faith belief that the agent's request is valid. User-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism, that

W311-3 cont.

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.

W311-3 cont.

Section 999.326

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may impose the following requirements and deny the request if any of these requirements are not met ~~require that the consumer do the following~~:

(1) Require the consumer to provide the authorized agent signed permission to submit the request ~~do so~~.

(2) Require the consumer to verify their own identity directly with the business.

(3) Require the consumer to directly confirm with the business that they provided the authorized agent permission to submit the request.

(4) Require the consumer or agent to take any other steps that are reasonably likely to confirm the authenticity of the agent's authorization to act on behalf of the consumer.

W311-4 cont.

(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 if (1) the agent ~~that~~ does not submit proof that they have been authorized by the consumer to act on their behalf, or (2) the business is unable to establish a reasonable, good-faith belief that the agent's request is valid.

Message

From: Kate Goodloe [redacted]
Sent: 3/27/2020 3:35:37 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Meghan Pensyl [redacted]
Subject: RE: BSA - Comments on Second Set of Modifications to Proposed CCPA Regulations
Attachments: 2020.3.27 - BSA Comments on Second Revised CCPA Regulations - FINAL.pdf

With apologies, please find attached a corrected PDF containing the final comments from BSA | The Software Alliance. Please treat this file as our formal comments to your office on the second set of modifications to the proposed regulations implementing the CCPA. (This file removes the draft watermark inadvertently included in the prior PDF.)

Best,

Kate Goodloe

Kate Goodloe
Director, Policy
BSA | The Software Alliance
P [redacted]
W bsa.org

From: Kate Goodloe
Sent: Friday, March 27, 2020 2:56 PM
To: PrivacyRegulations@doj.ca.gov
Cc: Meghan Pensyl <meghanp@bsa.org>
Subject: BSA - Comments on Second Set of Modifications to Proposed CCPA Regulations

Attached please find comments from BSA | The Software Alliance on the second set of modifications to the proposed regulations to implement the California Consumer Privacy Act (CCPA). We hope these comments are helpful. Please feel free to contact us if you have any questions or would like to discuss them further.

Many thanks.

Kate Goodloe

Kate Goodloe
Director, Policy
BSA | The Software Alliance
P 202-530-5122
W bsa.org

March 27, 2020

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

RE: Second Set of Modifications to Proposed Regulations to Implement the California Consumer Privacy Act

Dear Attorney General Becerra:

BSA | The Software Alliance appreciates the opportunity to submit comments on the second set of modifications to the proposed regulations to implement the California Consumer Privacy Act ("CCPA").

BSA is the leading advocate for the global software industry before governments and in the international marketplace.[1] Our members are enterprise software companies that create the technology products and services that power other businesses. They offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, and collaboration software. Our companies compete on privacy—and their business models do not depend on monetizing users' data. BSA members recognize that companies must earn consumers' trust and act responsibly with their data. We appreciate California's leadership on these important issues.

BSA's comments focus on the unique role of service providers, which create the products and services on which other businesses rely. As enterprise software companies, BSA members generally act as service providers under the CCPA.[2] Service providers are critical in today's economy, as more companies across a range of industries become technology companies—and depend on service providers for the tools and services that fuel their growth. Software is the backbone of shipping and transportation logistics. It enables remote workplaces and financial transactions all over the world. And it drives the growth of new

[1] BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] Of course, when BSA members collect data for their own business purposes, they take on responsibility for complying with the provisions of the CCPA that apply to "businesses" that "determine[] the purposes and means of the processing of consumers' personal information." For instance, a company that operates principally as a service provider will nonetheless be treated as a business when it collects data for the purposes of providing services directly to consumers.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

technologies like artificial intelligence, which have helped companies of all sizes enter new markets and compete on a global scale.

I. The Proposed Regulations Should be Modified to Reflect the Role of Service Providers

The CCPA already recognizes the unique role of service providers, which act on behalf of businesses that determine the purposes and means of collecting personal information from consumers.[3] We encourage the Attorney General to modify the draft regulations in two ways to avoid altering the service provider-business relationship set out in the CCPA: W312-1

1. ***Restore the language from the February revisions to Section 999.314(c)(1)***. Under the text of the revised draft regulations released in February, Section 999.314(c)(1) recognized that a service provider may retain, use, or disclose personal information to "perform the services specified in the written contract with the business that provided the personal information." That clear statement reflects the fundamental role of service providers as defined by the CCPA's legislative text: to process information "on behalf of a business" pursuant to a written contract.[4] The newly-revised text is less clear, and instead states that a service provider may "process or maintain personal information on behalf of the business that provided the information . . . and in compliance with the written contract for services required by the CCPA." This language creates uncertainty for service providers that serve joint ventures, or other situations in which multiple businesses seek to jointly engage a service provider. W312-2

   We recommend restoring the language from the February text of Section 999.314(c)(1). Alternatively, if the current language is retained, we suggest modifying it to recognize that multiple businesses may jointly engage a service provider, by adding the following italicized/underlined language: "To process or maintain personal information on behalf of the business*(es)* that provided the personal information, or that directed the service provider to collect the personal information, and in compliance with the written contract for services required by the CCPA."

2. ***Revise Section 999.314(c)(3), to clarify that service providers may appropriately augment and correct data for internal uses, but not for building or modifying consumer or household profiles.*** As currently written, Section 999.314(c)(3) may inadvertently reduce the ability of service providers to augment and correct data used for internal purposes, including to train machine learning algorithms. The current language states that a service provider may retain, use or disclose personal information "[f]or internal use by the service provider to build or improve the quality of its services, provided that the use does not include . . . correcting or augmenting data acquired from another source." Read broadly, this could prevent service providers from combining data from multiple sources, if combining the data sets may be viewed as "augmenting" one of the relevant data sets. That raises crucial concerns for W312-3

---

[3] Distinguishing between businesses and service providers is important from a privacy perspective, because adopting this type of role-based responsibility improves privacy protection. Indeed, the distinction is pervasive in the privacy ecosystem. For example, the EU's General Data Protection Regulation ("GDPR") applies to "controllers" that determine the means and purpose for which consumers' data is collected (similar to businesses under the CCPA), and "processors" that process data on their behalf (similar to service providers under the CCPA). W312-1 cont.

[4] Cal. Civil Code § 1798.140(v).

service providers that use machine learning algorithms – since improving the accuracy of an algorithm and reducing its potential bias may require a provider to combine training data from multiple sources. For example, an algorithm used to detect spam emails is more likely to be accurate if it is trained on data that includes spam emails received by multiple customers of a service provider. Moreover, the algorithm will be even more accurate if the provider specifies, for each spam email in the training data set, how many customers received it. That may be viewed as "augmenting" the underlying data set of spam emails — but is crucial to ensure the algorithm is accurate. Indeed, in this context reading Section 999.314(c)(3) to prohibit such activity may also inadvertently limit the scope of Section 999.314(c)(4), which recognizes that service providers may retain, use, or disclose personal information to detect cybersecurity incidents, or protect against fraud or illegal activity.

To avoid that result, and to ensure Section 999.314(c) does not inadvertently limit the ability of service providers to improve the accuracy and reduce the bias of machine learning algorithms, we recommend revising this clause of Section 999.314(c)(3), to focus more narrowly on prohibiting internal uses that involve augmenting or cleaning data for purposes relating to building or modifying consumer profiles. Narrowing the language in this way is consistent with the overall goal of this provision, while reducing concerns that arise from the current broad language.

W312-3 cont.

Specifically, we recommend revising Section 999.314(c)(3) to delete the following language in strikethrough and add the language in italics/underline: "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 to use in providing services to another business, ~~or~~ *including* correcting or augmenting data from another source *for use in such household or consumer profiles*."

II. The Proposed Regulations Should be Modified to Ensure Consumer Rights Are Not Exercised in a Manner that Undermines Consumer Security

Beyond the issues above that are specific to service providers, we also encourage Section 999.313(c)(3) be revised, to ensure that the new consumer rights created by the CCPA are not exercised in a manner that ultimately creates new security risks for consumers. We recommend the following change:

1. ***Restore the original language in Section 999.313(c)(3), and fold it into a revised version of the current four-part test.*** The original language of this section recognized that a business may decline to *provide* a consumer with specific pieces of information in response to a request to know if doing so "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." That is critical to ensuring that a consumer's right to access information is not implemented in a manner that creates security risks.

W312-4

In February, that language was removed from the draft regulations and replaced by a four-part test setting out instances in which business are not required to *search* for information. As an initial matter, the test should not require that all four parts be met, as the current draft would do. More concerning, though, none of those four parts clearly allow a business to deny a right to know request if compliance would create a security risk. For example, a bad actor could use access requests to try and better understand the business' server network structure and identify weak points in the system. Similarly, an individual involved in criminal activity may seek access to

information that would show whether the company has identified the criminal acts occurring on their platform, such as the successful or unsuccessful use of compromised credentials to access a protected environment. Disclosure of that information could thwart efforts by the company or even law enforcement to address such acts.

We recommend: (1) restoring the original language recognizing that businesses may deny requests to know that raise specific security risks, and (2) merging that language into a revised version of the current four-part test, so that not all parts of the test must be met in order to deny a request to know.

We recommend revising Section 999.313(c)(3) to state:

W312-4 cont.

(3) In responding to a request to know, a business is not required to search for personal information if:

(a) *Disclosure of the specific pieces of personal information creates a substantial, articulable, and unreasonable risks to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks;*
(b) *The business does not maintain the personal data in a searchable or reasonably accessible format, provided that the business: (1) does not sell the information, and (2) describes to the consumer the categories of records that may contain personal information that it did not search under this provision; or*
(c) *The business maintains the personal information solely for legal or compliance purposes, provided that the business: (1) does not sell the information, and (2) describes to the consumer the categories of records that may contain personal information that it did not search under this provision.*

* * *

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these comments. We welcome an opportunity to further engage with the Attorney General's Office on these important issues.

Sincerely,



Kate Goodloe
Director, Policy
BSA | The Software Alliance

Message

From: Mohammed, Shoeb [redacted]
Sent: 3/27/2020 4:43:00 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CalChamber Comments to Second Set of Modifications to Text of Proposed CCPA Regulations
Attachments: Final CalChamber Comments to AG Second Modified Regs.pdf

Privacy Regulations Coordinator,

Attached please find the California Chamber of Commerce's written comments on the Attorney General's Second Set of Modifications to Text of Proposed 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]

CalChamber.
CALIFORNIA CHAMBER OF COMMERCE

California Chamber of Commerce

Comments to the Attorney General's *Second Revised* CCPA Regulations

SHOEB MOHAMMED
Policy Advocate
[redacted]

EXECUTIVE SUMMARY

The California Chamber of Commerce (CalChamber) respectfully submits the following comments to the Attorney General's (AG) Second Revised Proposed Regulations for the California Consumer Privacy Act (CCPA), last modified on March 11, 2020. This report does not contain a collectively exhaustive list of concerns with the proposed regulations. Rather, this report supplements CalChamber's earlier comment letters as submitted during the instant rulemaking process, which comments are incorporated by reference herein. Additionally, we encourage the AG to reconsider those prior comments that were not adopted and remain unresolved.

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 issue with proposed regulation, and recommended change(s) to resolve or mitigate CalChamber's related concern(s).

REQUEST TO POSTPONE ENFORCEMENT

CalChamber respectfully urges the Attorney General (the "AG") to postpone enforcement of the California Consumer Privacy Act ("CCPA") regulations.

The business community's commitment to CCPA compliance has been noticeable across the state. Californians have seen disclosures on restaurant menus, signs in retail stores, emails about CCPA rights, links on websites, and notifications on mobile devices. However, as previously stated in CalChamber's Comments to the AG's Revised CCPA Regulations, modified February 10, 2020, the impending July 1, 2020 enforcement date is nevertheless a burdensome deadline to meet. And despite the AG's incredibly efficient work on this body of law, the regulations cannot be finished in time to give businesses a meaningful opportunity to digest the new rules and become compliant with them in full. Today, the COVID-19 crisis only exacerbates these circumstances, making the request to postpone enforcement of these regulations more urgent now than before. W313-1

Accordingly, we respectfully request that the AG postpone enforcement of these regulations to January 1, 2021 at the earliest.

TABLE OF CONTENTS

TABLE OF CONTENTS 3

I. NEW REGULATION NEEDED TO PROTECT INTELLECTUAL PROPERTY RIGHTS & TRADE SECRETS 5

A. Issue: CCPA requires that regulations provide protection for trade secrets and intellectual property rights. (Cal. Civ. Code §1798.135). 5

1. Proposed New Regulation: §999.319 Intellectual Property and Trade Secrets 5

II. SECTION 999.315 - REQUESTS TO OPT-OUT 5

A. Issue: The proposed changes contravene CCPA, and there is no global privacy control. (Cal. Civ. Code §1798.120(a)). 5

1. Proposed Regulation: §§999.315(d); 999.315(g) 5

B. Issue: Explicit consumer actions to submit personal information to a business should override broader privacy settings. 6

1. Proposed Regulation: §§999.315(d)(2); 6

III. SECTION 999.317 – TRAINING; RECORD KEEPING 7

A. Issue: CCPA does not provide any statutory authority for record-keeping requirement. 7

1. Proposed Regulation: § 999.317(g) 7

IV. SECTION 999.313 – RESPONDING TO REQUESTS TO KNOW AND REQUESTS TO DELETE 7

A. Issue: CCPA allows consumers to assert each enumerated right separately, but the regulations do not. (Cal. Civ. Code §§1798.100(b), 1798.110, 1798.115). 7

1. Proposed Regulation: §§ 999.313(c)(10) 7

B. Issue: CCPA does not contemplate disclosing Personal Information in response to unverifiable requests. (Cal. Civ. Code §1798.140(y)). 8

1. Proposed Regulation: §§ 999.313(c)(1) 8

C. Clarification needed to address new prohibition on certain biometric data. 8

1. Proposed Regulation: § 999.313(c)(4) 8

V. SECTION 999.305 – NOTICE AT COLLECTION 9

A. Issue: Providing oral notice to consumers over the phone would increase wait times and negatively impact consumer experience. 9

1. Proposed Regulation: § 999.305(a)(3)(d) 9

B. Issue: CCPA relies on "average consumer" expectations, regulations do not. (Cal. Civ. Code §1798.185) 9

1. Proposed Regulation: § 999.305(a)(4); 999.306 9

C. Issue: CCPA does not require duplicative notice requirements for notice at collection and notice in privacy policy 10

1. Proposed Regulation: §§ 999.305, 999.308 10

VI. SECTION 999.312 – METHODS FOR SUBMITTING REQUESTS TO KNOW & REQUESTS TO DELETE 11

A. Issue: Regulations do not address indirect consumer requests. 11

1. Proposed Regulation: §999.312(e) 11

VII. SECTION 999.301 – DEFINITIONS 11
A. Issue: Definition of right to know conflicts with language regulating how businesses respond to right to know requests. 11
1. Proposed Regulation: §§999.313(c)(10); 999.301(q) 11
VIII. SECTION 999.302 GUIDANCE REGARDING THE INTERPRETATION OF CCPA DEFINITIONS 12
A. Issue: The guidance in §999.302 should be reinstated. 12
1. Proposed Regulation: §999.302 12
IX. SECTION 999.307 – NOTICE OF FINANCIAL INCENTIVE 12
A. Issue: Data does not have independent value. 12
1. Proposed Regulation: §§999.307; 999.337 12

I. NEW REGULATION NEEDED TO PROTECT INTELLECTUAL PROPERTY RIGHTS & TRADE SECRETS

A. Issue: CCPA requires that regulations provide protection for trade secrets and intellectual property rights. (Cal. Civ. Code §1798.135).

1. **Proposed New Regulation:** §999.319 Intellectual Property and Trade Secrets

CCPA requires that the regulations promulgated by the AG include "[e]stablishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights..." 1798.185(a)(3). Because no draft regulation addresses intellectual property rights and trade secrets, we request a regulation establishing protections against violations of intellectual property rights and the disclosure of trade secrets. W313-2

2. **Recommended Language:**

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 the business's intellectual property rights or result in the disclosure of trade secrets.

II. SECTION 999.315 - REQUESTS TO OPT-OUT

A. Issue: The proposed changes contravene CCPA, and there is no global privacy control. (Cal. Civ. Code §1798.120(a)).

1. **Proposed Regulation:** §§999.315(d); 999.315(g)

The proposed changes to §999.315(d)(1) contravene the statute by removing a consumer's right to opt-out, giving pre-set global controls the power over consumer choice. §999.315(d)(1) removes the consumer's choice to opt out by removing the requirement that the privacy control shall not be designed with any pre-selected settings. This is in explicit contravention of the statute's grant to consumers, "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." (Cal. Civ.Code §1798.120(a)). Additionally, by removing the prohibition that the privacy control shall not be designed with any pre-selected settings, the draft rules appear to give browser publishers significant power by allowing them to unilaterally turn on an opt-out, or even do it selectively for certain companies. W313-3

There is no global privacy control. Because there is no global privacy control, businesses must have the option to provide consumers with a standardized opt-out button on their individual websites.

2. **Recommended Change:**

Strike §999.315(d) in its entirety.

Alternatively, revise § 999.315(d) as follows:

"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 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." W313-3 cont.

In addition, if this provision is retained, relevant language that was deleted in §999.315(d)(1) must be restored to ensure that consumers are making an affirmative choice. The language that should be restored is as follows:

"The privacy control shall require that the consumer affirmatively select their choice to opt out." (Previously deleted from 999.315(d)(1)).

B. Issue: Explicit consumer actions to submit personal information to a business should override broader privacy settings.

1. **Proposed Regulation:** §§999.315(d)(2);

User controlled privacy settings on browsers and plugins may override explicit actions by the consumer to submit personal information to a business. For example, if a consumer was submitting personal information and the submission had a clear and unambiguous authorization to sell the consumer's personal information, said authorization should take precedent over previously selected privacy settings. If not, a business could be prevented from using the information regardless of the consumer's intent to allow such activity because the consumer had previousy elected an 'opt-out' on the browser privacy settings, W313-4

2. **Recommended Change:**

Revise § 999.315(d)(2) as follows:

Except where a consumer takes specific action that exhibits intent to override the global privacy setting with the business-specific privacy setting, such as submitting personal information directly to the business with the intent to permit sales of 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 confirm the business-specific privacy setting or participation in the financial incentive program.

III. SECTION 999.317 – TRAINING; RECORD KEEPING

A. Issue: CCPA does not provide any statutory authority for record-keeping requirement.

1. **Proposed Regulation:** § 999.317(g)

The reporting requirement in §999.317(g) has no support in the language of CCPA and therefore has no support in the law. California Government Code Sections 11349-11349.6 set forth the standards that proposed regulations are analyzed for purposes of approval and publication, including: (1) necessity; (2) authority; (3) clarity; (4) consistency; (5) reference; and (6) non-duplication. The Civil Code sections cited as authority do not support a training or recordkeeping requirement. Accordingly, we believe this proposed section goes beyond the scope of the CCPA and beyond the scope of the Attorney General's regulatory authority. W313-5

2. **Recommended Changes:**

Strike §999.317(g).

IV. SECTION 999.313 – RESPONDING TO REQUESTS TO KNOW AND REQUESTS TO DELETE

A. Issue: CCPA allows consumers to assert each enumerated right separately, but the regulations do not. (Cal. Civ. Code §§1798.100(b), 1798.110, 1798.115).

1. **Proposed Regulation:** §§ 999.313(c)(10)

Conflating consumer rights contradicts CCPA. CCPA empowers consumers to assert each of their enumerated rights separately under §1798.100(b), §1798.110, and §1798.115, or assert them altogether, depending upon the consumer's interest. Nothing in the CCPA requires businesses to produce information that was not requested.

Businesses should not be required to overproduce when consumers request specific information. This section requires businesses to produce all categories of information with regard to a consumer's request to know, even if a consumer has only made a specific request for one category. 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 make requests for more specific information. Overproduction of information does not benefit the consumer or the business. W313-6

2. **Recommended Change:**
Revise §999.313(c)(10) to allow businesses the option to either provide consumers with the information they requested, or instead provide the six elements relating to their personal information when responding to a consumer's more specific request.

B. Issue: CCPA does not contemplate disclosing Personal Information in response to unverifiable requests. (Cal. Civ. Code §1798.140(y)).

1. **Proposed Regulation:** §§ 999.313(c)(1)

CCPA does not contemplate disclosure of Personal Information in response to unverifiable requests. Under CCPA, a business is not obligated to provide information to the consumer if the business cannot verify that the consumer making the request is the consumer about whom the business has collected information. In fact, the CCPA only requires disclosure of personal information after it has verified the identity of the requestor. The language in this section is contradictory to the intent and language of Civil Code section 1798.140(y). W313-7

2. **Recommended Change:**

Strike language in §999.313(c)(1) requiring 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).~~"

C. Clarification needed to address new prohibition on certain biometric data.

1. **Proposed Regulation: § 999.313(c)(4)**

This proposed section prohibits a business from disclosing certain sensitive data of a consumer, including "unique biometric data generated from measurements or technical analysis of human characteristics" in response to a right to know. The CCPA defines biometric data to include health or exercise data containing identifying information. (*See* Cal. Civ. Code. §1798.140(b)), but does not include a term or definition for "unique biometric data" as described in this section W313-8

2. **Recommendation:**
Further clarification to this section is needed to ensure that this prohibition only applies to the types of biometric data that can itself identify the individual.

V. SECTION 999.305 – NOTICE AT COLLECTION

A. Issue: Providing oral notice to consumers over the phone would increase wait times and negatively impact consumer experience.

1. **Proposed Regulation:** § 999.305(a)(3)(d)

Section § 999.305 (a)(3)(d) states that when a business collects personal information over the telephone or in person, it may provide the required notices orally. Providing oral notice to consumers that initiate phone-calls does not align with consumers' expectations and would cause increased wait times, especially at consumer contact centers that handle large volumes of calls. W313-9

2. **Recommended Change:**

The regulations should be amended to specify that if a consumer initiates a phone call with a business and chooses to provide personal information for the provision of a good or service, that the notice can be provided by email, or that the consumer can be directed to an online Privacy Policy. This method would allow for transparency and improve the consumer experience.

B. Issue: CCPA relies on "average consumer" expectations, regulations do not. (Cal. Civ. Code §1798.185)

1. **Proposed Regulation:** § 999.305(a)(4); 999.306

Section § 999.305 (a)(4) states that, "When a business collects personal information from a consumer's mobile device for a purpose that **the** consumer would not reasonably expect," - as opposed to – "for a purpose that an **average** consumer would not reasonably expect." … (emphasis added). W313-10

Businesses should not be expected to know what each and every consumer would personally expect. The term "average" clarifies this ambiguity and brings the language closer to the language of CCPA, which relies on "average consumer" expectations. (*See* Cal. Civ. Code § 1798.185).

2. **Recommended Change:**

The term "consumer" should be revised to "average consumer" for consistency with CCPA.

C. Issue: CCPA does not require duplicative notice requirements for notice at collection and notice in privacy policy.

1. **Proposed Regulation:** §§ 999.305, 999.308

Section 305(b)(4) states, "A business shall include the following in its notice at collection: A link to the business's privacy policy, or in the case of offline notices, where the business's privacy policy can be found online." This provision could be read to imply that two separate notices are required with the shorter notice "at or before collection" linking to the separate privacy policy. But Section 305(c) suggests that only a separate link is required near the point of online collection of PI that links to the relevant section of the privacy policy, "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) [i.e., information regarding the categories of PI to be collected and the purposes for which such PI will be used]". This reading is further confirmed by Section 305(a)(3)(a), "When a business collects consumers' personal information online, it may post a conspicuous link to the notice on the introductory page of the business's website and on all webpages where personal information is collected." W313-11

Read together, these various provisions indicate that two separate hyperlinks must appear on a business's website (even if located at the bottom of every webpage): one that is to the company's comprehensive privacy policy as described in Section 308, and the second that is to the shorter, more targeted notice required by Section 305 which focuses solely on the "categories of personal information to be collected from [consumers] and the purposes for which the personal information will be used."

Considering the purpose of the rules, if a business develops a comprehensive privacy policy that complies with the substantive requirements of both §§999.305 and 999.308, it should be deemed sufficient to satisfy the requirements of both provisions, eliminating any need for two separate notices or two separate links on the relevant web pages. This would also ease consumer frustration by creating one designated location where consumers can find all of this information, instead of navigating between two separate locations or links in order to find the information they are searching for.

2. **Recommended Change:**

Add a new subsection to 999.305 to harmonize the two requirements:

§999.305(h) A business that provides a link to a comprehensive privacy policy that (1) complies with the requirements of Section 308, (2) contains the information required in Section 305(b), and (3) appears on the introductory page of the business's website and on all webpages where personal information is collected shall be deemed to comply with the requirements of Section 305 and Section 308."

VI. SECTION 999.312 – METHODS FOR SUBMITTING REQUESTS TO KNOW AND REQUESTS TO DELETE

A. Issue: Regulations do not address indirect consumer requests.

1. **Proposed Regulation:** §999.312(e)

Consumers may submit indirect requests through unmonitored channels. This provision allows a consumer to submit requests through an undesignated, unauthorized channel to the business, and requires the business to comply as though it was authorized or respond with further directions on how to submit an authorized request. This provision imposes a significant monitoring burden on businesses to review all forms of communication with the business, including social media, in order to find and timely respond to these unauthorized requests. W313-12

2. **Recommended Change:**

Revise §999.312(e) to provide added clarity as follows:

"If a consumer submits a request through a customary support channel or point of consumer contact ~~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.

VII. SECTION 999.301 – DEFINITIONS

A. Issue: Definition of right to know conflicts with language regulating how businesses respond to right to know requests.

1. **Proposed Regulation: §§999.313(c)(10); 999.301(q)**

Section 999.301(q) is inconsistent with Section 999.313(c)(10). Section 999.301(q) gives a consumer a right to "any or all" of the following categories of personal information. But under section 999.313(c)(10), a business is required to disclose all enumerated categories even if a consumer makes a limited request. W313-13

2. **Recommended Change:**

For consistency, revise Section 999.313(c)(10) to mirror the language found in section 999.301(q), which is closer to the language of CCPA.

VIII. SECTION 999.302 GUIDANCE REGARDING THE INTERPRETATION OF CCPA DEFINITIONS

A. Issue: The guidance in §999.302 should be reinstated.

1. **Proposed Regulation: §999.302**

The guidance regarding the definition of "personal information" provided a helpful point of reference to businesses and should be reinstated. W313-14

2. **Recommended Change:**

Restore §999.302.

IX. SECTION 999.307 – NOTICE OF FINANCIAL INCENTIVE

A. Issue: Data does not have independent value.

1. **Proposed Regulation:** §§999.307; 999.337

Data does not have independent value. The reason certain businesses can offer their services for free or for reduced cost is not because they are being compensated for peoples' data, it is because they derive revenue through the sale of ads. Ads are valued using objective metrics such as the number of clicks or the number of views. It is misleading to communicate to consumers that their personal data is valued at a certain dollar amount. W313-15 & W313-16

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~~. W313-15 cont.

Strike §999.337 in its entirety. W313-16 cont.

Message

From: Keir Lamont [redacted]
Sent: 3/27/2020 4:42:36 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCIA Comments on Second Set of Modifications to Proposed Regulations
Attachments: CCIA Comments on CCPA Regulations Second Modification.pdf

Dear Privacy Regulations Coordinator:

Please find attached the comments of the Computer & Communications Industry Association on the second set of modifications to the CCPA draft implementing regulations.

Best regards,
Keir Lamont

--
Keir Lamont
Policy Counsel
Computer & Communications Industry Association (CCIA)

Computer & Communications Industry Association
Tech Advocacy Since 1972

March 27, 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: PrivacyRegulations@doj.ca.gov

Re: *Computer & Communications Industry Association comments on second set of modifications to proposed California Consumer Privacy Act regulations*

Dear Ms. Kim:

Thank you for the opportunity to comment on the California Department of Justice's (the Department) second set of modifications to the proposed implementing regulations for the California Consumer Privacy Act of 2018 (CCPA). The Computer & Communications Industry Association (CCIA) is an international nonprofit trade association representing a broad cross section of large, medium, and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications, and Internet products and services. Our members employ more than 750,000 workers and generate annual revenues in excess of $540 billion.[1]

CCIA members place a high value on protecting consumer privacy and support the consumer rights and privacy principles that underpin the CCPA including transparency, notice, and consumer control over data processing practices.[2] CCIA also appreciates the Department's public engagement and receptiveness in developing the Act's regulations. Unfortunately, the rushed legislative drafting of the CCPA and absence of critical input from stakeholders and compliance considerations has contributed to several areas of confusion and complexity in implementing the Act.[3] With the CCPA presently in effect and an impending enforcement date of July 1, 2020, it is important that the Department promulgate clear implementing regulations consistent with the text of the CCPA that establish uniform expectations for consumers and businesses of their rights and obligations under the Act.

The following modifications to the draft implementing regulations will support reliable operationalization of the rights and obligations established by the CCPA and promote consumer privacy rights within California.

[1] A complete list of CCIA's members is available online at www.ccianet.org/members.
[2] *See* CCIA, *Privacy Principles: A New Framework for Protecting Data and Promoting Innovation* (Nov. 7, 2018), http://www.ccianet.org/wp-content/uploads/2018/11/CCIA_Privacy_Principles.pdf.
[3] *See* Hannah Murphy, *California's privacy law arrives to confusion and costs for businesses*, Financial Times (Jan. 1, 2020), https://www.ft.com/content/7b541808-2bdf-11ea-bc77-65e4aa615551.

I. Draft regulation § 999.302 regarding the interpretation of "Personal Information" under the CCPA should be reinstated and clarified

Analysis: The Department's addition of § 999.302 to the February regulations regarding the interpretation "personal information" under the CCPA was a welcome inclusion.[4] This section provided helpful guidance for businesses that collect incidental or limited device information through online websites of their CCPA obligations. Furthermore, the regulation was consistent with the intent of the CCPA, which eschews *per se* categories of personal information in favor of contextual analysis of when information should be considered identifying.[5]

Recommendation: CCIA recommends that the Department reinsert regulation § 999.302 and provide additional clarification on the terms "reasonably" and "collects" in order to support the consistent interpretation and implementation of the CCPA.

First, the regulations should recognize that whether an organization can "reasonably link" information such as device signals and identifiers to a particular consumer or household may depend on internal technical measures and controls the organization takes to prevent such identification. This clarification will encourage privacy-preserving techniques such as pseudonymization and encryption consistent with both the goals of the CCPA and similar provisions under the European General Data Protection Regulation.[6] W314-1

Second, the regulations should provide additional guidance as to when an organization "collects" personal information for the purposes of the CCPA's right to access information.[7] Specifically, the regulations should clarify that the definition of "collects" does not refer to information generated internally about a consumer that is used only for internal business purposes. Such information is commonly not maintained in a human-readable way, is not linked to individual consumer accounts, and would not be relevant to consumers if produced pursuant to an access request. Furthermore, this clarification is consistent with the CCPA's definition of "collects," which is limited to information that is either "received" from a consumer or produced through "observation" of the consumer.[8]

II. New privacy policy requirements under regulation § 999.308 should be clarified

Analysis: Organizations that process personal information should be transparent about the categories of information that they collect and inform consumers about how they will process, store, and transfer data. It is important that notice requirements are carefully scoped to cover relevant information and contain sufficient flexibility to allow organizations to innovate in W314-2

[4] Modified CCPA Regulations, § 999.302 "Guidance Regarding the Interpretation of CCPA Definitions" (Feb. 10, 2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf.
[5] CCPA § 1798.140(o) ("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…") (emphasis added).
[6] *See* General Data Protection Regulation, Art. 25 & 32.
[7] *See* CCPA § 1798.115(a)(1) (establishing the right for consumers to request that a business disclose the "categories of personal information that the business *collected* about the consumer") (emphasis added).
[8] CCPA § 1798.140(e).

providing context-appropriate information to consumers in a clear, succinct, and meaningful manner.

The Department's additions to the privacy policy required under the CCPA in the March regulations will provide relevant information to consumers, including a description of the categories sources the organization collects information from.[9] However, as written, regulation § 999.308(c)(1)(e) could be read to suggest that a covered organization must describe the specific information collected from each category of source. Such a requirement would overlap with draft regulation § 999.308(c)(1)(d) and lengthen CCPA privacy notices without corresponding benefits to consumers. W314-2 cont.

Recommendation: CCIA recommends that the Department modify § 999.308(c)(1)(e) to clarify that it is limited to identifying and describing the categories of sources from which and organization collects personal information:

> *"§999.308(c)(1)(e): Identify the categories of sources from which the personal information is collected. The categories shall be described in a manner that provides consumers a meaningful understanding of the* ***sources from which the*** *information* ***is*** ~~*being*~~ *collected."*

III. Conditions for responding to user requests under draft regulation § 999.313 should account for security concerns and undue burdens

Analysis: The CCPA's 'right to know' requires businesses to disclose personal information that they have collected about a consumer.[10] However, this right is not absolute, as the Act instructs the Department to promulgate implementing regulations that account for both "security concerns" and the "burden on the business" of data access requests.[11] The draft regulations properly recognize that a business should not be required to search for and produce every category of personal information in response to a verified access request.[12] However the four-prong test delineated by § 999.313(c)(3) establishing conditions exempting certain information from the scope of access requests is deficient because as a practical matter, the conditions are contradictory. For example, information that is retained expressly for a legal purpose will necessarily be maintained in a reasonably accessible format. Therefore, as presently conceived this exception is contrary to the intent of the CCPA because it would require organizations to conduct burdensome searches for unstructured information and jeopardize consumer privacy and security by requiring organizations to conduct widespread linkage of information to individuals that would otherwise not be reasonably accessible. W314-3

Recommendation: In order to protect both businesses and consumers, the Department should reestablish the exception under § 999.313(c)(3) for responding to requests that create a

[9] Modified CCPA Regulations, § 999.308(c)(1)(e) & (f) (Mar. 11, 2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-second-set-clean-031120.pdf.
[10] CCPA § 1798.110.
[11] CCPA § 1798.185(a)(7).
[12] March Regulations, § 999.313(c)(3) & (4).

"substantial, articulable, and unreasonable risk to the security of that personal information."[13] Furthermore, the regulation should modify the four-prong test so that each condition is sufficient to exclude information from the search requirements:

> *"§ 999.313(c)(3): ...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 information it collects:***
>
> *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;* ***or***
> *c. The business does not sell the personal information and does not use it for any commercial purpose..."*

W314-3 cont.

IV. Draft regulation § 999.314 should be modified to clarify that service providers may use personal information for all business purposes permitted by the CCPA

Analysis: In its initial comments on the October regulations, CCIA raised concerns that the rules governing services providers infringed upon legitimate business purposes expressly recognized by the CCPA.[14] While the Department's February regulations largely addressed this concern, the March regulations' modifications to § 999.314(c)(1) appear to reintroduce uncertainty for service providers by creating new restrictions not supported by the CCPA. The CCPA recognizes the ability of service providers to process information for both a contracting organization's "business purposes" in addition to the service provider's "operational purposes" as may be necessary for the performance of a contractually specified service.[15] California businesses and consumers also benefit from the ability of service providers to internally process data from multiple sources consistent with privacy notices and CCPA-compliant written agreements in order to provide common services. By limiting the ability of service providers to process personal information to only doing so directly "on behalf of" a particular business that provided or directed the collection of information, the second revision appears to contradict both the text of the CCPA and public policy.

W314-4

Recommendation: In order to ensure that service providers can reasonably rely on the CCPA to process information for permitted business purposes, draft regulation § 999.314(c) should be modified as follows:

---

[13] Initial proposed regulations, § 999.313(c)(3) (Oct. 11, 2019), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf.

[14] *See* CCIA, *Comments on California Consumer Privacy Act proposed regulations* (Dec. 6, 2019) at 7, https://www.ccianet.org/wp-content/uploads/2019/12/CCIA-Comments-on-CCPA-draft-regulations.pdf (hereinafter "CCIA Dec. 6 Comments").

[15] CCPA § 1798.140(d) ("'Business purpose' means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected.").

"§ 999.314(c): A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except ***to the extent permitted by the CCPA including****:*

(1) ~~*To process or maintain personal information on behalf of the business that provided the personal information, or that directed the service provider to collect the personal information, and in compliance with the written contract for services required by the CCPA*~~ ***To perform the services specified in the written contract with the business that provided the personal information…"***

W314-4 cont.

V. Proposed Draft Regulation § 999.315 Should Not Circumvent Consumer Control Over Opt-Out Requests

Analysis: In its initial comments, CCIA addressed the practical drawbacks of departing from the CCPA's specific and uniform mechanisms of exercising consumer control by requiring organizations to recognize and respond to a limitless array of yet-to-be developed opt-out methods.[16] If the Department intends to recognize a new category of "global privacy controls" it should ensure that such mechanisms do not result in the transfer of control over the CCPA's privacy choices from consumers to third-party entities such as the developers of browsers, consumer devices, and plug-ins. The March regulations' removal of the prohibition on "pre-selected settings" creates the potential for businesses to leverage privacy controls for competitive purposes, selectively applying privacy controls without consumer choice or intent.

W314-5

Recommendation: In order to support consumer control over their information and privacy rights consistent with the intent of the CCPA,[17] the regulations should be amended as follows:

"§ 999.315(d) 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 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."*

Thank you again for the opportunity to comment on the draft implementing regulations for the California Consumer Privacy Act. If you have any questions regarding the comments and recommendations in this letter, please contact Keir Lamont at [redacted]

Sincerely,

Keir Lamont
Policy Counsel
Computer & Communications Industry Association

---

[16] CCIA Dec. 6 Comments at 8.
[17] CCPA Section 2(h).

Message

From: Liam McGregor [redacted]
Sent: 3/28/2020 1:00:41 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCPA: Comment on 2nd revisions—Which firms must calculate the value of my data?

Hi there! My name is Liam McGregor; I'm a resident of San Juan Capistrano, (Orange County, CA), and a student in economics at Stanford, in Santa Clara County, CA.

In section § 999.337. Calculating the Value of Consumer Data, I'm seriously concerned about the language around which companies are obligated to do this. The text currently reads,"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...". This seems very narrow, and, in my (lay) reading of the law, does not apply to companies such as Google and Facebook, who offer their services for "free".

The wording should be adjusted to include technology giants such as Facebook, or we should have an explanation for why they are intentionally omitted.

W315-1

Californians ought to know how much their data is worth, full stop. We're either paid for our data or we're bilked out of the value of our data because, as individuals, we cannot know how much it's worth. The companies hold all the cards.

How can I know "free" is a good price for my month on Facebook if the firm actually made $100 off of my data by serving me ads? I derive some value from Facebook, but that's a parasitic relationship because they're extracting more value from me than I get in return. That's an unfair deal. On the other hand, if they only make $5 a month off of my data, maybe that's a better deal for me. Consumers ought to have a right to know the value of the personal information we're giving away if the company is giving me the service "for free"—no matter if the company is paying me for it or not, and no matter if they vary service levels or not,

The value of our data is what we're *actually* paying. We have no way of knowing what we're really paying for these "free" services unless they tell us. They will not tell us unless legislation requires them to do so.

~ ~ ~

As an economist, I'm currently researching Facebook and their status under antitrust law in the US. Specifically, I'm examining their market power in American consumers' online attention, and the ways they hide their monopolistic price increases.

They do it this way: By creating a "free" product for consumers, they create a barter exchange in which they provide some service to users in exchange for huge amounts of data, which they turn around and use to sell access to consumers to advertisers at tremendously high margins. Californians ought to have a right to know how much Facebook makes off of their personal data. I applaud the intent of the law, but worry that in its current wording would not apply to Facebook.

The problem with this barter economy is, as of today, Facebook is the only one who can truly know how much my data is worth. Until they reveal that to me, I'm in the dark on whether or not I'm getting a good deal on their service.

~ ~ ~

Best,

Liam McGregor

Message

From: Tobin, Timothy P. [redacted]
Sent: 3/17/2020 10:17:12 AM
To: Stacey Schesser[redacted]
Subject: CCPA and Covid-19 Request for Relief

Dear Stacey,

Our clients and other companies are working in good faith to respond to CCPA individual rights requests. The current global pandemic is however, forcing numerous companies to institute work at home procedures. In addition, scarce resources are in many cases being diverted to address the emergency both in the U.S., and for multinational companies globally. These circumstances are making it very challenging for companies to comply with CCPA rights requests within statutory timeframes. I am writing to request that when its CCPA enforcement authority takes effect on July 1, 2020, that the California Attorney General refrain from enforcement actions against companies relating to delayed responses to CCPA rights requests that occurred during this pandemic.

Other regulators in the U.S. and globally are exercising appropriate restraint during this crisis. For example, in the United Kingdom, the Information Commissioner's Office has stated that it will not take regulatory action against companies based on delays in responding to information rights requests during the pandemic. *See* https://ico.org.uk/for-organisations/data-protection-and-coronavirus/. In the U.S., Health and Human Services has waived various HIPAA requirements and penalties for certain hospitals. *See* https://ico.org.uk/for-organisations/data-protection-and-coronavirus/. I am not suggesting the duty to respond to rights requests should not apply to companies, but that the Attorney General recognize that failing to meet statutory timeframes not result in enforcement action. I also believe It would be helpful for the California Attorney General to make a public release on this point. W316-1

I appreciate your consideration of this request.

Regards,

Tim

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.

About Hogan Lovells
Hogan Lovells is an international legal practice that includes Hogan Lovells US LLP and Hogan Lovells International LLP. For more information, see www.hoganlovells.com.

CONFIDENTIALITY. This email and any attachments are confidential, except where the email states it can be disclosed; it may also be privileged. If received in error, please do not disclose the contents to anyone, but notify the sender by return email and delete this email (and any attachments) from your system.

Message

From: Connor Gafner [redacted]
Sent: 3/27/2020 5:00:46 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Garrett Gillet [redacted]
Subject: CCPA changes
Attachments: CCPA Commet letter Vael Inc 3.27.20 .pdf

See attached proposed CCPA changes

Connor Gafner
Vael, Inc

Vael, Inc.

March 26, 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 March 2020

Dear Lisa,

Vael, Inc., is an early stage data privacy startup based out of San Francisco, CA. From personal experience coupled with 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.

The regulation lacks a standard method for authorized agents to contact businesses to submit requests on the behalf of consumers. This can inhibit CCPA from accomplishing its goal of creating new consumer rights relating to the access to, deletion of, and sharing of personal information collected by businesses. As it stands, the regulation requires that businesses only provide the methods of request submission that are most convenient for themselves not necessarily the consumer. This can easily be abused to dissuade consumers from putting in the excessive effort of using their new rights under CCPA. Given the nature of CCPA requests and the imperative for broad public participation this can jeopardize the effectiveness of the regulation as a whole.

W317-1

To this end we propose that the following be added to section:

§999.308 (c)(5)

Businesses shall, in their privacy policy, provide an email specifically for authorized agents to contact companies with information regarding the submission of requests on behalf of the represented consumers.

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]

Connor Gafner

Co-Founder, CEO

Vael, Inc.

[redacted]

Message

From: Markus Hastings [redacted]
Sent: 3/26/2020 11:22:00 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Mark Hastings [redacted]
Subject: CCPA Comment letter
Attachments: Hastings CCPA comment 1.pdf; Hastings CCPA comment 1.docx

Hi Lisa,
Thank you for taking a few minutes with me the other day to clarify the process for submitting a comment for the 2nd set of Modifications to the CCPA.

Please find attached my comment letter in Word and pdf format. I'm also including the text of my comment below.
Regards,
Mark Hastings

---TEXT OF COMMENT----
Mark Hastings
[redacted]
LinkedIn.com/in/MarkTHastings

Attn: 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: Comments on the Modified Proposed Regulations relating to the California Consumer Privacy Act of 2018 (CCPA, aka "the Act") for the comment period ending March 27, 2020

Dear Ms. Kim:
I appreciate the opportunity to provide a public comment regarding the regulations of the California Consumer Privacy Act. This comment letter is submitted solely on behalf of myself as I have a business interest in the CCPA.
My background is in the Marketing Automation and Customer Relationship Management (CRM) technology industry. I have many years of experience working directly with customer lists, and I have managed teams of data managers for CRM and Marketing Automation systems. My expertise in this field enables me to consult professionally in these areas.
I have read prior comments regarding section 999.337 of the Act from other professionals and organizations, and I understand the objection to this section, as the valuation of a customer data asset is not currently a well-defined standard. However, my position is this section should remain as is currently written, as I have developed an accurate and reliable methodology for valuation of a customer data asset that I believe can become a new standard. There is no need to record my methodology in the Act, as there is already an allowance for a new methodology in subsection (a), number (8), specifically, "Any other practical and reasonably reliable method of calculation used in good-faith."
At some point in the future, it may be prudent to revisit this section of the Act and refine the list of methods available for use in this exercise. For now, section 999.337 is sufficiently prescriptive while still allowing for flexibility of methods.

W318-1

Regards,

Mark Hastings

---END TEXT OF COMMENT---

Regards,
Mark
O: [redacted]
C: [redacted]

----- Forwarded Message -----
From: CCPA Mailing List <webmaster@doj.ca.gov>
To: "ccpalist@doj.ca.gov" <ccpalist@doj.ca.gov>
Sent: Wednesday, March 11, 2020, 05:44:55 PM EDT
Subject: CCPA Regulations - Notice of 2nd Set of Modifications

[redacted]

March 11, 2020

CCPA Regulations - Notice of 2nd Set of Modifications

NOTICE OF SECOND SET OF MODIFICATIONS TO TEXT OF PROPOSED REGULATIONS

[OAL File No. 2019-1001-05]

Pursuant to the requirements of Government Code section 11346.8, subdivision (c), and section 44 of Title 1 of the California Code of Regulations, the California Department of Justice (Department) is providing notice of a second set of modifications made to the proposed regulations regarding the California Consumer Privacy Act.

The Department first published and noticed the proposed regulations for public comment on October 11, 2019. On February 10, 2020, the Department gave notice of modifications to the proposed regulations, based on comments received during the 45-day comment period. Subsequently, the Department received around 100 comments in response to the modifications. This second set of modifications is in response to those comments and/or to clarify and conform the proposed regulations to existing law.

This Notice, the text of the second set of modifications to the proposed regulations, and comparison of the text as originally proposed with both the first and second set of modifications reflected are available at www.oag.ca.gov/privacy/ccpa. The originally proposed regulations and all

available at this website.

The Department will accept written comments regarding the proposed changes between Wednesday, March 11, 2020 and Friday, March 27, 2020. All written comments must be submitted to the Department **no later than 5:00 p.m. on March 27, 2020** by email to PrivacyRegulations@doj.ca.gov, or by mail to the address listed below.

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

All timely comments received that are relevant to the second set of modifications will be reviewed and responded to by the Department's staff as part of the compilation of the rulemaking file. Please limit written comments to those items.



You may find more information about the California Consumer Privacy Act (CCPA) on our website at: https://oag.ca.gov/privacy/ccpa

Please visit the remainder of the Attorney General's site at: https://oag.ca.gov/

Unsubscribe from this list

Mark Hastings

[redacted] | [redacted] | [redacted] | LinkedIn.com/in/MarkTHastings

Attn: 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: Comments on the Modified Proposed Regulations relating to the California Consumer Privacy Act of 2018 (CCPA, aka "the Act") for the comment period ending March 27, 2020

Dear Ms. Kim:

I appreciate the opportunity to provide a public comment regarding the regulations of the California Consumer Privacy Act. This comment letter is submitted solely on behalf of myself as I have a business interest in the CCPA.

My background is in the Marketing Automation and Customer Relationship Management (CRM) technology industry. I have many years of experience working directly with customer lists, and I have managed teams of data managers for CRM and Marketing Automation systems. My expertise in this field enables me to consult professionally in these areas.

I have read prior comments regarding section 999.337 of the Act from other professionals and organizations, and I understand the objection to this section, as the valuation of a customer data asset is not currently a well-defined standard. However, my position is this section should remain as is currently written, as I have developed an accurate and reliable methodology for valuation of a customer data asset that I believe can become a new standard. There is no need to record my methodology in the Act, as there is already an allowance for a new methodology in subsection (a), number (8), specifically, "Any other practical and reasonably reliable method of calculation used in good-faith."

At some point in the future, it may be prudent to revisit this section of the Act and refine the list of methods available for use in this exercise. For now, section 999.337 is sufficiently prescriptive while still allowing for flexibility of methods.

Regards,

Mark Hastings

Mark Hastings

Mark Hastings

[redacted] | [redacted] | [redacted] | LinkedIn.com/in/MarkTHastings

Attn: 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: Comments on the Modified Proposed Regulations relating to the California Consumer Privacy Act of 2018 (CCPA, aka "the Act") for the comment period ending March 27, 2020

Dear Ms. Kim:

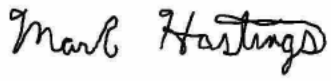
I appreciate the opportunity to provide a public comment regarding the regulations of the California Consumer Privacy Act. This comment letter is submitted solely on behalf of myself as I have a business interest in the CCPA.

My background is in the Marketing Automation and Customer Relationship Management (CRM) technology industry. I have many years of experience working directly with customer lists, and I have managed teams of data managers for CRM and Marketing Automation systems. My expertise in this field enables me to consult professionally in these areas.

I have read prior comments regarding section 999.337 of the Act from other professionals and organizations, and I understand the objection to this section, as the valuation of a customer data asset is not currently a well-defined standard. However, my position is this section should remain as is currently written, as I have developed an accurate and reliable methodology for valuation of a customer data asset that I believe can become a new standard. There is no need to record my methodology in the Act, as there is already an allowance for a new methodology in subsection (a), number (8), specifically, "Any other practical and reasonably reliable method of calculation used in good-faith."

At some point in the future, it may be prudent to revisit this section of the Act and refine the list of methods available for use in this exercise. For now, section 999.337 is sufficiently prescriptive while still allowing for flexibility of methods.

Regards,



Mark Hastings

Message

From: Chris Allen [redacted]]
Sent: 3/27/2020 3:34:56 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCPA Comments on Second Round of Modifications
Attachments: CCPA AG Comment Letter 3-27-2020 Patelco.pdf

Kim, attached is Patelco's comments on the Second Round of Modifications to CCPA. Please let me if you have any comments or questions. Thanks

Chris Allen
Patelco Credit Union
Chief Risk Office
3 Park Place
Dublin, Ca 94568
[redacted]

========== DISCLAIMER ==========
Information contained herein is the sole and exclusive property of Patelco Credit Union. The information within this document or item is confidential; it shall not be disclosed to a third party or used except for the purpose of the recipient providing a service to Patelco Credit Union or for the benefit of Patelco Credit Union. Your retention, possession or use of this information constitutes your acceptance of these terms. Please note that the sender accepts no responsibility for viruses and it is your responsibility to scan attachments (if any).

Patelco
CREDIT UNION

3 Park Place
Dublin, CA 94568

March 27, 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 to Proposed CCPA Regulations Second Round of Modifications

Dear Ms. Kim:

On behalf of Patelco Credit Union, a California state-chartered federally insured credit union, we write to provide our input into the Attorney General's Office ("AG") proposed California Consumer Privacy Act (CCPA) Regulations ("Proposed Regulations"). We understand the purpose of the Proposed Regulations is to operationalize the CCPA and provide clarity and specificity to assist in implementing the CCPA which took effect on January 1, 2020. Given that CCPA imposes several obligations on most businesses, as an institution that is seemingly subject to it, we seek to obtain clarification on several areas that do not appear to be addressed in the Proposed Regulations and in the modifications. Further clarification we believe is needed.

The effective date for CCPA was January 1, 2020. Given how general the statue is and many of the previously provided comments were not fully addressed, we believe it would be prudent to have the effective date extended. Businesses should be afforded ample time to design and implement a comprehensive system to address are the requirements. Due to the complex proposed regulations, enforcement should also be delayed until six months after publication of the final regulations. In addition, with California in the middle of a Global Pandemic, businesses need to focus on the consumers they service. Meeting the many CCPA regulatory compliance rules, takes critical time away from serving consumers in their time of need. W319-1

While the Second Round of Proposed Modifications provide clarification in some areas within CCPA and it will assist businesses subject to the CCPA in complying, we believe there are still many areas that remain ambiguous or unaddressed.

Section 999.302 Guidance Regarding the Interpretation of CCPA Definition. This section provided a definition for "personal information". This section was confusing and was much broader than Gramm-Leach-Bliley ACT (GLBA) and California Financial Information Privacy Act (CFIPA) definition of nonpublic personal information. This section was deleted. However, there remains confusion regarding the exemption of personal information that is collected, processed and/or sold. The confusion arises because CCPA utilizes terms that are inconsistent with GLBA and CFIPA. GLBA and CFIPA utilizes nonpublic personal information which is defined as personally identifiable financial information. We recommend that proposed regulation clarity these terms and better define personal information.

W319-2

W319-3

We support some of the recent changes such as: removing the requirement to have opt out bottom on the company's website; adding that a business that does not collect personal information directly from a consumer does not need to provide a notice of collection; clarifying that a service provider can collect information about a consumer on behalf of another business, even if that information is not collected directly from the consumer and deleting the requirement to provide a notice of collection of employee-related information.

W319-4

W319-5

We appreciate the opportunity to provide input into the AG's Proposed Regulations to implement the CCPA and we look forward to reviewing the Final Regulations. We kindly ask again to please reconsider comments previously received from other credits, as well as the California Credit Union League (CCUL). We are available to discuss these comments at any time and would be pleased to provide further feedback to the AG upon request.

Sincerely,

Chris Allen

Chris Allen, Chief Risk Officer

PATELCO CREDIT UNION

Message

From: Kammerer, Susan [redacted]
Sent: 3/27/2020 2:06:29 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Merz, Jeremy [redacted]; Gleason, Angela [redacted]
Subject: CCPA Proposed Regulations - P&C Insurance Industry Coalition Comments
Attachments: 20-3-27 CA CCPA Revised Regulations - PC Coalition Comments (Final)_.pdf; 20-2-25 CA CCPA Revised Regulations - APCIA Comments - Final.pdf; 19-12-06 CA CCPA Regulations - APCIA Comments - Final.pdf

To Whom it May Concern:

Thank you for the opportunity to provide comments on the CCPA rulemaking process. Please see attached comment letter, (along with the two previously submitted letters).

Thank you,

Susan Kammerer
APCIA Western Region
1415 L Street, Suite 670
Sacramento, CA 95814
[redacted]



American Property Casualty Insurance Association
INSURING AMERICA apci.org

NAMIC
NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES
SHAPING OUR MUTUAL FUTURE®

PIFC
Personal Insurance Federation of California

March 27, 2019

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

VIA Electronic Mail: PrivacyRegulations@doj.ca.gov

To Whom It May Concern:

The American Property Casualty Insurance Association (APCIA)[1], Personal Insurance Federation of California (PIFC), and the National Association of Mutual Insurance Companies (NAMIC) appreciate the Attorney General's continued work and the opportunity to provide feedback on the revised California Consumer Privacy Act Regulations (revised regulations). APCIA strongly approves of the addition to Section 999.305, which clarifies that a business that collects personal information indirectly about consumers does not need to provide a notice at collection, if that business does not sell that information. There were also helpful clarifications in sections 999.313(d)(1) and 999.317(e)and(f). W320-1 W320-2 W320-3

Unfortunately, overall, the changes were not very substantive in nature and therefore many of our prior concerns remain. We refer to all of our earlier letters, and have attached a copy of the previous APCIA letter for your continued consideration, but emphasize the following issues: (1) While there have been some improvements, the revised regulation continues to focus on prescriptive, detailed and inflexible communication requirements; (2) The revised regulation continues to promote industry recognized standards for web content accessibility without recognition that what works for one industry may not work for another; (3) the prohibition on fees for verifications in Section 999.323(d) will prevent charging for the cost to obtain a notarized affidavit. The notary affidavit costs could be significant depending on the number of requests and may force companies to implement less robust authentication measures. We urge the Attorney General to clarify that a business cannot charge a direct fee for verification, but costs to the consumer, such as out of pocket expenses to provide required paperwork should be the consumer's responsibility; (4) continued expectations that businesses not only have to identify the category of personal information and the categories of third parties, but also to connect the W320-4

CCPA_2ND15DAY_00066

category of personal information and third parties, are beyond what the statute authorizes; (5) section 999.314(b) continues to perpetuate confusion by using "person or entity" instead of "business"; and (6) the telephonic notification and metric requirements are unworkable and not consumer friendly. W320-4 cont.

Additionally, the items identified below are new concerns raised by some of the substantive changes proposed in the revised (March 11, 2020) regulations:

999.301. Definitions

Sub-section (j) contains a change to the definition of "financial incentive." This would expand notice of incentives obligation in the regulations well beyond the non-discrimination right in the CCPA. Both the CCPA and its non-discrimination obligation apply to sale, right to know, deletion, access and portability rights, but do not regulate or apply to waivers of or collection of personal information. We believe this change creates ambiguity and request the changes be reversed. W320-5

999.302 Guidance Regarding Interpretation of CCPA Definitions

The second draft suggests deleting this new section. We respectfully request that it be retained. This provided some of the most helpful guidance in the regulation, particularly on IP addresses and the definition of personal information. W320-6

999.308 Privacy Policy

New sub-section (e) & (f) add categories of sources and the business or commercial purpose as required disclosures under the privacy policy. These exceed the elements of the privacy policy set out in the CCPA and are particularly problematic for companies that have already rolled out their CCPA privacy policies based on the statute and early draft of the regs. Importantly, (f), which requires disclosure of the business or commercial purpose for collecting or selling personal information, is not only onerous, but raises the question of whether the business can use the information for other legitimate purposes that may not have been disclosed. W320-7

999.313 Responding to Requests to Know and Requests to Delete

Sub-section (c)(4) has been amended to add provisions regarding the request to know and sensitive data: *"The business shall, however, inform the consumer with sufficient particularity that it has collected the type of information. For example, a business shall respond that it collects "unique biometric data including a fingerprint scan" without disclosing the actual fingerprint scan data."* This added layer of specificity is counterintuitive to the requirement to not give out the specific pieces of data. We are concerned that requiring more specificity provides more information for those seeking to commit fraudulent activities. W320-8

Since this new language adds administrative burdens and opens more doors for fraudulent activities without a sufficient argument as to its necessity, we request that it be deleted.

Thank you for the opportunity to comment. 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]

Seren Taylor
Senior Legislative Advocate
Personal Insurance Federation of California
1201 K Street, Suite 950
Sacramento, CA 95814
P: [redacted] | [redacted]

American Property Casualty Insurance Association
INSURING AMERICA apci.org

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. W320-4 cont.

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

[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.

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. W320-4 cont.

> 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

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."

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.

> 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.

W320-4 cont.

> 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

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.

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.

W320-4 cont.

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.

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.

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.

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.

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~~."

W320-4 cont.

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.

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."

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

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.

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?

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. W320-4 cont.

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."

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.

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.

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

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.

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.

W320-4 cont.

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?

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.

***

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]

American Property Casualty Insurance Association
INSURING AMERICA apci.org

December 6, 2019

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

VIA Electronic Mail: PrivacyRegulations@doj.ca.gov

To Whom It May Concern:

The American Property Casualty Insurance Association (APCIA) appreciates the opportunity to provide feedback on the proposed California Consumer Privacy Act Regulations (proposed regulations). 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.

The insurance industry has been subject to the Gramm-Leach-Bliley Act (GLBA) and implementing regulations in all 50 states and the District of Columbia for over two decades. In California, compliance obligations specific to insurers are found in Cal. Fin. Code §§4050, et seq.; Calif. Ins. Code §791 et seq.; and Calif. Code Regs. tit. 10, §2689.1 et seq. As recognized by the California Consumer Privacy Act (CCPA) exemptions, this foundation has served the industry and consumer well. Therefore, it is from industry experience and potential concerns raised by the lack of clarity in the CCPA that we provide the comments below for consideration in the development of the broader all industry regulation.

W320-4 cont.

General Observations

The proposed regulations demonstrate a thoughtful and diligent effort to balance competing concerns pertaining to the disclosure of consumer information that businesses collect and security and fraud risks that result from authenticating and providing this information to consumers in a portable manner. The proposed regulations also add clarity for what should be included in a tracking log, which will make it easier to develop compliance procedures. Unfortunately, many areas of the proposed regulation, especially those pertaining to notice, will only serve to increase consumer confusion and cause harm rather than promote meaningful consumer choice and transparency. For example, while well-

intentioned, the multitude of consumer notifications are contrary to the trend in consumer demand for shorter, yet informative, notifications.

Timing Concerns

In addition, there are requirements in the proposed regulations that pose substantial operational obligations that exceed, or conflict with, what the CCPA requires with no appreciable consumer benefit. The operational concerns are heightened by the short timeframe for implementation. While businesses are fully engaged in compliance efforts to meet the CCPA's January 1, 2020 effective date, the proposed regulations may, in some instances, require businesses to re-configure the labor- and capital-intensive technical configurations that have been undertaken in the past year to meet CCPA statutory obligations. It will be very difficult for businesses to retool their programs so close to the effective date. Consequently, a delayed or tiered effective date(s) of the regulation and "statement of prospective enforcement only" is essential.

A Complicated Notice Framework is not in the Best Interest of the Consumer

The proposed regulations outline various required consumer notices – notice at collection, notice of the right to opt-out, notice of financial incentive, and the privacy policy. Based on experience, we strongly believe this notification regime is not in the best interest of the consumer. The insurance industry has a long history of protecting consumer privacy and providing privacy notices and believe that it is not always beneficial to have more information, particularly extremely detailed, and repetitive information in its privacy policies and notices. Consumers can become inundated with information to the point they ignore it. In fact, the current insurance-specific privacy framework is built on a strong foundation of laws and regulations that have evolved to meet consumer expectations. For instance, the federal government recognized that consumer notices would benefit from a more streamlined and compact format. As such Congress and state insurance regulators have adapted their legal frameworks to meet this objective. As the Attorney General considers the abundance and detail of notification obligations, it should consider that for businesses that provide privacy policies at collection, the Notice at Collection, may not also be necessary or at the very least a notice as detailed as the one described in these regulations is not necessary.

W320-4 cont.

The specifics of our concerns are outlined in more detail below; however, APCIA highlights the following examples: (1) the notice at collection obligations suggest a possible interpretation contradictory to the CCPA that would require notices that would be so long and inflexible that consumers would become desensitized; (2) consent requirements inconsistent with the CCPA may introduce issues that frustrate and delay consumer transactions; and (3) operational challenges to harmonize all the notification obligations in the CCPA, these proposed regulations, and existing state and federal notification obligations. This proposed framework will only serve to complicate notices and confuse consumers.

Notice at Collection

Non-written communications

The proposed regulations prescribe the content, design and presentation of the pre-data collection notices. These prescriptions are focused on scenarios that contemplate an in-person or internet interaction between the business and consumer. Considering the motivation behind the CCPA, this

limited scope is understandable. However, insurers interact with consumers in a variety of media, including non-written means of communication such as telephone interactions.

APCIA recommends that the proposed regulations clarify in section 999.305(a)(2)(e) that in a non-written interaction with a consumer that it is sufficient to notify the consumer of the existence of the privacy policy and, as appropriate, the web address where the notice at collection and privacy policy can be found. This approach would be analogous to the in-person examples provided for in the proposed regulations.

Connecting the Business use with Personal Information

Section 999.305 (b)(2) requires that a business include in the notice at collection, "the business or commercial purpose(s) for which each category will be used." A strict reading may suggest that the notice should indicate separately for each category of personal information, how each category is going to be used. However, it is APCIA's interpretation that a strict reading is not consistent with the intent of the CCPA as it will have negative consumer consequences. To require a business to identify every innumerable reason for the initial collection of personal information that results in the need for a notice is unrealistic, unworkable, and does not create transparency for consumers in a meaningful way. For example, a consumer could be calling a business to report a claim, request information, ask for a quote, change a policy, etc. Depending on the reason for the call, the purpose for collecting the information would vary.

A strict interpretation is contrary to the Attorney General's objectives and effectively requires businesses to be so prospective and over inclusive that such notice would only serve to overwhelm the consumer. Further, businesses should be free to decide to abandon certain uses. Doing so means minimizing the use of personal information, which is fully consistent with the consumer privacy-protection policy of the CCPA. Lengthy notices or an abundance of notices are not in the consumer's best interest. W320-4 cont.

Such a strict interpretation is also beyond the statutory requirement contained in Section 1798.110(a)(3). Section 1798.110(a)(3) simply gives the consumer the *right to request* information about the business or commercial purpose for collecting or selling personal information. The statute suggests a more reasonable and consumer friendly approach that balances providing relevant information and the ability of the consumer to request additional information, if desired. Therefore, we recommend eliminating section 999.305(b)(2).

Requirement to obtain Affirmative Consent for New Uses of Information

In accordance with the CCPA, businesses do not need to collect consent for their disclosed uses of information when they first interact with consumers. There is no reason to require consent when businesses decide to make new uses, especially since consumers can request deletion of their personal information if they disagree with new uses disclosed to them. Further, obtaining "explicit consent" from anything beyond a de minimis proportion of consumers will be essentially impossible for many businesses.

Further, the CCPA does not require explicit consent; rather, it just requires notice of a new use. For the regulations to now require explicit consent is not only beyond what is contemplated by the statute, but it is in direct conflict with the language and intent of the CCPA.

Additionally, requiring explicit consent upon a businesses' use of personal information for a not yet specified purpose is problematic since a business may not be able to identify every use at the outset. This requirement will limit innovation as it would limit our business practices to what we identify as the current and possible future uses at the time the notices and privacy policies were drafted. To comply a business would have to produce massive disclosures, which would be nearly useless to the consumer given the disclosure's size.

APCIA recommends Section 999.305 be made to read as follows: "A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use ~~and obtain explicit consent from the consumer to use it for this new purpose~~."

If eliminating affirmative consent is not possible, which is our primary recommendation, the consent obligation should be limited to when there is a new use that is "materially" different from that previously specified. The Initial Statement of Reasons has referenced back to the Federal Trade Commission's report, "Protecting Consumer Privacy in an Era of Rapid Chang." (report). This report focuses on the need to get affirmative consent if certain material retroactive changes to the privacy practices were made. This materiality is determined on a case-by case basis based on the context of the consumer's interaction with the business. An example provided by the report would be sharing with third parties after committing to not sharing with third parties. This seems to be a more manageable and consumer friendly approach. Also, Article 6 of the General Data Protection Regulation (and Recital 50) has a compatibility standard that allows processing for a purpose other than that for which the personal data had been collected and is not based on the data subject's consent if it were compatible with the purpose for which the personal data was initially collected.

W320-4 cont.

CCPA Disclosure in the Privacy Policy

Section 995.305(b)(4) and (c) contradict one another. Section 999.305 (c) contemplates the ability to place the CCPA disclosure in the privacy policy; however, Section 995.305 (b)(4) suggests the opposite. For technical clarity, APCIA recommends amending (b)(4) as follows: "If the notice is not part of the business' privacy policy, a link to the business' privacy policy, or in the case of offline notices, the web address of the business' privacy policy."

Right to Opt-Out

While the proposed regulation is helpful in that it details when a business is exempt from providing a right to opt-out, it is very problematic to state that "[a] consumer whose personal information is collected while a notice of right to opt-out notice is not posted shall be deemed to have validly submitted a request to opt out." This requirement does not contemplate the fact that the notice may not be posted, because one is not needed or there is some inadvertent circumstance, like a website being down, that would essentially force the consumer to opt-out. This is not only troubling from a business perspective but could be frustrating to a consumer who had no intent to opt-out, but now may be subject to unintended consequences, such as product and service availability, that comes with this type of presumption.

APCIA respectfully recommends deleting this requirement or amending it to read: "A consumer whose personal information is collected while a notice of right to opt-out notice is not available, but should be, ~~posted~~ shall be deemed to have ~~validly~~ submitted a request to opt out, unless the unavailability of such notice is accidental, due to a website outage, or unanticipated and of short duration."

Privacy Notice

Privacy Policy Examples

As a general observation, the Initial Statement of Reasons suggests that the Attorney General would like to dictate the language to be used to identify "categories of sources" and "categories of third parties." We strongly recommend against creating prescriptive language requirements. Inflexible dictation of specific language will lead to inaccurate statements and as such consumer confusion. Given the CCPA's broad scope it is impossible to draft specific language that would apply universally to all businesses and all business practices. Nevertheless, illustrative examples, explicitly identified as nothing more than an illustrative example, of the categories of personal information may be helpful to allow some level of comparability or consistency in business application without requiring certain language that could be inaccurate and may change over time.

Availability in Multiple Languages

There is a requirement that the privacy policy must be available in the languages in which the business provides contracts, disclaimers, sale announcements, and other information to consumers. How is this supposed to work operationally for a global business? If a business operates in every country on the globe, does the privacy policy have to be in every imaginable language? It seems that the limitation should be that the privacy policy should be available in the languages in which the business provides contracts, disclaimers, etc. to California consumers. In addition, what does "other information to consumers" mean? Businesses may have individuals who speak other languages and as needed provide translation-type assistance. Does a business need to account for these potentially unknown customer service resources? The policies should advance the concept that the English language version prevails, in the event of any conflicts.

W320-4 cont.

APCIA recommends that the language of the proposed regulation clearly state that a business must only communicate notices in the languages it uses in California, clarify what "other information" means, and identify the English version as the controlling document. Such an approach would help address the uncertainty identified above.

Webpage Link for CA Specific Consumer Privacy Rights

The requirement to have a conspicuous link for consumer privacy rights has the potential to cause confusion for businesses that operate nationally. The business should be able to freely identify how it will conspicuously post its privacy policy in a way that benefits all consumers nationally.

Disclosure of the Verification Process

Section 999.308(b)(1)(c) should be deleted. This requirement provides no additional benefit for consumer transparency but does have the potential to cause harm. Given that there is no indication as to how much detail the business is expected to disclose about the verification process, including this in the privacy policy could overwhelm consumers. There may be different processes for different types of consumers and as

the business gains experience with the verification process, it may want to streamline and update its process. Changes to the process would then necessitate an update to the privacy policy and all the obligations that are associated with a privacy policy update.

More significantly, the verification process is intended to protect consumers from fraud and potential identity theft. This requirement, however, is diametrically opposed to this intention. Revealing the details of this type of process will put consumers at risk by providing critical procedural intelligence to potential bad actors who can use this knowledge to accumulate sensitive information from not only a CCPA disclosure but also other identity verification systems that rely on similar information. For example, information obtained through a CCPA disclosure could be the basis of a challenge question for gaining access to a consumer's financial accounts and information. For this reason and those noted above, we strongly urge the Attorney General to eliminate this requirement.

Notice of Improper Use of Minor's Data

Section 999.308(b)(1)(e)(3) is unnecessary redundant with other provisions of the regulation, since a business may not sell the personal information of a minor under 16 years of age without affirmative authorization.

W320-4 cont.

Too Many Required Disclosures in the Privacy Policy

Item 2 of subparagraph d in Section 999.308 subdivision (b) paragraph 1 significantly changes the disclosure requirements as defined in the law under sections 1798.110 and 1798.130. The law does not require that the items in these sections be reported ***per category of personal information***.

This additional level of granularity exceeds statutory obligations. It will lead to a more convoluted disclosure and will cause consumer confusion while essentially rendering the disclosure meaningless due to the vast repetition of information across the personal information categories.

Additionally, while on the surface this change seems rather simple, it is in fact exponentially more complex from a technical perspective and would place undue burden on many businesses to develop the capability to report the information with this additional level of detail.

For these reasons, this requirement should be eliminated or reworded to remove this added level of complexity and increased scope of the law.

Responding to Requests to Know and Delete

In some ways the proposed regulations add helpful clarification as it relates to data deletion. However, many of the deletion requirements in the proposed regulation are beyond what is provided for in the statute or they enhance existing CCPA concerns. The practical implication of these concerns includes a level of uncertainty as to how to fulfill a request to delete when the business needs the information to fulfill its obligations and in some situations, such as data backup, is necessary to protect information systems.

Section 999.313(a) is beyond the statutory requirements and should be deleted. For the same concerns outlined earlier in this letter, a business should not be required to detail its verification process.

Also, the proposed regulations applied timeframes in 999.313(b) are not found in the statute. If the proposed regulations can apply a 45-day limit on deletion requests, does this also mean businesses only have to delete the previous 12 months' data?

Requests to Know

Further, 999.313(c)(4) should be amended as follows: "A business shall not at any time in response to a consumer's request to know, disclose a consumer's social security number, driver's license number . . ." This additional language adds certainty to the scope of this prohibition and prevents any unintended consequences that would limit a business' ability to use this information in a situation that may be necessary to verify an individual's identity such as in the case of a father and son who have had the exact same name and live in the same house.

APCIA also believes it is important to have a clear sentence in section 999.313 (c) that excludes businesses from disclosing personal information obtained for insurance fraud investigating purposes. A new sentence that states the following is important: "A business shall not at any time disclose personal information that such business collects pursuant to its obligations to conduct fraud investigations under the California Insurance Fraud Prevention Act (California Insurance Code Section 1871, et seq.) and any other state or federal statute or regulation regarding the conduct of a fraud investigation."

Additionally, if a business denies a consumer's verified request, Section 999.313(c)(6) outlines strict communication requirements for identifying the basis of the denial. This detailed information will provide no value to the consumer. What's more, providing such information would create technical difficulties that most businesses would have trouble meeting. For example, the right to delete has many exceptions under CCPA, including where information must be retained for legal reasons or to satisfy a contract with the consumer. These are particularly relevant in the insurance and financial services industries. The proposed regulations would require any denial to delete on such grounds to "describe the basis for denial, including any statutory or regulatory exception therefor." Consumers generally do not, and should not, be expected to understand the overlapping and nuanced legal frameworks that apply to their interactions with regulated industries. Providing such information will only cause confusion and adds nothing meaningful to the consumer's understanding.

W320-4 cont.

Further, the requirement to provide an individualized response to the consumer when responding to a verified request is beyond the scope of the statute and does not provide enhanced transparency in any meaningful way. In fact, the requirement is so extensive that it has the potential to overwhelm consumers and is truly unmanageable for businesses. Ideally, section 999.313(c)(9) should be deleted; however, at the very least, the statute clearly does not require individualized categories of third parties or business purposes and these references must be deleted.

At the same time there is guidance provided on how to respond to a verified request for categories of information, but there is no guidance on how to respond to a verified request for specific personal information. Further, sections 999.313 and 999.325(b) and (c) discuss two different types of requests, one for specific pieces of information and one for categories of information; nevertheless, there is no real differentiation between what is considered a category and what is considered a specific piece, particularly, where there is an overlap. It would be helpful to have examples of what is a category vs. what is a specific

piece of information. Ultimately, there are too many consumer notices that provide redundant and detailed information where category information should be sufficient.

Moreover, there is a blanket requirement that if a business could not verify the identity of the requestor it must deny the request to delete and, instead, treat the request as one to opt-out. Our position is that 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 giving the ex-spouse the authority to automatically opt the current consumer out of anything. This appears contrary to the rights that the CCPA advocates for, such as individual control.

Requests to Delete

Data deletion requirements in the proposed regulation that are out of statutory scope include, but are not limited to: (1) the automatic opt-out if a deletion request cannot be verified is new scope; (2) the requirement for deletion on archived/back up system based on the next time it is accessed or used; (3) disclosing the manner of deletion to the consumer; (4) the suggestion that partial deletion is permissible; and (5) prohibiting the use of retained personal information except for the reason disclosed is problematic (there may be multiple reasons that data is collected).

W320-4 cont.

Significantly, Section 999.313 (d)(3), which permits a business to delay compliance with a request to delete information stored in an archive or backup system until the system is next accessed, is inconsistent with 999.313(d)(2)(a), which requires permanent deletion by erasing information on existing systems with the exception of archived or back-up systems. We urge the Attorney General to delete 999.313.(d)(3) altogether or provide a lot of clarification about what Is meant by this requirement. For example, a backup system is "accessed" when it performs additional backups. A business does not generally have the ability to delete information a requirement like Section 999.313(d)(3) may be interpreted to require.

Also, various sections of the CCPA provide consumers the right to request that a business delete self-provided personal information. There are also numerous exceptions to this rule, yet despite these exceptions the proposed regulations still require businesses to respond to each deletion request. This will require a significant amount of time, both of the business and the consumer. The proposed regulations should exempt businesses that only collect personal information covered by a deletion exemption. This exemption could be structured in the same manner as the one found in section 999.306 (d), which exempts businesses that do not intend to sell information from notifying consumers of their right to opt out of the sale of such information.

Service Provider

As drafted proposed regulation sections 999.314(a) and (b) are ambiguous.

Authorized Agent

The definition of an authorized agent is unclear. Do both a natural person and a business entity need to register with the Secretary of State and what are they registering? There is also a lack of clarity on how a business is supposed to verify an authorized agent's request. Further, it should not be the business community's obligation to tell consumers how to designate an authorized agent, but rather the Attorney General should determine the process for Secretary of State registration and provide and explain such process on the Attorney General's website. At the very least, the proposed regulation should be amended

to require the privacy policy to only alert the consumer that they can designate an authorized agent. APCIA recommends the following amendment to Section 999.308(b)(5)(a): "Explain ~~how~~ that a consumer can designate an authorized agent…"

Methods for Submitting Requests

APCIA urges the Attorney General to delete sections 999.312(f) and 999.313(c)(1). The proposed regulations require extensive detailed request responses that create new obligations and layer CCPA's rights on top of one another. The result creates work-flow processes and exception that would be difficult, if not impossible to automate, train internally, and improve going forward. The proposed regulation requires businesses to treat each request under the "right to know" or the "right to delete" as potentially another kind of request – if specific pieces of information were not available, provide categories of information per this section and if deletion were not available, submit an opt-out request per (d)(1).

The option in 999.312(f)(1) to allow a business to treat a deficient request as if it was submitted in accordance with a designated manner could be problematic under various circumstances. For instance, if a consumer wrote "delete my data" on a napkin and handed it to a business' employee, should that business now have an obligation under 999.312(f)(1) despite the alternative outlined in (f)(2)?

W320-4 cont.

The cascading effect created by these new obligations is truly problematic as noted above. The level of complexity this would add to the verification and disclosure processes will make business work flows unsustainable and create unintended confusion for consumers.

APCIA recommends that if the consumer submits a request that is not readable and understandable, it should only be required to provide the consumer with the specific directions on how to submit the request correctly.

A request to know specific pieces of information requires signed declarations under penalty of perjury, but there is no clarity on how to execute such declaration. Also, to determine the level of certainty needed (reasonable or reasonably high), does the consumer have to detail whether he/she were requesting categories or specific pieces of information within his/her request? Could a business default to one standard over the other, if the consumer did not specify or does the business have to reach out to the consumer to determine the consumer's request with specificity?

Requests to Opt-Out

Section 999.315 could be interpreted to require all businesses to provide a "Do Not Sell" link, This would be inconsistent with CCPA Section 1798.135, which only requires a business that sells the consumers' personal information to third parties to provide the "Do Not Sell" link. We recommend that all sub-sections of 999.315 be limited to those businesses selling consumer's personal information.

The Attorney General should also consider the practical implications of the proposed opt-out requirements. For instance, if a business is required to accept an opt-out request via webform, how do they do this for cookies? A business can associate a cookie with a machine, but not a specific individual. It is not just a cookie issue, but concerns device ID's. To interpret the requirements in this manner seems contrary to the objectives of the CCPA, because businesses would need to start collecting more data to

make personal connections they do not already make. The drafters need to be careful to take a technology neutral approach that will remain useful with technological evolution.

Section 999.315(c) and the last sentence of (g) should be deleted as they envision an implied opt-out. All expressions of opt-out should be express as envisioned by the statute. To permit an implied opt-out only creates significant technical problems. In addition, this section is confusing because it contemplates that the browser communicates a signal as to the consumer's opt-out choice. A browser sends a "do not track" signal, not an "opt out of sale" signal. These represent different choices. A do not track signal does not prevent collection and sharing of information; it only expresses a desire to cease the use of behavioral advertising. This is another example where the breadth of the CCPA and proposed regulations haven't fully contemplated the entire potential impact of the proposed regulations beyond the technology firm business model that served as the motivating factor for the CCPA.

Subsection (g)(2) of 999.317 should be deleted as it is an overreach and not required by the statute. The statute does not identify that the privacy policy include statistical data on the number of consumer requests and how the company handled these. More importantly this section will only serve to confuse the consumer by adding yet another piece of information to include or be linked from the already overburdened privacy policy. This type of statistical data serves no meaningful purpose for the individual consumer.

W320-4 cont.

Definitions

The definition of categories of sources is not helpful in a meaningful way. As an example, if "publicly available" information were not "personal information, then "government entities from which public records are obtained" would not be within the "categories of sources" from which a business collects personal information.

The examples of "categories of third parties" makes sense for the "mobile ecosystem" but does not make much sense for "the broader spectrum of businesses that collect personal information," particularly when personal information is not collected electronically.

CCPA Scope

There remain questions regarding the territorial reach of the CCPA. The Attorney General could add clarity in this respect by explaining that the revenue thresholds apply to revenues derived solely from California. Additionally, guidance that limits scope to protect California citizens could include clarifying: (1) that "device" apply solely to devices used/owned by California residents; and (2) application of the CCPA and implementing regulations only to California households (there are statements in the implementing regulations that suggest this, but a specific statement would avoid any doubt). These requests seem consistent objectives of the CCPA and proposed regulations, but specific statements would be helpful.

***

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]

Message

From: Fatima Khan [redacted]
Sent: 3/27/2020 1:54:05 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCPA Proposed Regulations Comments
Attachments: Okta_PublicComment_CCPA_3.27.20_Final.pdf

Hi –

Please see the attached document for Okta's comments. Thank you for your consideration.

Best,
Fatima

March 27, 2020

The Honorable Xavier Becerra
California Attorney General
California Department of Justice
Attn: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Via E-mail: privacyregulations@doj.ca.gov

Re: California Attorney General – California Consumer Privacy Act of 2018: Proposed Regulations
Comments of Okta, Inc.

Dear Mr. Attorney General Becerra:

Okta, Inc. ("Okta") appreciates the opportunity to provide these comments in connection with the California Attorney General's ("AG") proposed regulations for the California Consumer Privacy Act of 2018 ("CCPA").

Okta Overview

Okta is a publicly-traded (NASDAQ: OKTA) cloud computing company that offers identity and access management software-as-a-service to businesses, governments, non-profit entities, and other organizations across the United States and around the world. Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables the company's customers to securely connect people to technology, anywhere, anytime and from any device. The company was incorporated in January 2009 as Saasure Inc., a California corporation, and was later reincorporated in April 2010 under the name Okta, Inc. as a Delaware corporation. Okta is headquartered in San Francisco, California.

Okta's customers use our services to work with some of their mission-critical, sensitive data, including the names, email addresses, and mobile phone numbers of their users. As a growth company, Okta continues to surpass key milestones, including serving millions of users [1]. Accordingly, acting with integrity and transparency, so that we earn and maintain our customers' trust, is critically important to all of us at Okta. To that end, Okta maintains privacy protections across its suite of services, as detailed in our third-party audit reports and standards certifications.

Although many companies may view privacy compliance as a burden, Okta views it as a strategic differentiator and a competitive advantage — we provide tools and resources to our customers, to help ensure that their own systems are kept safe and secure, so that critical data can remain private and protected.

For these reasons, Okta commends California's current work towards implementing a comprehensive privacy law with the hope that such law protects consumers and enables businesses to strengthen their approach to privacy through clear compliance obligations. Okta's approach to privacy aligns with the CCPA, including support for the view that "it is possible for businesses both to respect consumers' privacy and provide a high level transparency to their business practices."[2]

Introduction

Okta agrees with the AG's sentiments that today more than ever, strong privacy and security programs are essential to the people of California and our economy.[3] As technology advances, California is continuously the leader at the forefront of protecting the privacy and security of consumers, and Okta supports the state's efforts. In addition to being a trailblazer in protecting consumer privacy, Okta also encourages the state of California and the AG to remain engaged with both federal and other states' efforts | W321-1

to further privacy protection in order to create regulation and guidance that will best allow companies to strengthen privacy practices for consumers. W321-1 cont.

Furthermore, Okta encourages California to continue to advance consumer privacy through risk-based, flexible privacy regulation that provides clear compliance obligations for businesses. We believe that being unduly prescriptive can result in stifling compliance checklists that inhibit the creation of innovative privacy solutions or frustrate consumer privacy efforts due to implementation hurdles. Benefits should be measurable and quantifiable, and any new state privacy legislation should first take into account the outcomes sought by consumers, and also align with California residents' understanding of meaningful data protection. W321-2

Key Points for Consideration

We offer three key areas for consideration as part of the AG's analysis on updating the proposed California Consumer Privacy Act Regulations ("Proposed Regulations").

First, it is important that the AG account for the complexity of technology and the different scenarios that arise through the use of personal information. Okta is aware of the risks associated with processing personal information and believes that there are instances when businesses best positioned to protect consumer privacy and security through the use of personal information may have to provide privacy rights to individuals that have an unintended effect of undermining security or otherwise result in a disproportionate impact on the business to make compliance unachievable. As follows, it is important to ensure that the CCPA accounts for different business models and proportionately scopes individual rights to ensure that there is no substantial adverse impact on security measures required by other sections of the CCPA, not impact maintenance of personal information for compliance or legal purposes, or otherwise require disclosure of personal information that cannot be accessed by the business without undue burden. W321-3

Second, Okta wishes to comply with the CCPA and requests that the California AG clarify the difference between "Personal Information" and "Deidentified" information. As a service provider that must use data in specific ways to protect its Customers and promote general Internet safety for its users, Okta requests that the California AG clearly delineate the difference between the two defined terms and reinstate the previous illustrative example or otherwise provide further clarification. W321-4

Third, Okta believes that the CCPA would benefit from clarification and alignment with existing global and federal privacy and security standards around identity, to ensure that proper identity verification is in place for consumer privacy rights requests. In line with these global standards, Okta encourages the AG add in a clarification to require businesses to use multi-factor authentication (MFA), when possible, for satisfying requests to know or delete, to prevent the abuse of privacy rights and to ensure personal information is only furnished to individuals upon a properly verified request. W321-5

1. Request the clarification of section 999.314(c)(3) of the Proposed Regulations to reinstate the previously proposed exception for security and update the new test to a three-pronged test.

As stated in the CCPA, "it is almost impossible" to conduct even the most mundane tasks without sharing personal information.[4] Based on the pervasive need to collect personal information to carry out even the most simple technical tasks, it is important for the state of California to account for the wide array of business models that need to collect personal information to carry out the services they provide to consumers and to businesses. Okta does not monetize personal information, but provides a cloud-based enterprise solution that helps to streamline identity management and increase efficiencies for companies and their end users to securely access cloud-based applications, including by processing data to help our customers protect against pervasive security threats. W321-3 cont.

Section 999.313(c)(3) of the Proposed Regulations states that a business is not required to search for personal information only if a four-pronged test is met. Okta believes that these four prongs are important and should remain in the Proposed Regulations; however, Okta requests that the California AG clarify the

exceptions to constitute two separate exceptions – a more precise security exception and a three-pronged test:

a. Reinstate the previously included security exception and clarify the standard required for the exception to enable compliance with the Proposed Regulation:

In harmony with security requirements found within the CCPA and other existing California law that requires companies to implement and maintain reasonable security procedures and practices, Okta requests the clarification of section 999.313(c)(3) of the Proposed Regulations to reinstate the security exemption to the right to know. The previously included security exception should be reinstated because it prevents bad actors from being able to access personal information and circumvent security controls after these bad actors have been identified as such. For example, if a service provider provides security insights to its customers and empowers customers to use that information to prevent bad actors from perpetrating malicious attacks, then providing the same data to a bad actor through the right to know enables the bad actor to take an alternative approach when they have the right to access the associated personal information. As a result, companies and their customers become engaged in a longer cat-and-mouse game to catch the bad actor and security controls become less valuable for maintaining security.

Okta further requests that the California AG reinstate the previous exception with a slight change to use a "reasonable" standard that is "articulable". As follows, businesses would be able to apply the existing "reasonable security" standard to ensure compliance with the Proposed Regulation rather than trying to understand how to apply a new standard of "substantial". As such, we request the removal of the word "substantial" to avoid arbitrary judgments and application of the law based on an unclear standard not based in existing law. Such a clarification is consistent with the implementation of existing *reasonable security* standards because by sharing personal information where the disclosure "creates an articulable and unreasonable risk to the security" of the individual or a business' systems or networks would be tantamount to creating a right directly in conflict with reasonable security measures. W321-3 cont.

Proposed language:

- *A business shall not provide a consumer with specific pieces of personal information if the disclosure creates an ~~substantial and~~ 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.*

b. Update the proposed four-pronged test to the following three-pronged test to enable businesses to comply:

Okta supports the California legislature's provision of reasonable and legitimate personal information to individuals. Such rights should be balanced against legitimate and articulated concerns that could impact businesses, their customers, and overall individual and Internet safety. With this balance in mind and an aim to enable compliance with the Proposed Regulation, Okta requests that the California AG change the four-pronged test to a three-pronged test. If businesses are required to satisfy requests for the right to know, Okta agrees that the business should be subject to reasonable restrictions, including (1) no sale of the personal information and no right to use personal information for a commercial purpose, and (2) the business should be required to provide sufficient transparency about what information the business did not search. As the third prong, we request that either of these two requirements, not both, be required to satisfy the test: (3) (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.

For example, a business may maintain either backup data that cannot be readily searched or data that is subject to special security requirements where it cannot be readily accessible or searched. Creating a right to know in these two situations could result in undue cost and operational burdens to access personal information that is not easily accessible and otherwise maintained in a fashion that is

protected and the data is put "beyond use", such as backup tapes or unstructured data or data that has to be reviewed manually. Removing rights to access data "beyond use" would also enable businesses to comply with the Proposed Regulation in a manner that is interoperable with existing global standards on data access rights.[5] In addition to this, creating a right to know for personal information that is protected by strong security measures and not otherwise readily accessible can effectively undermine security protections in place to protect that same personal information because businesses will need to implement an additional operational process to access such personal information not readily available. In another situation, a business may be required to maintain specific personal information based on legal or compliance reasons where it does not otherwise process the personal information except to maintain it. Adding in a right to know for such personal information requires a business to create an additional process to analyze and process such personal information in addition to only maintaining it as necessary.

Okta agrees with the California legislature that the right to know is important, and to enable businesses to adequately comply with this right, requests that this right is scoped appropriately using a reasonable test.

Proposed language:

W321-3 cont.

- *In responding to a request to know, a business is not required to search for personal information if all of the following conditions are met:*

  (a) The business does not sell the personal information and does not use it for any commercial purpose;
  (b) 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; and
  (c) Either: (i) the business does not maintain the personal information in a searchable or reasonably accessible format; or (ii) the business maintains the personal information solely for legal or compliance purposes.

2. Request for the clarification of information that is not necessarily classified as "Personal Information" or "Deidentified" information.

At present, "Personal Information" is defined as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household". In contrast, "Deidentified" means "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, direct or indirectly, to a particular consumer, provided that a business that uses deidentified information: (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain. (2) Has implemented business processes that specifically prohibit reidentification of the information. (3) Has implemented business processes to prevent inadvertent release of deidentified information. (4) Makes no attempt to reidentify the information." While these definitions seem to be the opposite in nature, there are "safeguards" or "processes" that need to be applied even when information is deidentified to qualify it as not "Personal Information" per section 1798.140(o)(3). In turn, there is a gap between the definitions of "Personal Information" and "Deidentified" that require clarification and illustrative examples to enable businesses to comply with the law.

W321-4 cont.

As follows, Okta requests that the California AG reinstate the illustrative guidance removed in the last iteration in section 999.3012 *Guidance Regarding the Interpretation of CCPA Definitions* or instead provide similarly clarifying guidance in the next revision.

Propose reinstatement of the following:

§ 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."

W321-4 cont.

A failure to include such illustrative guidance results in a gap for information that is already maintained in a manner that is not "Personal Information" but does not necessarily merit the application of "safeguards" and "processes" required by the definition of "Deidentified" because it already is processed in a manner in which it is not considered "Personal Information". Clarity on how such information should be defined and the steps required by a business to ensure it is "Deidentified" would be helpful to understand how to classify information and enable businesses to take the steps necessary to ensure such information is considered "Deidentified".

3. Request for the inclusion of multi-factor authentication as part of identity verification process for privacy rights requests.

Okta is at the forefront of identity verification and promotes using secure practices to enable consumers to delete or access, view, and receive a portable copy of their personal information, in line with reasonable data security controls. According to Trace Security, 81% of company data breaches are due to poor passwords [6] and using multi-factor authentication ("MFA") is an easy way to prevent most cyberattacks and helps protect against fraudulent requests. To avoid having an adverse effect on individual privacy, we believe that the verification process described in section 999.313 (*Responding to Requests to Know and Requests to Delete*) and 999.324 (*Verification for Password Protected Accounts*) of the Proposed Regulations should be robust and include appropriate identity verification steps before permitting access to individuals' personal information.

In section 999.323 (*General Rules Regarding Verification*) of the Proposed Regulations, the AG notes that businesses must account for "the likelihood that fraudulent and malicious actors would seek the personal information" and determine "whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests…". This acknowledgement of potentially fraudulent activity through the verification process prompts the need for the AG to clearly require MFA, when appropriate, as part of the verification process including listing it as one type of "available technology for verification" described in section 999.323(b)(3)(f). The approach to use multiple factors is consistent with privacy guidance recently released to verify identity for responding to individual rights requests under the General Data Protection Regulation, such as to access personal information.[7]

W321-5 cont.

As indicated in section 999.323(d), the verification standards put forward by the AG should prioritize guidance on implementation of reasonable security as part of the process by either (i) requiring businesses that maintain a password-protected account with the consumer to use of MFA to delete or access, view, and receive a portable copy of their personal information under sections 999.313(c)(7) and 999.324 or (ii) making the use of MFA to verify identity based on the existing account details on file as an alternative to collecting additional personal information from an individual for verification in line with the requirements under sections 999.323(c) and 999.325 (*Verification for Non-account holders*). The foregoing clarifications to utilize MFA for verification when appropriate are also consistent with the reasonable security measures to detect fraudulent identity described in section 999.323(d). We encourage lawmakers to look at security frameworks to make sure that privacy processes are developed with security in mind. Requiring the use of MFA is interoperable with existing federal security frameworks [8] and helps to promote more secure identity access management processes for personal information sharing.

In sum, including the requirement to use MFA, when appropriate, would allow the state of California to further twin aims to both promote privacy and require reasonable security in furtherance of consumer rights.

Conclusion

Okta praises the State of California's work in this area and appreciates the consideration of our views and perspectives. While Okta is firmly in favor of strengthening consumer privacy and security, we also understand the challenges and high compliance costs, productivity losses, and administrative burdens that arise as an effect of disparate regulatory requirements. Okta welcomes further discussions in this area and is happy to serve as a resource for the AG.

Respectfully Submitted,

Okta, Inc.
Privacy and Product Legal Department
legal@okta.com

---

[1] "Okta Now Has Over 100 Million Registered Users, Says CEO" - https://finance.yahoo.com/news/okta-now-over-100-million-234824968.html
[2] AB-375 Section 2(h)
[3] https://oag.ca.gov/privacy
[4] AB-375 Section 2(h)
[5] https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf
[6] https://www.tracesecurity.com/blog/articles/81-of-company-data-breaches-due-to-poor-passwords
[7] Rights of data subjects guidance, Autoriteit Persoonsgegeven (Dutch Data Protection Authority) https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen#hoe-kan-ik-de-identiteit-vaststellen-wanneer-iemand-zijn-haar-privacyrechten-uitoefent-7212
[8] Draft NIST Special Publication 800-207, Zero Trust Architecture; NIST 800-63, Digital Identity Guidelines; and NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

Message

From: Daly, Barbara [redacted]
Sent: 3/27/2020 1:58:22 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCPA Regulations Comment Letter
Attachments: 2020.03.27 - CCPA Reg Comments final.pdf

Attached please find comments regarding the second set of modifications to the California Consumer Privacy Act Regulations.

Sincerely,

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

March 27, 2020

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

RE: Second Set of Modifications to the Proposed California Consumer Privacy Act Regulations Released March 11, 2020

Dear Ms. Kim:

The Transportation Corridor Agencies (TCA) are two joint powers authorities, comprised of the 18 cities and three county supervisorial districts in Orange County, formed to plan, finance, construct, and operate Orange County's 51-mile toll road system. TCA, along with twelve other agencies in California, have implemented a statewide electronic toll connection system, branded as FasTrak®, to enable road users to be charged for and pay tolls for their toll road usage with a single account.

TCA offers this letter as a supplement to its February 25, 2020, comments on the First Set of Modifications to the Proposed California Consumer Privacy Act (CCPA) Regulations. This letter further explains TCA's concerns regarding the Proposed Regulations.

As a government entity, TCA is not a "business" subject to the CCPA. The Proposed Regulations provide, however, that the definition of "categories of third parties" includes government entities. The inclusion of government entities as categories of third parties could hamper the ability of TCA and other toll operators in the state to carry out their governmental functions.

Therefore, we are writing to you today to request that the Attorney General confirm in the Proposed Regulations that a government entity is, in fact, not subject to California Civil Code section 1798.115(d) when it releases, discloses, or otherwise makes available personal information to carry out its governmental functions. In particular, TCA believes that it is not subject to section 1798.115(d) if it releases, discloses, or otherwise makes available personal information to enable toll road interoperability or support the collection and enforcement of tolls.

W322-1

We believe this interpretation is consistent with the spirit behind other parts of the CCPA. For example, section 1798.145 includes exemptions to permit entities to comply with federal, state, and local laws and to pursue legal claims. California toll agencies operate under several state statues that govern the collection and enforcement of tolls, as well as the requirement for statewide interoperability, all of which dictate the sharing of data. ***Given the important considerations at stake, TCA requests confirmation that its interpretation is accurate and asks the Attorney General to make this point clear in the final CCPA regulations.***

By way of background, California Civil Code section 1798.115(d) states that "[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. . . ." "Sale" is broadly defined to mean "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration." Cal. Civ. Code § 1798.140(t)(1).

Section 999.301(e) of the Proposed Regulations, in turn, defines "categories of third parties" to include "government entities." If a government entity is considered a third party, the CCPA should not be misinterpreted to restrict government entities' ability to carry out their functions in ways not intended in the law.

Electronic toll collection systems enable users to have an account with a single toll operator and pay for use of tolled roadways throughout California and in states across the country. 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.

W322-1 cont.

In order to have interoperable payment systems, toll agencies must be able to share information with other government entities, toll road operators, and third-party service providers necessary to collect tolls. Application of section 1798.115(d) to public toll road operators like TCA could be wrongly interpreted to restrict their ability to share necessary information and, in so doing, prevent California toll operators from complying with federal requirements to have a national interoperable toll system.

In addition, TCA must share information with other government entities and certain third party service providers to enforce tolls. It is critical that TCA be able to enforce tolls since it relies on toll revenues for operating expenses, capital improvements and to pay down the debt it incurred to construct The Toll Roads.

Given the points discussed above, TCA requests that the Attorney General confirm in the final CCPA regulations that a government entity acting as an operator of a toll road is not subject to Section 1798.115(d) if it releases, discloses, or otherwise makes available personal information to carry out its governmental functions, including to enable toll road interoperability and support the collection and enforcement of tolls.

We appreciate your consideration of these important issues.

Sincerely,

Samuel Johnson
Chief Toll Operations Officer

Message

From: Gibbons, Jennifer [redacted]
Sent: 3/27/2020 2:14:28 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Desmond, Edward [redacted]; Leigh Moyers [redacted]; Sheila Millar, Esq. [redacted] Pasierb, Stephen [redacted]
Subject: CCPA Revised Regulations -- Toy Association Comments March 2020
Attachments: TA Comments to CA AG Second Revision to Proposed CCPA Regulations_032720.pdf

Hello,

Attached, please find comments from the Toy Association, on behalf of its members, regarding the second revision to the proposed California Consumer Privacy Act (CCPA) regulations.

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

March 27, 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 Second Set of Modifications to Proposed Regulations Under the CCPA

Dear Attorney General 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 Second Set of Modifications to the Proposed Regulations (Proposed Regulations) implementing the California Consumer Privacy Act (CCPA) (Cal. Civ. Code §§ 1798.100–1798.199) noticed on March 11, 2020. As we indicated in our earlier two sets of comments, incorporated by reference herein, 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.

TTA greatly appreciated the changes the Attorney General (AG) made in the first set of modifications to the Proposed Regulations, which addressed several of the concerns TTA expressed in its first set of comments. However, TTA is disappointed that the AG chose not to adopt the simple and straightforward changes recommended by TTA in its February 25, 2020 comments. These changes would have gone a long way to addressing the conflicts between the CCPA and the Children's Online Privacy Protection Act (COPPA), as well as some specific operational problems in implementing the CCPA. As TTA noted previously, COPPA preempts inconsistent state laws. Provisions of the CCPA and any final implementing regulations that are inconsistent with COPPA will not be enforceable, so the failure to make the recommended changes is puzzling. Equally importantly, however, the changes we recommend have demonstrably been effective in the children's privacy arena, allowing businesses to operate while protecting children's privacy. The existence of conflicting requirements creates regulatory uncertainty and complicates the efforts of companies to come into compliance with the CCPA and implementing regulations. W323-1

TTA reiterates the need for the following changes to address the conflicts and inconsistencies between COPPA and the CCPA and its implementing regulations, as well as to reduce unnecessary burdens on businesses and consumers:

- 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." The change in the Proposed Regulations, replacing "whether" with "that" in § 999.330(c) is helpful, but lacks the clarity that an affirmative statement limiting such requests to parents and guardians, as TTA recommends, would have. W323-2

- Amend § 999.314, allowing service providers to use or disclose personal information for certain reasons to exempt the *full* range of activities constituting "support for internal operations" recognized by the Federal Trade Commission (FTC) for both service providers and businesses. Companies have relied on the FTC's "support for international operations" provision to conduct business-critical activities in a privacy-safe way when handling the sensitive personal information of children. There is no evidence that these activities have resulted in any privacy harm to children. Because the FTC's approach protects the privacy of children, there is no reason that they should not equally apply to handling the personal information of teens and adults. W323-3

- Amend § 999.330(a)(2) to explicitly permit the use of new methods for verifying parental consent that may be 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). W323-4

- To lessen the burden on parents making requests to access or delete household information which includes information of children under the age of 13, amend § 999.322 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. W323-5

Conclusion

TTA applauds the AG's willingness to continue its review and reconsideration of the Proposed Regulations, and to give affected stakeholders the opportunity to comment on these important proposed regulations. TTA appreciates the AG's previous changes addressing many of its comments, and also welcomes the AG's deletion of the requirements for a "Do Not Sell" button in the Proposed Regulations. W323-6

As a signatory to March 17, 2020 letter from 66 trade associations, companies, and organizations requesting temporary forbearance from CCPA enforcement in light of the coronavirus pandemic, TTA stresses the urgent need for both clarity in the regulations, consistency with preemptive laws like COPPA, and adequate time for businesses to plan to implement new regulatory requirements. It is more critical than ever to meet these goals to avoid unnecessary burdens on businesses and their employees during these difficult and uncertain times. For example, for some companies to ensure that they have fulfilled their obligation under the regulations to provide all data collected or to ensure fulfillment of a data deletion request within the timeframes mandated, it may be necessary for those companies to have employees W323-7

onsite at their places of work or to require that employees engage in non-essential travel and other actions that may not be consistent with social distancing norms and obligations. Avoiding unnecessary risks to employees tasked with responding to these requests - not just in California, but across the country – and assuring that those businesses meet local and state mandates to protect workers and the public by sheltering at home are also compelling reasons to delay enforcement. W323-7 cont.

With that in mind, we also urge the AG to work with the California legislature to delay application of CCPA obligations as to handling of employee data for at least one year. It is hard to see how there will be adequate time to update regulations to address employee data with adequate time for the business community to review and comment on them, and for businesses to consider operational impacts of those changes, implement and test compliance measures, and still meet a January 1, 2021 timeframe. W323-8

The toy industry remains steadfast in its support for strong national consumer privacy and data security frameworks. We hope this submittal will assist the AG 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

Message

From: Howard Fienberg [redacted]
Sent: 3/23/2020 2:02:26 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Stuart L. Pardau [redacted]; Blake Edwards [redacted]
Subject: CCPA round 3 comments
Attachments: Insights Association CCPA Comments 3-23-20.pdf

I've attached comments from the Insights Association on the AG's 3rd draft of CCPA regulations.

Sincerely,
Howard Fienberg
VP Advocacy
The Insights Association
[redacted]
1156 15th St, NW, Suite 700, Washington, DC 20005
http://www.InsightsAssociation.org

(In 2017, CASRO and the Marketing Research Association (MRA) merged to form the Insights Association, representing the marketing research and data analytics industry.)

The Honorable Xavier Becerra
Attorney General, State of California
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

March 23, 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 third draft of the regulations circulated by your office on March 11, 2020.[1]

As previously indicated in comments submitted on December 6, 2019[2] and February 25, 2020[3] regarding the first two drafts of CCPA regulations, both of which are attached hereto (attachments #1 and #2, IA is the leading nonprofit trade association for the marketing research and data analytics industry and represents more than 545 individual and company members in California, with more than 5,500 members in total. Virtually all of these members will fall within the jurisdiction of the CCPA due to the fact that personal information of California residents is collected and transmitted for legitimate purpose by marketing research and data analytics companies and organizations in most instances. Since CCPA will have a profound impact on our industry, we appreciate the opportunity to submit additional recommendations on the latest draft of CCPA regulations.

After explaining who we are and what marketing research is, these comments will cover seven main points

[1] https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-second-set-mod-031120.pdf

[2] IA comments on 1st draft:
https://www.insightsassociation.org/sites/default/files/misc_files/insights_assoc_ccpa_reg_comments_12-6-19.pdf

[3] IA comments on 2nd draft:
https://www.insightsassociation.org/sites/default/files/misc_files/insights_association_ccpa_comments_to_ag_2-25-20.pdf

INSIGHTS ASSOCIATION
1156 15TH ST, NW, SUITE 700, WASHINGTON, DC 20005 • [redacted]
WEBSITE: www.InsightsAssociation.org • EMAIL [redacted]

CCPA_2ND15DAY_00102

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, 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."

1. Clarify the significance of deleting § 999.302 for defining personal information.

In the February 10 edits, your office added § 999.302 to the regulations, which reiterated that CCPA's "personal information" definition "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.'" The section went on to clarify that IP addresses which could not reasonably be linked to a particular consumer or household would not be personal information. This section was deleted from the March 11 draft. W324-1

We respectfully submit that this addition and subsequent deletion create unnecessary confusion, and we request that you clarify your office's position. It is obviously critical for businesses to understand, as well as possible, the contours of CCPA's "personal information" definition. As you're no doubt aware, IP addresses in particular have been a much-discussed and somewhat controversial aspect of "personal information" definitions in other privacy laws. Following these most recent edits, your office's position on IP addresses is especially unclear.

2. Treat notice via telephone differently and at least allow for a short-form option.

The February 10 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," but as we explained previously, the notices required to be read over the phone might often include not just collection notices, but also opt-out notices and financial incentive notices. Such a lengthy "preamble" to a phone call would be disastrous to research conducted over the phone. W324-2

Response rates for U.S. telephone surveys are lucky to reach ten (10) percent and adding an extended notice to the front-end of all calls will crater already low response 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 input for a public opinion or political poll or in response to a government-sponsored survey, for example.

INSIGHTS ASSOCIATION
1156 15TH ST, NW, SUITE 700, WASHINGTON, DC 20005 • [redacted]
WEBSITE: www.InsightsAssociation.org • [redacted]

Therefore, we again urgently request that the CCPA 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.

W324-2 cont.

Such a short-form notice would, by shortening the amount of "legalese" confronting consumers, better serve the goals of the CCPA without unnecessarily inhibiting legitimate research.

3. Loosen restriction on passing through costs of verification to accommodate special circumstances.

W324-3

While the draft regulations prohibit businesses in § 999.233(d) from "requir[ing] the consumer *or the consumer's authorized agent* to pay a fee for the verification of their request to know or request to delete," the Insights Association's reservations remain.

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. Limitations need to be set in certain circumstances on the pass-through of verification costs, in order to avoid an undue burden on businesses. To review our previous comments on this issue,[4] please see attached.

4. Expand the email-only option for all requests, and apply to all relationships with consumers that are "exclusively online."

W324-4

The CCPA draft regulations 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." IA once again urges expanding this email-only option to all requests, not just requests to know, and generally expanded to all relationships between consumers and businesses that are exclusively online, even if the businesses in question operate separately in a non-online context. To review our previous comments on this issue,[5] please see attached.

5. Broaden financial incentive disclosure guidance to contemplate situations where additional, non-monetary consideration is given in exchange for personal information.

W324-5

The Insights Association also must reiterate that the financial incentive "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. A person choosing to participate in research is subject to a more complicated mix of motivations or "consideration" someone participating in a typical company loyalty program and the final CCPA regulations should reflect this reality. To review our previous comments on this issue,[6] please see attached.

---

[4] Point 5, IA comments on 2nd draft,: https://www.insightsassociation.org/sites/default/files/misc_files/insights_association_ccpa_comments_to_ag_2-25-20.pdf

[5] Point 2, IA comments on 2nd draft: https://www.insightsassociation.org/sites/default/files/misc_files/insights_association_ccpa_comments_to_ag_2-25-20.pdf

INSIGHTS ASSOCIATION
1156 15TH ST, NW, SUITE 700, WASHINGTON, DC 20005 • [redacted]
WEBSITE: www.InsightsAssociation.org • EMAIL: [redacted]

6. Clarify the meaning of "reasonably expect" and "just in time" in the mobile notice requirements.

W324-6

IA respectfully requests that your office further clarify the meaning of "reasonably expect" and "just in time" in § 999.305(a)(4). To review our previous comments on this issue,[7] please see attached.

7. Delay enforcement of CCPA regulations.

The Insights Association previously urged that enforcement be delayed a further six months, until January 1, 2021, given the absence of lag time between the release of final CCPA regulations and the onset of CCPA enforcement this summer. The need for delay has been heightened exponentially due to the ongoing coronavirus pandemic. This was also stressed by a March 20, 2020 letter IA sent with 65 other organizations requesting forbearance.[8]

W324-7

In many cases right now, businesses are struggling to implement CCPA compliance measures while working remotely. Furthermore, the costs of compliance must also now be balanced against the crushing macroeconomic impacts of the virus, including a looming recession. This delay would give businesses the bare minimum time to analyze the final regulations and respond accordingly and responsibly.

Conclusion

The Insights Association hopes the above comments will be useful to you and your staff as you finalize the CCPA regulations. 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 the concomitant clarity on CCPA compliance.

Sincerely,

Howard Fienberg
Vice President, Advocacy
Insights Association

Stuart L. Pardau
Outside General Counsel
The Insights Association
(and Ponemon Institute Fellow)

---

[6] Point 3, IA comments on 2nd draft:
https://www.insightsassociation.org/sites/default/files/misc_files/insights_association_ccpa_comments_to_ag_2-25-20.pdf

[7] Point 4, IA comments on 2nd draft:
https://www.insightsassociation.org/sites/default/files/misc_files/insights_association_ccpa_comments_to_ag_2-25-20.pdf

[8] Joint industry letter requesting forbearance:
https://www.insightsassociation.org/sites/default/files/misc_files/joint_industry_letter_requesting_a_delay_in_ccpa_enforcement_-_updated_3.20.2020.pdf

INSIGHTS ASSOCIATION
1156 15TH ST, NW, SUITE 700, WASHINGTON, DC 20005 [redacted]
WEBSITE: www.InsightsAssociation.org • EMAIL: [redacted]

ATTACHMENT #1

Insights Association comments on 1st CCPA regulations draft

12/6/19

INSIGHTS ASSOCIATION
1156 15TH ST, NW, SUITE 700, WASHINGTON, DC 20005 • [redacted]
WEBSITE: www.InsightsAssociation.org • EMAIL: [redacted]

The Honorable Xavier Becerra
Attorney General, State of California

Privacy Regulations Coordinator
California Office of the Attorney General

Email: privacyregulations@doj.ca.gov

December 6, 2019

Dear Attorney General Becerra

The Insights Association ("IA") submits the following comments regarding the proposed regulations[9] implementing the California Consumer Privacy Act ("CCPA") (CAL. CIV. CODE, § 1798.100 et seq.).

IA represents more than 530 individual and company members in California, with more than 5,300 members in total. Virtually all of these members will fall within the jurisdiction of the CCPA due to the fact that personal information of California residents is collected and transmitted for legitimate purpose by marketing research and data analytics companies and organizations in most instances.

IA is the leading nonprofit trade association for the marketing research and data analytics industry. IA's members are the world's leading producers of intelligence, analytics and insights defining the needs, attitudes and behaviors of consumers, organizations, employees, students and citizens. With that essential understanding, leaders can make intelligent decisions and deploy strategies and tactics to build trust, inspire innovation, realize the full potential of individuals and teams, and successfully create and promote products, services and ideas.

What is "marketing research"? Marketing research is the collection, use, maintenance, or transfer of personal information as reasonably necessary to investigate the market for or marketing of products, services, or ideas, where the information is not otherwise used, without affirmative express consent, to further contact any particular individual, or to advertise or market to any particular individual. An older definition of marketing research, used in California S.B. 756 in 2017, was "the collection and analysis of data regarding opinions, needs, awareness, knowledge, views, experiences and behaviors of a population, through the development and administration of surveys, interviews, focus groups, polls, observation, or other research methodologies, in which no sales, promotional or marketing efforts are involved and through which there is no attempt to influence a participant's attitudes or behavior."

W324-8

The CCPA will have a profound impact on the business community, including the marketing research and data analytics industry. According to the August 2019 estimate from Berkeley Economic Advising and Research for the Attorney General's office, compliance with CCPA regulations (not including compliance

[9] https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf

INSIGHTS ASSOCIATION
1156 15TH ST, NW, SUITE 700, WASHINGTON, DC 20005 [redacted]
WEBSITE: www.InsightsAssociation.org • EMAIL [redacted]

with the statute itself) would amount to $467 million to $16.454 billion per year.[10] In this regard, we appreciate the opportunity to submit IA's recommendations on the draft regulations.

Our primary concerns focus on: (1) limiting the "authorized agent" concept to minors, and elderly or incapacitated individuals; (2) exempting marketing research from notices of financial incentives for research participation or, alternatively, providing for an opt-in regime in place of the notices; (3) allowing for email requests in lieu of an interactive webform; (4) clarifying how § 999.315 relates to existing "Do Not Track" requirements, and delaying implementation of this requirement; (5) setting the response times for requests to know or delete and opt-out requests at a uniform 45 days; and (6) issuing further guidance on how CCPA applies to personal information collection via telephone.

1. Limit the "authorized agent" concept to minors, and elderly or incapacitated individuals.

W324-8 cont.

Under the draft regulations, a consumer may designate an authorized agent[11] to submit opt-out requests, and requests to know and delete. Per § 999.326, when a consumer makes a request through an authorized agent, "the business may require that the consumer: (1) Provide the authorized agent written permission to do so; and (2) Verify their own identity directly with the business."

As currently drafted, there would be no tangible limitation on this procedure; anyone could submit a request through an authorized agent.
This option will be unnecessary in most cases, increase paperwork associated with the verification process, and open the door for fraudulent requests. Except in cases where the consumer is a minor, or someone who genuinely needs an authorized agent to submit a request (such as an elderly or incapacitated individual), requiring requests to be submitted by consumers themselves would better serve CCPA's purpose.

2. Exempt marketing research from notices of financial incentives for research participation or, alternatively, provide for an opt-in regime in place of the notices.

Under § 999.307, businesses would need to give notice of financial incentives for the purpose of explaining to the consumer "each financial incentive or price or service difference a business may offer in exchange for the retention or sale of a consumer's personal information so that the consumer may make an informed decision on whether to participate."[12] The notice would have to include a "good faith

---

[10] "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations." August 2019.
http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf

[11] As defined by § 999.301, an "authorized agent" is "a natural person or a business entity registered with the Secretary of State that a consumer has authorized to act on their behalf subject to the requirements set forth in section 999.326."

[12] § 999.307. "Notice of Financial Incentive (a) Purpose and General Principles (1) The purpose of the notice of financial incentive is to explain to the consumer each financial incentive or price or service difference a business may offer in exchange for the retention or sale of a consumer's personal information so that the consumer may make an informed decision on whether to participate. (2) The notice of financial incentive shall be designed and presented to the consumer in a way that is easy to read and understandable to an average consumer. The notice shall: a. Use plain, straightforward language and avoid technical or legal jargon. b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable. c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers. d. Be accessible to consumers with disabilities. At a minimum, provide information

INSIGHTS ASSOCIATION
1156 15TH ST, NW, SUITE 700, WASHINGTON, DC 20005 • [redacted]
WEBSITE: www.InsightsAssociation.org • [redacted]

estimate of the value of the consumer's data that forms the basis for offering the financial incentive." Section 999.337 spells out eight different methods for calculating that value.[13]

The regulations requiring notice of financial incentives seem primarily designed to deal with situations where companies offer some discount or free service in return for the sharing or sale of the consumer's personal information. Such situations often involve passive data collection under terms that are not entirely transparent.

Financial incentives in marketing research are different.

W324-8 cont.

Marketing research requires robust participation and representation to be effective. IA members frequently achieve this by offering financial incentives to research participants (also known as respondents). For example, a doctor may be offered an honorarium to complete a survey about various pharmaceuticals, or an individual may be offered a gift card to participate in a half-day focus group about important public policy issues in their community.

In these and other similar cases, research respondents often participate for a variety of non-monetary reasons, including a desire to share opinions that will help improve product/service quality or simply on subject matter that a respondent may be passionate about. People care about the issues our members ask about, and like giving their opinions. Nevertheless, because of the costs sometimes associated with fielding a research study, insights professionals cannot afford to take participation for granted. Financial incentives of various kinds help complete research as quickly and effectively as possible.
Many exchanges between businesses and consumers involving personal information (such as those between researcher and respondent) are complicated interactions motivated by a variety of reasons. Often, there is no simple *quid pro quo* involving money for information.

---

on how a consumer with a disability may access the notice in an alternative format. e. Be available online or other physical location where consumers will see it before opting into the financial incentive or price or service difference. (3) If the business offers the financial incentive or price of service difference online, the notice may be given by providing a link to the section of a business's privacy policy that contains the information required in subsection (b). (b) A business shall include the following in its notice of financial incentive: (1) A succinct summary of the financial incentive or price or service difference offered; (2) A description of the material terms of the financial incentive or price of service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference; (3) How the consumer can opt-in to the financial incentive or price or service difference; (4) Notification of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and (5) An explanation of why the financial incentive or price or service difference is permitted under the CCPA, including: a. A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and b. A description of the method the business used to calculate the value of the consumer's data."

[13] § 999.337 "(b) To estimate the value of the consumer's data, a business offering a financial incentive or price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data. The business shall use one or more of the following: (1) The marginal value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data; (2) The average value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data; (3) Revenue or profit generated by the business from separate tiers, categories, or classes of consumers or typical consumers whose data provides differing value; (4) Revenue generated by the business from sale, collection, or retention of consumers' personal information; (5) Expenses related to the sale, collection, or retention of consumers' personal information; (6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference; (7) Profit generated by the business from sale, collection, or retention of consumers' personal information; and (8) Any other practical and reliable method of calculation used in good-faith."

INSIGHTS ASSOCIATION
1156 15TH ST, NW, SUITE 700, WASHINGTON, DC 20005 • [redacted]
WEBSITE: www.InsightsAssociation.org • EMAIL: [redacted]

These exchanges are also, at least in the research context, generally entered into freely by both parties. If consumers knowingly consent to a financial incentive like those described in the marketing research scenarios described above, the CCPA's drafters likely did not intend to interfere in such a relationship.

The regulations do not appear to have been written with marketing research in mind and would inhibit research in an unintended way. Accordingly, the regulations should exempt marketing research participation from notices of financial incentives.

In the alternative, if such an exemption is not feasible, the regulations should provide an opt-in regime whereby the amount of the financial incentive (if any) will be disclosed prior to the commencement of the marketing research, and the respondent (or individual whose information is being used for marketing research purposes) will have the sole option to determine whether their personal information will be used for research or not.

3. Allow for email requests in lieu of an interactive webform.

Under Sections 999.312 and 999.315 of the draft CCPA regulations, businesses must provide two or more designated methods for submitting requests to know and opt-out, including, at a minimum, a toll-free telephone number and, if the business operates a website, an "interactive webform" accessible through the business's website.

Many California businesses, including many of our members, have limited resources, both in terms of personnel and technological expertise. Requiring these businesses to launch an interactive webform imposes new burdens without furthering CCPA's purposes. As such, email correspondence would better serve CCPA's purposes by allowing consumers to state their questions and concerns directly, and to start a conversation regarding their privacy on their own terms. W324-8 cont.

4. Clarify how § 999.315 relates to existing "Do Not Track" requirements, and delay implementation of this requirement.

Under § 999.315, "[i]f a business collects personal information from consumers online, the business shall treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid [opt-out] request."

IA seeks clarification on how this regulation relates to existing requirements related to "Do Not Track" signals. Under current California law, businesses are required to disclose in their privacy policies how they respond to such signals, but are not required to honor them. Would the regulations require that businesses honor "Do Not Track" signals, or would the regulations only apply to "a browser plugin or privacy setting" which more specifically communicates a consumer's desire that a business not *sell* their personal information?

A "Do Not Track" signal is not the same as a "do not sell" request. For example, a consumer may set her browser to "Do Not Track" because she does not want businesses tracking her browsing activities (and perhaps serving her with targeted ads), but it does *not* necessarily follow that the consumer would want to opt out of the sale of her information in every scenario.

Irrespective of this desired clarification, IA requests that the Attorney General's office delays implementation of any regulation related to a "browser plugin or privacy setting or other mechanism" for

INSIGHTS ASSOCIATION
1156 15TH ST, NW, SUITE 700, WASHINGTON, DC 20005 • [redacted]
WEBSITE: www.InsightsAssociation.org • EMAIL: [redacted]

an additional year. As discussed above, many of our members are smaller companies with limited technological capabilities. This concern is obviously not just limited to the marketing research and data analytics industry. We believe such smaller businesses will need additional time to work out the complicated implementation and response procedures related to this question.

5. Set the response times for requests to know or delete and opt-out requests at a uniform 45 days.

Under §999.313 of the draft CCPA regulations, businesses must confirm receipt of requests to know or delete information within 10 days, and respond substantively to the requests within 45 days. Under § 999.315, businesses must "act upon [an opt-out] request as soon as feasibly possible, but no later than 15 days from the date the business receives the request."

These deadlines are unnecessarily complicated. The timeframe to respond to all requests should be set at a uniform 45 days.

However, the extension to 90 days under § 999.313 ("provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request") and the requirement under § 999.315 that third parties be notified of opt-out requests within 90 days should both remain unchanged. W324-8 cont.

6. Issue further guidance on how CCPA applies to personal information collection via telephone.

Finally, the CCPA applies to the collection of all personal information, by whatever means, but does not give any guidance on unique compliance issues with different modes of collection.

In particular, the current draft regulations do not efficiently address information collection via telephone. For example, in a marketing research phone call where a financial incentive is involved, the caller would have to verbally read out the contents of three different notices: the notice at collection, notice of the opt-out right, and the notice of financial incentive. Such a three-part notice, delivered at the outset of the call, would be unduly cumbersome and likely result in significantly fewer respondents ever completing a research interaction via telephone (current response rates for U.S. telephone surveys rarely break 10 percent already). Such an outcome would not further the purposes of the CCPA.

As an alternative, the finalized regulations could require instead that, where information is collected via telephone, listeners may be directed to a URL where the required notices are posted, or callers may read out a short-form version of the notices.

Conclusion

The Insights Association hopes that the above comments will be useful to you and your staff.

We look forward to answering any questions you or your staff may have about the marketing research and data analytics industry, and working with you and your office in furtherance of consumer privacy in California.

Sincerely,

Howard Fienberg
Vice President, Advocacy
Insights Association

Stuart L. Pardau
Outside General Counsel
Insights Association (and Ponemon Institute Fellow)

INSIGHTS ASSOCIATION
1156 15TH ST, NW, SUITE 700, WASHINGTON, DC 20005 • PH: [redacted]
WEBSITE: www.InsightsAssociation.org • EMAIL: [redacted]

ATTACHMENT #2

Insights Association comments on 2nd CCPA regulations draft

2/25/20

INSIGHTS ASSOCIATION
1156 15TH ST, NW, SUITE 700, WASHINGTON, DC 20005 • [redacted]
WEBSITE: www.InsightsAssociation.org • EMAIL: [redacted]

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.[14]

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.

W324-9

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,

[14] 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 • [redacted]
WEBSITE: www.InsightsAssociation.org • [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,[15] 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.

W324-9 cont.

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:

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.

---

[15] 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 • [redacted]
WEBSITE: www.InsightsAssociation.org • [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.

3. Broaden financial incentive disclosure guidance to contemplate situations where additional, non-monetary consideration is given in exchange for personal information.

W324-9 cont.

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.

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."

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 • EMAIL: [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.

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.

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.

W324-9 cont.

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.

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 • [redacted]
WEBSITE: www.InsightsAssociation.org • [redacted]

Message

From: Tonsager, Lindsey [redacted]
Sent: 3/27/2020 2:59:38 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CCPA Rulemaking - Written Comments of the Entertainment Software Association
Attachments: CCPA Comments - Entertainment Software Association 3.27.2020 Signed.pdf

Dear Privacy Regulations Coordinator:

Please find attached the comments of the Entertainment Software Association regarding the second set of 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

This message is from a law firm and may contain information that is confidential or legally privileged. If you are not the intended recipient, please immediately advise the sender by reply e-mail that this message has been inadvertently transmitted to you and delete this e-mail from your system. Thank you for your cooperation.

March 27, 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 Second Set of Modified CCPA Regulations

To Whom It May Concern:

The Entertainment Software Association ("ESA")[1] submits this letter in response to the Attorney General's notice of the second set of modifications to the proposed regulations implementing the California Consumer Privacy Act ("CCPA").[2] ESA and its members appreciate the Attorney General's continued efforts to provide businesses and consumers more clarity in order to facilitate compliance. We write to confirm our understanding that the Attorney General did not intend for the most recent changes to the draft regulations to alter the plain meaning of the statutory text, which does not treat data as regulated "personal information" if the business does not link the data to any particular consumer or household, and maintains the data so that the business cannot reasonably link the data with a particular consumer or household.

W325-1

Specifically, the second proposed modifications strike Section 999.302 of the proposed regulations, which restated the statutory definition of "personal information" and explained that, 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.'" Because the statutory text and legislative history is clear on this point, we understand that Section 999.302 was removed because it was redundant with the statute, and not because the Attorney General intended any substantive change in meaning.

[1] ESA is the U.S. association for companies that publish computer and video games for video game consoles, handheld devices, personal computers, and the internet. There are over 900 video game companies in the State of California.

[2] California Department of Justice, Notice of Second Set of Modifications to Text of Proposed Regulations (Mar. 11, 2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-mod-020720.pdf?.

Entertainment Software Association • 601 Massachusetts Ave. NW • Suite 300 • Washington, DC 20001 • Phone: (202) 223-2400
CCPA_2ND15DAY_00118

As you know, the California legislature amended the statutory text in September 2018 to reiterate that any category of information enumerated in the statute constitutes "personal information" only if "it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household."[3] This definition was further amended in October 2019 to emphasize that a reasonableness standard applies when determining whether information is "personal information" or non-personal, de-identified information for purposes of the CCPA; if the business is not *reasonably* capable of associating or linking the data to a particular consumer or household, it is not personal information.[4] In addition, the statute specifies that nothing in the CCPA requires that a business "reidentify *or otherwise link* information that is not maintained" in a manner that identifies or is reasonably capable of identifying a particular consumer or household.[5]

W325-1 cont.

Consequently, the plain meaning of the statutory text and legislative history is that information, such as an IP address, is not "personal information" if the business does not link the data to any particular consumer or household, and maintains the data so that the business cannot reasonably link the data with a particular consumer or household. Any interpretation that would treat the deletion of Section 999.302 from the draft regulations as broadening the "personal information" definition to ignore the limits on its scope would be in direct contradiction of the statutory text and legislative intent, and therefore would be invalid.[6]

For these reasons, ESA and its members respectfully request that the Attorney General either reinstate Section 999.302 in the final regulations or explain in the Final Statement of Reasons that this section was removed because it was unnecessary.

Sincerely,



Gina Vetere
Senior Vice President and General Counsel
Entertainment Software Association

---

[3] SB 1121 (adding the following italicized language: "'Personal information' means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following *if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:* [enumerated examples, including IP address]").

[4] AB 874 (adding the following italicized language: "'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: [enumerated examples, including IP address]").

[5] Cal. Civ. Code § 1798.145(l) (emphasis added).

[6] *See, e.g., Ontario Community Foundations, Inc. v. State Bd. of Equalization*, 201 Cal.Rptr. 165, 168 (1984).

Message

From: Dale Smith [redacted]
Sent: 3/27/2020 8:54:32 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Dale R. Smith Jr. [redacted]
Subject: CCPA Written Comment on Proposed Regulations Due March 27 (Transmitting)
Attachments: CCPA_Comments_20200327.pdf

Dear Privacy Regulations Coordinator:

Attached to this email is our .pdf document containing PrivacyCheq's submission of comment for the NOTICE OF SECOND SET OF MODIFICATIONS TO TEXT OF PROPOSED REGULATIONS published March 11, 2020 (Comment period closing on March 27)

Thank you for the opportunity to comment.

Dale Smith

DALE R. SMITH, CIPT
Futurist [redacted]
PrivacyCheq

Attachments area

PrivacyCheq

March 27, 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 NOTICE OF SECOND SET OF MODIFICATIONS TO TEXT OF PROPOSED REGULATIONS Released March 11, 2020

Dear Mr. Becerra:

We are writing concerning the removal of guidance[1] regarding the Opt-Out Logo or Button as originally called for in AB-375, now in force[2].

While the logo/button concept as a means for consumers to signal the DO NOT SELL MY PERSONAL INFORMATION (DNSMPI) preference has proved elusive to prescribe, we believe that **the concept of using a recognizable and uniform "trigger" graphic offering key just-in-time information to consumers is a sound concept and should not be abandoned**.

W326-1

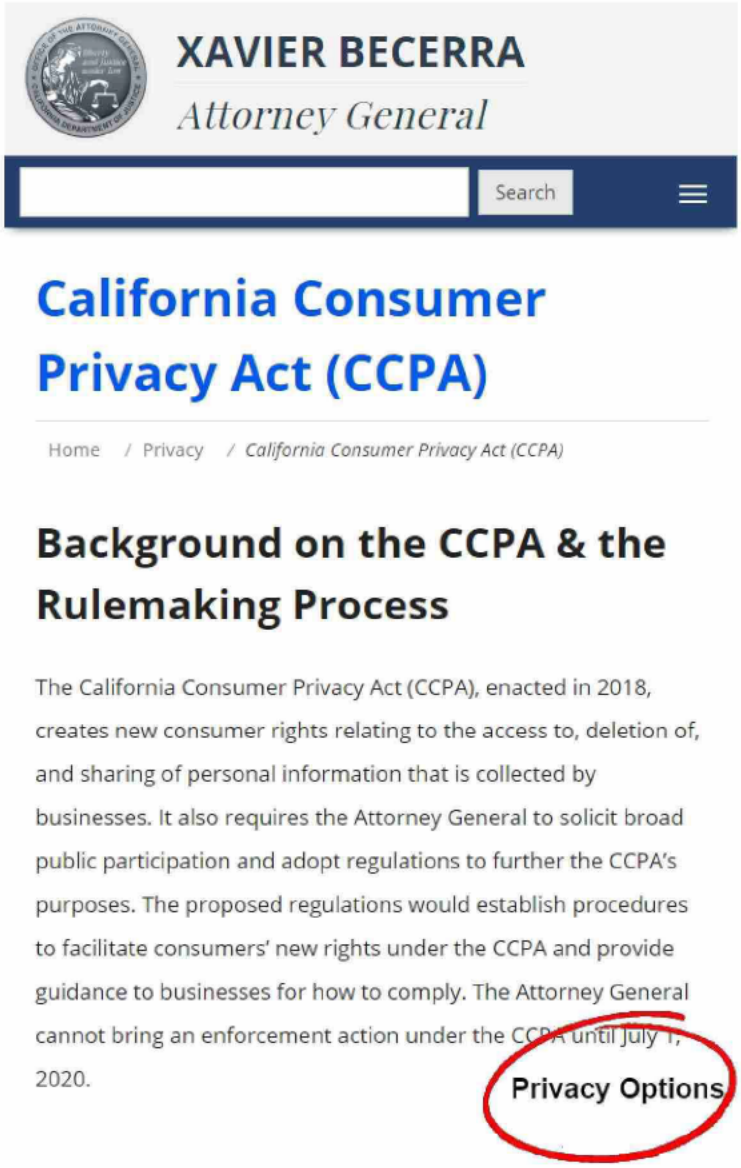
Instead of using a single-purpose Button/Logo graphic to just trigger the DO NOT SELL preference, we suggest that the regulation recognize the utility of a standardized graphic trigger (Figures 1 and 2) offering consumers a pop-up menu of interactive "just-in-time" information and choices.

For the trigger graphic, we suggest adapting the public domain "Nutrition Facts" format which is widely used, understood, and trusted by consumers around the world. By substituting the words "Privacy Options" for the words "Nutrition

[1] §999.306(f) Opt-Out Button or Logo specification has been deleted in its entirety
[2] §1798.185(a)(4)(C) The development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt out of the sale of personal information.

Facts", and by making the framework interactive, the consumer can be presented with a familiar, trusted display of privacy options. Below are some examples demonstrating how such a trigger graphic might function in practice:

Figure 1 illustrates how a trigger graphic would appear on a sample website as viewed on a large screen (laptop, tablet, etc.). The proposed **Privacy Options** trigger is highlighted.



W326-1 cont.

PrivacyCheq

Figure 2 illustrates how the same trigger graphic would appear on the screen of a mobile device.

The proposed **Privacy Options** trigger is highlighted.



W326-1 cont.

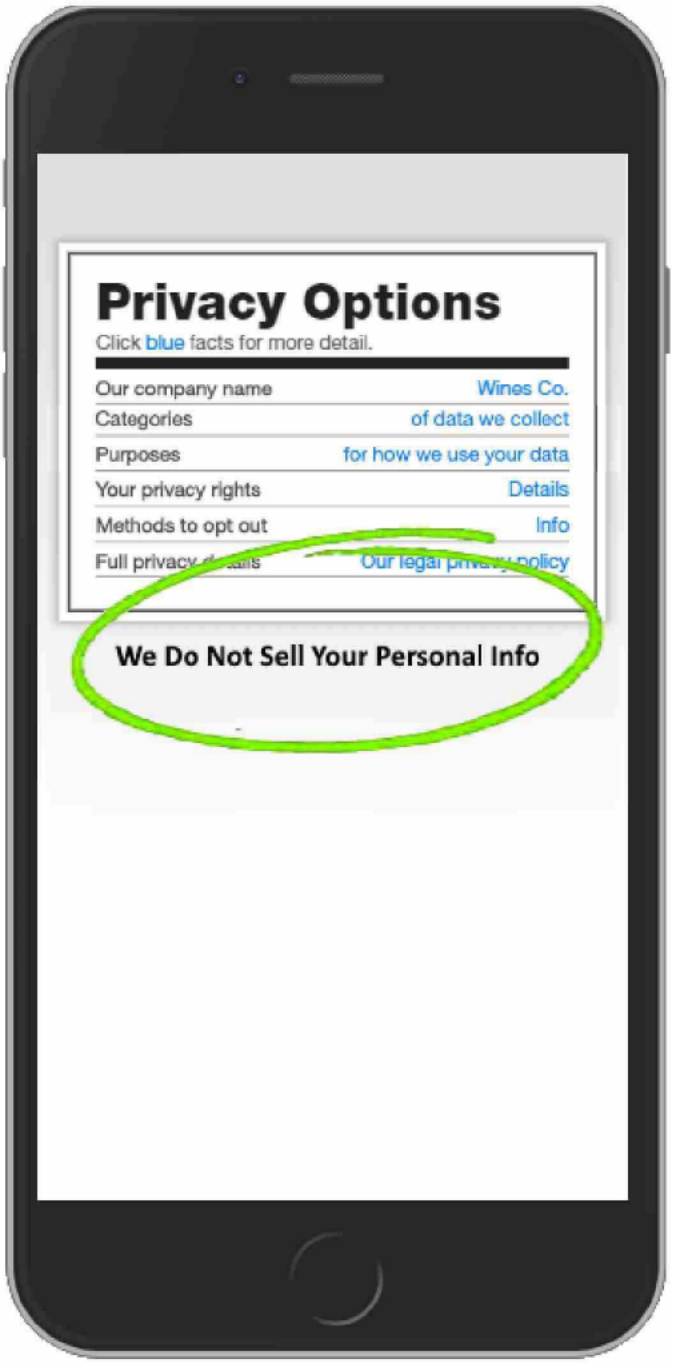
PrivacyCheq

With a Privacy Options trigger graphic in place, a consumer clicking on that trigger can be immediately presented with an interactive[3] "just-in-time" menu of the business's information and options. An important distinction here is that the **consumer is presented with <u>all</u> relevant options, not just a single, binary opt-out option presented by a logo or button choice.**

Figure 3 illustrates a sample "just-in-time" Notice at Collection on a mobile screen for a business that **does <u>not</u> sell** consumer's PI.

Hotlinks to appropriate category, purpose, rights, etc. info are clearly displayed, but DNSMPI (Opt-Out) is not displayed as it is not a relevant choice. Confusion is eliminated and consumers' trust is enhanced.

To further enhance clarity for the consumer, a business may choose to declare outright that they do not sell consumer's PI (highlighted).



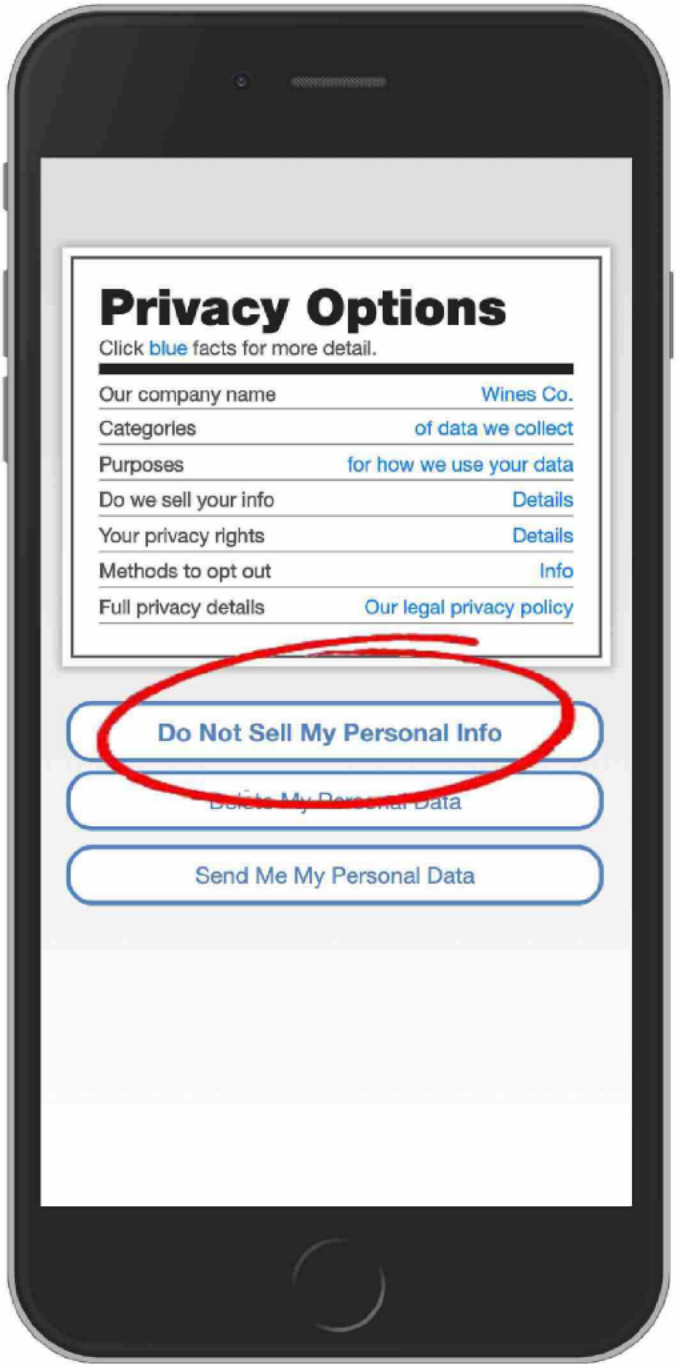
W326-1 cont.

[3] A live demonstration of interactivity can be seen by texting the word "ccpa" to 717-467-3214.

PrivacyCheq

Figure 4 illustrates "just-in-time" choices on a mobile screen for a business that **<u>does</u> sell consumer's PI**. The DNSMPI Opt-Out choice (highlighted) is now prominently presented, but still in context with basic category, purpose, rights, and other transparency information.

This is a great benefit to the consumer in that s(he) has single click access to the business's salient privacy facts <u>before</u> making what is now an informed Opt-Out decision, rather than blindly clicking a binary yes/no button.

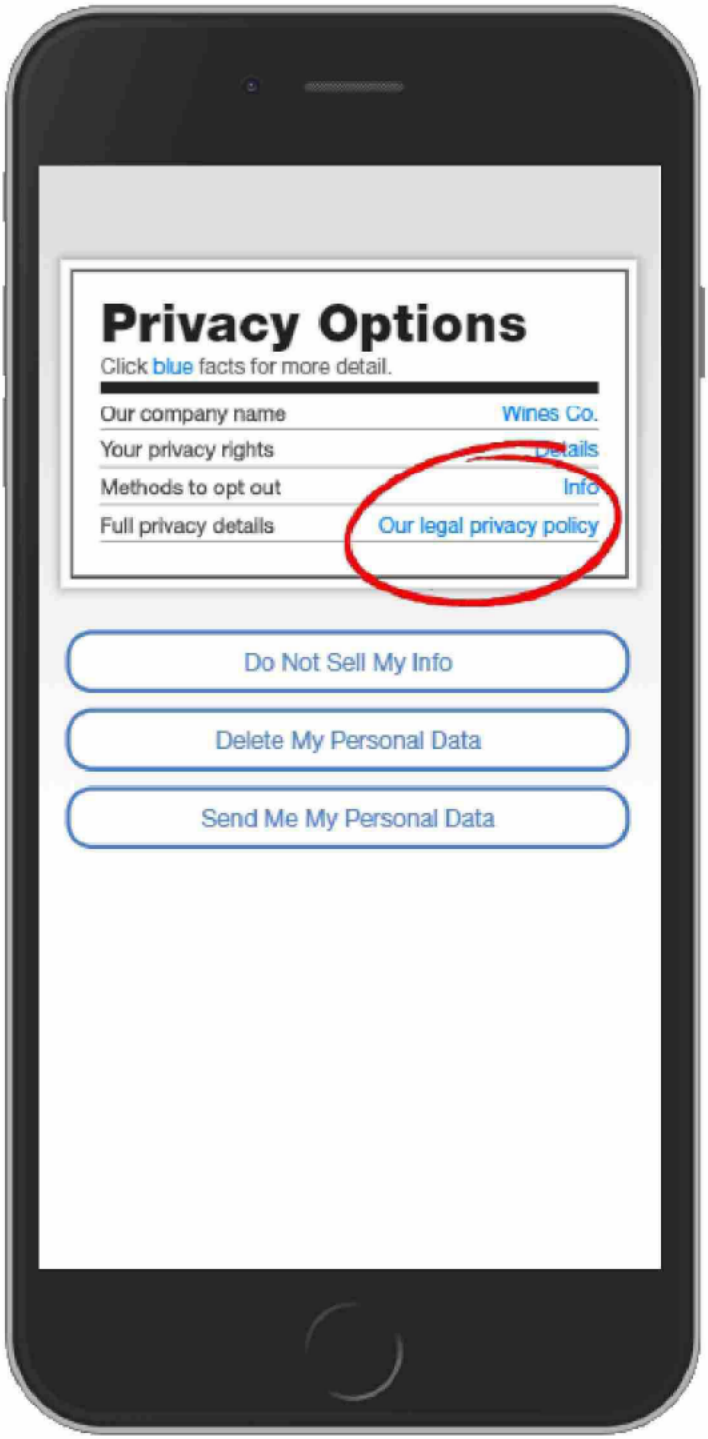


W326-1 cont.

PrivacyCheq

Figure 5 illustrates how the consumer can use the "just-in-time" interactive notice to access the business's full privacy policy if/when full detailed information is desired.

Clicking on the highlighted element will link immediately to the business's full legal privacy policy.



W326-1 cont.

PrivacyCheq

Concluding, we suggest that operationalizing DNSMPI choice to consumers can best be accomplished by making the Do Not Sell choice a feature of a larger **standardized framework offering all relevant choices to the consumer, not just the DNSMPI choice**. We suggest that the ubiquitous Nutrition Label framework be named within the regulations as an example of a readily adaptable standard and functional implementation of what is called for in §1798.185(a)(4)(C)[4].

Thinking more generally, as CCPA is implemented, California has the opportunity to inspire a de facto standard for "just-in-time" notice design that could be embraced as best practice within the privacy community at large. As other jurisdictions implement similar regulations across the United States, California's leadership in defining this standard could foster important harmonization of state and federal laws going forward.

W326-1 cont.

Additional information on practical CCPA just-in-time notice implementation can be found in PrivacyCheq's previous comment submissions to the CCPA Proposed Regulation which closed on December 6, 2019 and February 24, 2020 respectively:

W326-2

http://model.consentcheq.com/20191205-ccpa1010-comment.pdf
http://model.consentcheq.com/20200225-ccpa-comment-update.pdf

Thank you for these opportunities to comment.

Sincerely,



Dale R. Smith, CIPT
Futurist
[redacted]

[4] §1798.185(a)(4)(C) The development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt out of the sale of personal information.



via email to: PrivacyRegulations@doj.ca.gov

Message

From: Elizabeth Bojorquez [redacted]
Sent: 3/27/2020 3:04:49 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Jacqueline Kinney [redacted]
Subject: CCTA Comments on CCPA Second Modified Regulations 3.27.20
Attachments: CCTA Comments to AG on 2nd Modified Regs FINAL 3.27.20.pdf

Good Afternoon,

The California Cable and Telecommunications Association submits the attached comments regarding the Second Set of Modifications to Proposed 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)
[redacted]

Carolyn McIntyre
President

1001 K STREET, 2ND FLOOR
SACRAMENTO, CA 95814

916/446-7732
FAX 916/446-1605

March 27, 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 – Second Set of Modifications

The California Cable and Telecommunications Association ("CCTA") hereby responds to the "Notice of Second Set of Modifications to Text of Proposed Regulations" issued March 11, 2020 ("Second Revised Regulations"), by the Attorney General ("AG") as part of its rulemaking to implement the California Consumer Privacy Act ("CCPA").

CCTA submitted comments on December 6, 2019, on the AG's originally proposed CCPA regulations and appreciates that the AG's First Revised Regulations issued on February 10, 2020, included changes to address some of the issues raised in CCTA's comments. CCTA submitted additional comments on February 25, 2020, asking for a small number of narrow and targeted additional revisions to the First Revised Regulations. CCTA is disappointed that the AG's Second Revised Regulations do not meaningfully address the discreet changes that CCTA requested to improve the CCPA regulations. W327-1

CCTA respectfully requests that our requested changes be included when the AG issues final CCPA regulations. Attached are CCTA's comments submitted on February 25, 2020, with a corresponding redline of those changes against the Second Revised Regulations. Adopting these recommended revisions will improve the final regulations' consistency with the statute, further the legislative purpose, and achieve greater clarity that will enhance compliance with the CCPA and meet requirements of the Administrative Procedure Act.

Respectfully submitted,

/s/Jacqueline R. Kinney

Jacqueline R. Kinney
CCTA Senior Vice President and General Counsel

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").

W327-2

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.

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.

W327-2 cont.

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."

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.

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. Service Providers – Section 999.314(c)(3) and (d)

4-A -- 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."

W327-2 cont.

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) ***The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose***." (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.

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.

W327-2 cont.

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.

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."

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.

W327-2 cont.

Respectfully submitted,

/s/Jacqueline R. Kinney

Jacqueline R. Kinney
CCTA Senior Vice President and General Counsel

CCTA RECOMMENDATIONS
MARCH 27, 2020

TEXT OF MODIFIED REGULATIONS

The original proposed language is in single underline. First set of modifications (noticed on February 10, 2020) are illustrated in red double underline for proposed additions and by ~~strikeout~~ for proposed deletions. Second set of modifications (noticed on March 11, 2020) are illustrated by green double zigzag underline for proposed additions and by blue ~~double 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~~.

CCTA Recommendation #1 W327-2 cont.

(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 and their dependents 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, related to ~~as compensation, for~~ the collection, retention ~~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 collection, retention, ~~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 collection, retention, ~~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 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.

(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 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~~ny~~ 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, subsection (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) A business that does not collect personal information directly from a consumer does not need to provide a notice at collection to the consumer if it does not sell the consumer's personal information.

(e) ~~(d) If a~~ A business that does not collect information directly from consumers ~~is~~ A data broker 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.~~

(f) ~~(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 is not required to provide a link to the business's privacy policy~~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~~.

(g) ~~(f)~~ Subsection (ef) 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.

CCTA Recommendation #2

W327-2 cont.

(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 Ssection 999.315, subsection (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.~~

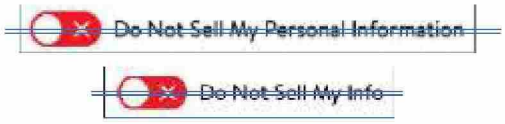
(e) A business shall not sell the personal information it collected during the time the business did not have a notice of right to opt-out notice posted unless it obtains the affirmative authorization of the consumer.

(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 collection, retention 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 or ~~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~~ policy 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.

(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. Identify the categories of sources from which the personal information is collected. The categories shall be described in a manner that provides consumers a meaningful understanding of the information being collected.

f. Identify the business or commercial purpose for collecting or selling personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected or sold.

g. ~~(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, subsection (g), the information compiled in section 999.317, subsection (g)(1), or a link to it.

(9) If the business has actual knowledge that it sells the personal information of minors under 16 years of age, a description of the processes required by sections 999.330 and 999.331.

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, ~~clearly~~ 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. The business shall, however, inform the consumer with sufficient particularity that it has collected the type of information. For example, a business shall respond that it collects "unique biometric data including a fingerprint scan" without disclosing the actual fingerprint scan data.

CCTA Recommendation #3 — W327-2 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 doings so by law. If the request is denied only in part, the business shall disclose the other information sought by the consumer.

(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 required by section 999.317, subsection (b) ~~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) If a business that denies a consumer's request to delete 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.

(8) ~~(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, or about 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 process or maintain personal information on behalf of the business that provided the personal information, or that directed the service provider to collect the personal information, and in compliance with the written contract for services required by the CCPA ~~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 to use in providing services to another business, ~~or cleaning correcting or augmenting data acquired from another source~~;

CCTA Recommendation #4-A — W327-2 cont.

(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~~ subdivision (a)(1) through ~~(a)~~(4).

(d) A service provider shall not sell ~~data~~ personal information of a consumer on behalf of a business when ~~a~~ such consumer has opted-out of the sale of their personal information with the business~~.~~, except as necessary to perform the business purpose for which the business contracted with such service provider. ~~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.~~

CCTA Recommendation #4-B — W327-2 cont.

(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.

(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 has the substantial effect of subverting or impairing a consumer's decision to opt-out.

(d) ~~(c)~~ 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 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 sales ~~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

(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.

CCTA Recommendation #5-A

W327-2 cont.

(b) ~~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.

CCTA Recommendation #5-B
(this recommendation was addressed in Second Revised Regulations and is withdrawn)

W327-2 cont.

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 except as necessary to comply with a legal obligation.

(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 knows or reasonably should know that it, 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~~ 10,000,000 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 household personal information, ~~subject to verification requirements set forth in Article 4. (b) If~~ 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, ~~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 or the consumer's authorized agent 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~~ subsection (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~~ subsections (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~~ that 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 a state or 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 of the data of all natural persons in the United States 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.

Message

From: Kyla Christoffersen Powell [redacted]
Sent: 3/27/2020 3:39:16 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CJAC Comments on CCPA Regulations as Revised March 11, 2020
Attachments: CJAC Comments CCPA Revised Regulations 3-27-20.pdf

Dear Privacy Regulations Coordinator:

Attached are CJAC's comments on the CCPA Regulations, version March 11, 2020.

Best regards,

Kyla Christoffersen Powell
President and Chief Executive Officer
[redacted] | www.cjac.org
CIVIL JUSTICE
ASSOCIATION OF CALIFORNIA

CIVIL JUSTICE
ASSOCIATION OF CALIFORNIA

March 27, 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 March 11, 2020*

Dear Attorney General Becerra:

The Civil Justice Association of California ("CJAC") appreciates the opportunity to provide comments on this latest version of the proposed regulations implementing CCPA.

CJAC strongly urges the Office of the Attorney General to address two pressing issues that remain completely overlooked in the regulations, namely the need for delayed enforcement of the CCPA and the need to mitigate the private right of action.

We also ask the Attorney General to respond to concerns about previously proposed provisions that remain in the latest version, as well as some of the new changes.

These issues and concerns are detailed below:

1. The regulations should delay enforcement until at least January 1, 2021

CJAC recently signed onto a coalition letter addressed to your Office requesting delay of the enforcement date to January 1, 2021. The business community has repeatedly requested additional implementation time because of the complexity and substantial compliance burden associated with CCPA.

As spelled out in the letter, recent developments surrounding the coronavirus, however, greatly compound the need for additional time. Remote and scattered workforces make development of the complicated systems needed to implement CCPA nearly impossible. The need for delayed enforcement, while important before, is now critical. The fact that implementation of other systems such as tax filing have been delayed underscores the legitimacy of this request.

W328-1

An even longer implementation time window with an additional year to January 1, 2022 is eminently reasonable and more in line with what was provided for GDPR implementation, which was two years. CJAC previously asked the Attorney General to delay enforcement

until 2022 and again asks for consideration of a longer implementation window.

Alternatively, delayed implementation until at least January 1, 2021 is an extremely modest ask, given the current coronavirus crisis. The regulations should also clarify that any enforcement is prospective only.

W328-1 cont.

2. The regulations should mitigate the potential for unwarranted private rights of action.

CJAC additionally implores the Attorney General to revise the regulations to respond to major concerns expressed by the business community over the potential for unwarranted and unnecessary litigation under the CCPA's private right of action provisions.

There are several ways the Attorney General can mitigate this potential problem while promoting privacy safeguards, including:

W328-2

- 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.

- Second, 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 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. On the other hand, adoption of clear standards will promote ubiquitous adoption of best security practices.

3. The requirement to treat global privacy controls as opt-out requests should be eliminated due to technological and consumer choice limitations. (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 technologically feasible and limits consumer choice.

W328-3

From a technology standpoint, a major problem is that browser and global device settings are not designed to consistently convey affirmative user choice, versus the pre-selected choice of a third party such as the browser company, operating system provider, or internet service provider. Moreover, not every browser clearly communicates whether a user is a California resident.

Treating global settings as opt-outs will therefore limit consumer choice and access to online content. For example, consumers will likely be asked to pay for what would otherwise by free, ad-supported content or be blocked from access. Moreover, treating settings that may have been pre-selected by third parties, rather than the user, will empower large technology platforms to dictate content access rather than the consumer.

W328-4

In this vein, CJAC requests the that "shall" be changed to "may" under 999.315(d) and the last sentence of (d)(1) be reinstated:

> (d) 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 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 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.

W328-3 cont.

W328-4 cont.

Without these changes, the result will ultimately be less free and beneficial content online for consumers. Already-struggling content providers such as independent publishers and news outlets will see less traffic and fewer opportunities to generate revenue through advertising.

W328-3 cont.

4. New restrictions on service providers should be removed, as they are inconsistent with the CCPA. (Section 999.314(c).)

The new restrictions placed on service providers in section 999.314(c) concerning the use, disclosure, and retention of personal information go beyond the statute. Civil Code section 1798.140(v) permits service providers to use personal information pursuant to ***any*** contract for a business purpose, not just contracts for services required by CCPA. Furthermore, it allows processing of information by the service provider so long as it is for the specific purpose spelled out in the contract or otherwise permitted by statute:

> (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***

W328-5

> ***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 (emphasis provided).

W328-5 cont.

We therefore ask that section 999.314(c) be struck in its entirety, since it exceeds the scope of the statute. Alternatively, the section should be restored to the February 10 version.

5. **The requirement to quantify financial incentives and the value of consumer data should be eliminated because it provides no benefit and could be misleading. (Sections 999.307(b), 999.336, and 999.337.)**

We again ask the Attorney General to eliminate the requirement that businesses make and disclose calculations about financial incentives and data value.

W328-6

Requiring businesses to assign a number to incentives and data value provides little or no consumer benefit and can be misleading. 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. Additionally, a single customer's business or data holds little independent "value," since data gains value when it is aggregated.

The Attorney General should remove this quantification requirement from the regulations altogether, or alternatively, the Attorney General could simply require businesses to disclose whether they have a financial incentive or whether the data has value.

6. **The requirement that businesses reimburse consumers for costs associated with verification is unworkable and should be removed. (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 continue to object to businesses having to provide reimbursement for steps individuals may need to take to verify their identity. Requiring businesses to provide reimbursement for the multitude of ways in which consumers may verify their identity fails to consider the potential volume of these requests and resulting operational burdens on businesses.

W328-7

7. **The regulations should restore and expand guidance on information exempted from disclosure and deletion requests for security and other reasons. (Sections 999.302, 999. 313(c)(3), 999. 313(d)(3).)**

In our last set of comments, CJAC expressed our appreciation for the new guidance provided in now-deleted section 999.302 interpreting the term "personal information." We are disappointed to see the latest proposed revisions eliminate this guidance and ask that it be restored.

W328-8

Additionally, we had asked previously that the deleted portion of section 999.313(c)(3) be restored, but it was not. The deleted portion allowed a business to forgo disclosure that "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 is a critical basis for not disclosing information and should be

W328-9

restored. Finally, we re-ask that clarifications a.-d. that were added in the February 10 revisions to section 999.313(c)(3) be added to deletion requests in section 999.313(d)(3). W328-10

Conclusion

CCPA regulations that are unworkable or unduly burdensome will give rise to unnecessary and unproductive enforcement actions and litigation. We again stress that the goal of the regulations should be to facilitate implementation of and compliance with the CCPA. This will benefit consumers, while reducing unnecessary litigation burdens on businesses, the courts, and 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

Message

From: Rob Clarke [redacted]
Sent: 3/11/2020 3:02:30 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Clarification of the Sell My Info Opt Out requirement

CA AG Office,

Our business sells mostly on the web, about 80%. Further, while we do sell information about our customers, it is a certain class of our customers only (only about 5% of our customers).

Our question is, since we only sell customer information for abut 5% of our customers, can we ONLY target and offer the Opt-Out for the Sale of My Info to ONLY those customers? The 5%, and NOT offer the Sell My Info to our core customer base of 95% and still be compliant? W329-1

Common sense wise this makes sense, but it would be good to have the CA AG's office approval on only offering the Opt Out to our 5% customer base.

Thanks!

Robert Clarke
Chief Financial Officer
[redacted] | [redacted]
818.332.4172 Fax

National Notary Association
9350 De Soto Ave. | Chatsworth, CA 91311-4926
www.nationalnotary.org

Training | Membership | Advocacy | Insurance | Supplies

This message and any attached documents contain information from National Notary Association that may be confidential and/or privileged. If you are not the intended recipient, you may not read, copy distribute or use this information. If you have received this e-mail in error, please notify the sender immediately by reply e-mail and then delete this message.

Message

From: Robert Rutkowski [redacted]
Sent: 3/28/2020 11:32:35 AM
To: Xavier Becerra [Xavier.Becerra@doj.ca.gov]; Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Close Loopholes, Respect "Do Not Track" With 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: Close Loopholes, Respect "Do Not Track" With Regulations

Dear Attorney General:

A coalition of privacy advocates filed comments on the latest proposed regulations for the California Consumer Privacy Act (CCPA). The CCPA was passed in June 2018 and took effect on January 1, 2020. Later this year, California Department of Justice will finalize regulations that dictate how exactly the law will be enforced.

While the first set of proposed regulations were a "good step forward" that could have gone further, the first revision to those regulations–published earlier this year–was largely a step backwards for privacy. Two weeks ago,a second set of revisions to the draft regulations were released. With the enforcement deadline approaching, the public is running out of chances to weigh in on the rulemaking process. Some of the worst features of the regulations have been cut, but this round of modifications still falls short of a user-friendly implementation of CCPA. In fact, some new provisions added this round threaten to undermine the intent of the law.

For example, the CCPA sets aside a special set of companies, called "service providers," which are exempt from certain parts of the law. Consumers can't opt out of having their data sold to service providers in some interactions. In exchange, CCPA is meant to tightly restrict the ways service providers can use data they collect. However, the new draft regulations would greatly expand the ways service providers may use personal data, even allowing them to build profiles of individual people. The new regulations would also allow data brokers that collect information directly from consumers to avoid notifying them of the collection. W330-1

Other issues remain from earlier drafts. The latest draft still makes it hard for consumers to exercise their right to opt out of the sale of their personal information. Businesses may not need to treat clear signals like Do Not Track (DNT) as requests to opt out of sale. W330-2

Finally, some industry advocates have asked to extend the enforcement deadline–by 6 months or more–amid the global health crisis. But the CCPA went into effect on January 1st, 2020, more than 18 months after its passage, and companies should already be complying with the law. Now, more than ever, consumers need the legal protections offered by CCPA. The AG should not extend the enforcement deadline on behalf of companies who would violate user privacy and the law. W330-3

The coalition letter goes into more detail about these and other issues they have identified with the latest draft regulations. Close these business-friendly loopholes and make the CCPA an effective, enforceable tool for user 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=SfXZBZrDBuOzOawenWBVqlsrUHk7w701Rii07JqfVcg&s=5LQj44iDxYhq5LHFQjl5Qey8HzN-9qpskgc3zcOm4Rk&e=

2527 Faxon Court
Topeka, Kansas 66605-2086
P/F: 1 785 379-9671
E-mail: [redacted]

Re: Comment letter:
https://urldefense.proofpoint.com/v2/url?u=https-3A__www.eff.org_files_2020_03_27_2020.03.27-5F-2D-5Fprivacy-5Fcoalition-5Fcomments-5Fre-5F2nd-5Fmod-5Foag-5Fccpa-5Fregs.pdf&d=DwIDaQ&c=uASjV29gZuJt5_5J5CPRuQ&r=kXcUIWCJFJC3Y7A6WPl5oNx0wEUzL_7MxjOspe9bxxI&m=SfXZBZrDBuOzOawenWBVqlsrUHk7w701Rii07JqfVcg&s=GBsCxNuwsLDcdVFl9CVeS1kYMr2wjsY1pxK_nDGPkuQ&e=

Message

From: BC Smith [redacted]
Sent: 3/27/2020 1:11:15 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comment: § 999.315. Requests to Opt-Out

W331-1

Hello - thank you for your time. Below I outline my comments after conducting my own opt-out requests for various companies that sell personal information.

Comment:

As it relates to § 999.315. Requests to Opt-Out, there should be more clarity on how companies can allow authorized agents to opt-out an individual on their behalf. When I attempted to opt-out a friend as her authorized agent, I followed the correct guidelines and presented a signed document to a publicly traded company with 18,000 employees with a Request to Opt-Out.

The company responded with the following:

1. First, to tell the individual themselves to login to their account and opt-out

2. Second, they requested that the individual themselves respond to an email sent to their personal account email in order to opt-out.

This is problematic because it makes the job of the authorized agent impossible and defeats the point of allowing individuals to have authorized agents to opt-out on their behalf altogether. If the individual themselves is still required to take a number of actions in order to opt-out, why have authorized agents?

For more detail and evidence, below are two email responses I received from the public company:

Company Response 1:

"In order to facilitate the Opt-Out request for [INDIVIDUAL'S EMAIL ADDRESS], you can authenticate under their email address at [COMPANY URL] and follow the instructions found there.

NOTE: If you are acting on behalf of this consumer you may need to utilize the password associated with their [COMPANY] account in order to authenticate."

Company Response 2:

"In order for me to assist with the request for [INDIVIDUAL'S EMAIL ADDRESS] I just need two additional pieces of information noted below:

<!--[if !supportLists]-->• <!--[endif]-->The unique code that has been sent to the email address [INDIVIDUAL'S EMAIL ADDRESS]

<!--[if !supportLists]-->• <!--[endif]-->Please confirm [INDIVIDUALS] state of residence."

The companies second response came after I made it aware how problematic it would be for an authorized agent to login to an individuals account on their behalf. However, this response is still not sufficient and does not allow the authorized agent to fulfill their duties as the individual must still be involved in the process (responding to an email with a unique code).

Suggestions to act on Comment:

As it relates to § 999.315. Requests to Opt-Out, Request to Opt-out from authorized agents should not require the individual they are representing to take further steps in order to complete the opt-out. This includes having to respond to an email. Additionally, authorized agents should not be forced to login to password protected accounts for individuals in order to opt them out. As long as the authorized agent has followed the law, presented identifying characteristics about the individual, as well as a signature from the

individual, there should be a clear method or path to complete the opt-out and one that does not involve further action from the individual they represent.

W331-1 cont.

Thank you!

Message

From: Rachel Nemeth [redacted]
Sent: 3/27/2020 2:33:19 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments from CTA
Attachments: CTA Letter on Second Set of Modifications to Proposed CCPA Regulations (3-27-20) .pdf

Good afternoon,

See attached for comments from Consumer Technology Association (CTA).

Thank you,
Rachel

Rachel Sanford Nemeth
Senior Director, Regulatory Affairs
Consumer Technology Association, producer of CES®
d: [redacted]
m: [redacted]
CTA.tech | CES.tech

Disclaimer

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

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

Consumer Technology Association™

1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

March 27, 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 second set of modifications to the proposed California Consumer Privacy Act ("CCPA")[2] regulations.[3] As CTA has previously explained, since the CCPA was signed into law, companies of all sizes have raced to establish processes, policies, and systems to come into compliance. For many, this effort has already been a significant, challenging, and expensive initiative.[4]

CTA therefore supported those changes in the initial set of modifications that sought to reduce some of the confusion regarding businesses' regulatory requirements. CTA now recommends the following changes to provide more clarity and predictability for the many businesses that have implemented CCPA requirements in good faith:

- ***Section 999.302 – Guidance on What Information Constitutes Personal Information.*** CTA strongly supported the clarification 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."[5] CTA is disappointed that the guidance, which provided businesses with important clarifications as to what is being considered personal information, has been removed in the latest set of modifications. CTA believes it should be restored. W332-1

  The Department also should add new guidance clarifying the term "collect." Specifically, consistent with the definition set forth in the statute,[6] the Department W332-2

[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, Notice of Second Set Modifications to Text of Proposed Regulations, OAL File No. 2019-1001-05 (Mar. 11, 2020).
[4] *See* Comments of Consumer Technology Association on Proposed Adoption of California Consumer Privacy Act Regulations (filed Dec. 6, 2019) ("CTA Initial Comments"); Comments of Consumer Technology Association on Modifications to Proposed Regulations (filed Feb. 25, 2020) ("CTA Comments on First Set of Modifications")
[5] CTA Comments on First Set of Modifications at 1.
[6] Cal Civ. Code § 1798.140(e) (defining "collects" to mean "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means").

should make clear that "collect" does not refer to personal information that a business generates internally about a consumer, provided such information is not transferred or disclosed to any third parties. Without this clarification, businesses may feel that they need to provide this internal information in response to requests to know, a significant and burdensome operational challenge, despite the fact that this information typically will be confusing and not useful to consumers. W332-2 cont.

- ***Section 999.307(b)(5) – Notice of Financial Incentive; Section 999.301(j) – Definition of "Financial Incentive."*** CTA previously explained 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 such data.[7] CTA continues to believe that the Department should strike the requirements in subsection (b) to include information estimating the value of the consumer's data.[8] W332-3

  In addition, the most recent modifications define "financial incentive" to include "a program, benefit, or other offering, including payment to consumers, *related to* the collection, retention, or sale of personal information." This definition is overbroad, potentially capturing, for example, the delivery of a product purchased by a consumer simply because the consumer receives a benefit (*i.e.,* the product) that relates to the collection of his or her personal information, which is necessary for delivery. The modification is also not supported by the statute, which contemplates financial incentives more narrowly as "payments to consumers as *compensation*" for the collection, sale, or deletion of their personal information.[9] W332-4

- ***Section 999.313(c)(3) – Exceptions to Responding to a Right to Know Request.*** The draft regulations' four-part test for an exception to responding to requests to know is too narrow. There are many legitimate privacy, security, and operational reasons to not disclose specific pieces of information to a consumer that will not satisfy the current test.[10] At minimum, the Department should restore the exception for a disclosure that "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," and apply it to privacy risks as well. This exception ensures that businesses never have to face an impossible choice between compliance on the one hand and privacy and security on the other. W332-5

  The Department also should expressly exempt disclosures that would (1) interfere with law enforcement, judicial proceedings, investigations, or efforts to guard against, detect, or investigate malicious or unlawful activity or enforce contracts; (2) reveal the

[7] CTA Initial Comments at 5-6; CTA Comments on First Set of Modifications at 1-2.

[8] *See* CTA Comments on First Set of Modifications at -2.

[9] Cal. Civ. Code § 1798.125(b)(1) (emphasis added).

[10] In fact, it's unclear if the four-part test will be satisfied in most situations. For instance, if a business maintains personal information solely for legal or compliance purposes, then it typically will maintain such information in a searchable or reasonably accessible format, failing that part of the test.

covered entity's trade secrets or proprietary information; (3) require the covered entity to re-identify or otherwise link information that is not maintained in a manner that would be considered personal information; or (4) violate federal, state, or local laws, including rights and freedoms under the United States Constitution.[11]

W332-5 cont.

- ***Sections 999.313(c)(5) and 999.313(d)(6) – Responses to Denied Access and Deletion Requests.*** CTA generally reiterates its concerns about disclosing the reason why a particular request was denied.[12] Such individualized responses can significantly slow down the speed with which businesses are able to process and respond to consumers' requests. They also pose particular challenges to small businesses and startups that often need to rely on a lean staff and more manual processes to comply with the CCPA. Moreover, because businesses would need to provide the reason they deny the request except where they are prohibited from doing so by law, businssess would effectively be revealing that a legal restriction exists any time they decline to provide an explanation – that revelation alone could be inappropriate in many circumstances.

W332-6

- ***Section 999.314(c) – Service Providers.*** As revised, the proposed regulations impermissibly restrict service providers' use of personal information they receive beyond what's contemplated in the statute. Specifically, as currently drafted, a service provider may be prohibited from retaining, using, or disclosing personal information for the provider's own operational purposes as part of performing the services specified in the contract with the business, even though explicitly permitted by the statute.[13]

W332-7

- ***Section 999.315(d) – Requests to Opt Out through User-Enabled Privacy Controls***. As CTA previously explained, requiring businesses to respond to global opt-out mechanisms and signals that do not currently exist presents an unworkable situation to implement and operationalize, and can result in a distorted marketplace.[14] Although CTA's preference would be to strike the requirement entirely, CTA believes at minimum additional clarity is needed so that any such privacy controls actually effectuate consumers' determinations, rather than make judgments for consumers in the guise of consumer choice. To do so, the Department could restore the first clause of the sentence that was stricken in the latest set of modifications: "The privacy control shall require that the consumer affirmatively select their choice to opt-out."

W332-8

- ***Sections 999.323, 999.324, and 999.325 – Verification Methods.*** CTA continues to believe that the regulations should afford more flexibility in how businesses establish their verification procedures.[15] In particular, complying with the verification requirements for non-accountholders poses a particular challenge for many businesses, including small businesses and startups. For many businesses, it may not be practical to

W332-9

---

[11] Relatedly, the Department should make clear that businesses are not required to produce substantially similar or duplicative specific pieces of personal information in their responses to verified requests to know.

W332-5 cont.

[12] CTA Initial Comments at 7-8; CTA Comments on First Set of Modifications at 2.

[13] *See* CTA Initial Comments at 9-10.

[14] CTA Comments on First Set of Modifications at 3.

[15] *See* CTA Initial Comments at 12-13.

implement multiple identity verification methods that vary based on the request (right to know categories versus specific pieces of personal information) or sensitivity of the data. As a result, many businesses may need to default to a higher bar of verification, which in turn may lead to more consumer requests being denied if the consumer cannot be adequately verified.

W332-9 cont.

* * *

CTA appreciates the Department's continued efforts to adopt and implement CCPA regulations in a manner that enhances consumer privacy without being unduly burdensome on businesses, especially startups and other small businesses. With the two-year anniversary of the enactment of the CCPA quickly approaching – and businesses almost two years in on investing in, developing, and deploying systems and processes to comply with the CCPA – CTA encourages the Department to focus final modifications to the proposed regulations on providing additional clarity to both businesses and consumers, reducing still-remaining unjustified burdens on businesses, and ensuring that the regulations properly adhere to the requirements of the statute.

Sincerely,

/s/ Michael Petricone
Michael Petricone
Sr. VP, Government and Regulatory Affairs

/s/ Rachel Nemeth
Rachel Nemeth
Senior Director, Regulatory Affairs

Message

From: Tony Ficarrotta [redacted]
Sent: 3/27/2020 12:41:22 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: David LeDuc [redacted]; Leigh Freund [redacted]
Subject: Comments from the Network Advertising Initiative (NAI)
Attachments: NAI Comment Letter - CCPA Second Set of Modified Regulations (March 27, 2020).pdf

Thank you for the opportunity to submit comments regarding the second set of 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

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

March 27, 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: Second Set of Modifications to the 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 second set of modifications to the regulations proposed for adoption[1] under the California Consumer Privacy Act of 2018 (the "CCPA").[2]

The NAI is looking forward to the conclusion of the rulemaking process and appreciates the continued efforts of the Office of the Attorney General ("OAG") to that end. The NAI has identified several issues in the second set of modifications to the proposed regulations (the "Regulations") that would benefit from further clarifications and changes before the Regulations are finalized, 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 March 11, 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 Regulations. For example, the NAI Code requires member companies to provide consumers with an easy-to-use mechanism to opt out of different kinds of Tailored Advertising,[5] to disclose to consumers the kinds of information they collect for Tailored Advertising, and to explain how such information is used.[6] The NAI Code's privacy protections go further than the CCPA and the Regulations 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 Regulations should include guidance on the definition of personal information.

The first set of modifications to the Regulations added a new section titled "Guidance Regarding the Interpretation of CCPA Definitions," which consisted of guidance on the CCPA's definition of "personal information," as follows:[9]

> *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."*

In the NAI's comments on the first set of modifications to the Regulations,[10] we requested further clarification from the OAG as to when IP addresses would not be considered personal information. However, the second set of modifications to the Regulations did not provide any further guidance, and instead deleted the above guidance. W333-1

Removing this guidance without explanation is likely to cause confusion among businesses as they struggle to understand the OAG's intent in proposing the guidance in the first place (which many businesses will presume remains the OAG's intent, notwithstanding the deletion of the language). Further, there likely still are circumstances wherein an IP address does not meet the statutory definition of personal information. For example, merely establishing a TCP/IP connection essential to all internet communications involves collecting the IP address of the device; however, many website operators (like bloggers or other small business website operators) that are technically "collecting" IP in this way do not, and could not reasonably, connect that information to a particular consumer or household. Unfortunately, with the deletion of the guidance, it is now very unclear whether the OAG's expectation is for those businesses to treat their unavoidable and purely technical collection of IP addresses as involving personal information.

Consistent with our previous comments, the NAI recommends restoring the guidance on the definition of "personal information," but further clarifying it by specifying that information such as an IP address is not personal information unless the business processing such information

---

[9] CAL. CODE REGS. tit. 11, § 999.302 (proposed Feb. 10, 2020).

[10] *See* Letter from Leigh Freund, President & CEO, Network Advert. Initiative, to Xavier Becerra, Attorney Gen., Cal. Dep't of Justice 3-4 (Feb. 25, 2020), https://www.networkadvertising.org/sites/default/files/nai_comment_letter_-_ccpa_modified_proposed_regulations_february_25_2020.pdf.

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 and residential address.

Recommended Amendments to the Regulations:

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 addresses to any information known by the business to identify a particular consumer or household, such as a full name and residential address, and could not reasonably link the IP addresses with such information, the IP addresses would not be "personal information."

W333-1 cont.

Part II: Consumer Exercises of CCPA Rights and Business Responses

A. **The proposed regulations should clearly specify that businesses are not required to honor global privacy controls that do not represent an authentic consumer choice to opt out of sales.**

The second set of modifications to the Regulations include a change that could be interpreted as allowing software developers that will offer global privacy controls to offer those controls set "on" by default, despite the reality that the consumer using the control may never have interacted with those default settings, nor intended to opt out of a business's sale of personal information.[11]

W333-2

However, in order for the Regulations to implement the letter and spirit of the CCPA, it is imperative that they clearly stipulate the need for consumers to affirmatively elect to opt out of sales of personal information. If software developers aren't clearly prohibited from setting global privacy controls to "on" by default, that would risk reversing the CCPA's intended opt-out framework and put the onus on consumers to take affirmative steps to turn off global privacy controls (*i.e.*, forcing them to opt in). This would muddle the clear intent of the CCPA (and the original draft regulatory language) to establish a framework where businesses are permitted to sell personal information, subject to a consumer's right to opt out of those sales.

For example, suppose that a web browser developer updates its web-browsing software to include a new "do not sell" signal. Under the second set of modifications to the Regulations,

[11] *See* CAL. CODE REGS. tit. 11, § 999.315(d)(1) (proposed March 11, 2020) (removing the language prohibiting privacy controls from using pre-selected settings).

that developer would not have as clear an indication that such a signal could not be turned on by default.[12] In that case, and even assuming that the browser adequately notified users about the "do not sell" mechanism and informed them that it is turned on by default, users of the browser would still be in the position of having to take affirmative action to turn off the opt-out signal. This would present substantial challenges for businesses trying to determine which opt-out signals represent true consumer requests to opt out of sales, and which are contentless default settings. If the final regulations take this approach, it will likely result in extensive confusion in the marketplace.

If the language clearly prohibiting default settings is not restored, it will also put NAI member companies in the difficult position of needing to comply with the unambiguous requirement in the Regulations to honor "user-enabled" privacy controls[13] without any equally clear indication in the Regulations that software developers may not send opt-out signals by default. As highlighted above, the possibility of default-on settings is not consistent with the statute, and will undermine the ability of NAI member companies to determine in which cases a global privacy control is truly user-enabled (not enabled by software developers). For example, if a web browser ships an update with a "do not sell" setting on by default, the Regulations do not appear to require businesses to honor that signal because it is not "user-enabled." However, if a user were to toggle the setting off for a time, and then toggle it back on at a later time, it arguably *would* be user-enabled. But businesses receiving the signal would have no way of differentiating which opt-out signals from that type of browser are user-enabled and which are not. As such, the best way to ensure that user-enabled global privacy settings are consistently honored is to clearly prohibit them from being set on by default. That way, businesses will know that whenever they encounter such signals, they were enabled by the user.

W333-2 cont.

Finally, and not least of all, the proposed change places enormous discretion in the hands of large browser providers, who often are large businesses with significant data assets, and in some cases have their own advertising operations. Giving them the ability to control – virtually unilaterally, without consumer choice – the data rights of their (generally much smaller) competitors implements a business framework that is structurally anti-competitive. Even ascribing the best of intentions to those browser companies, by implementing a data rights structure that permits the largest of companies to control the data rights and data inventories of their competitors is a bad idea – at a minimum, it will deter competition and market entry. It is thus anti-competitive and ultimately will narrow choices for advertisers, publishers and consumers by significantly limiting competition (and presumably, driving up prices) in a US market that is vital to both advertisers (large and small), content publishers, and news organizations.

For those reasons, the NAI recommends that the Regulations be amended to restore the language prohibiting pre-selected opt-out settings:

[12] *See id.*
[13] *See id.*

Recommended Amendments to the Regulations:

Section 999.315(d)(1):

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.

W333-2 cont.

Part III: Service Providers

A. The proposed regulations should further clarify permissible internal uses of personal information by service providers obtained in the course of providing services.

The first set of modifications to the Regulations referred to a service providers' ability to "clean" or "augment" data acquired from another source.[14] The NAI advocated for removing reference to the terms "cleaning" and "augmenting" because they are not defined by the CCPA or the Regulations, and have no common meaning in the digital advertising industry.[15] Imposing requirements on service provider activity using terms without definitions or accepted meanings is likely to lead to inconsistent interpretations of those requirements. Nonetheless, the second set of modifications to the Regulations retained the basic structure of the requirement, but changed the word "cleaning" to "correcting."[16]

W333-3

Even with this change, the Regulations are likely to cause confusion as to when service providers may engage in the simple and beneficial practice of improving the quality of data provided by one business with data already acquired from another business. The ability of service providers to improve the accuracy of data used by businesses they serve in this way does not present any appreciable risk to consumer privacy – but confusion about whether the Regulations permit it would lead to additional costs to businesses who may end up directing communications to consumers using, *e.g.*, an email or physical mailing address with a typo or other error. Costs for errors like that may run into the billions of dollars per year.[17] Those errors may also prevent consumers from receiving mis-directed communications.

To address the issues identified above, the NAI recommends further amending the Regulations as follows.

---

[14] CAL. CODE REGS. tit. 11, § 999.314(c)(3) (proposed Feb. 10, 2020).
[15] *See* Letter from Leigh Freund, President & CEO, Network Advert. Initiative, to Xavier Becerra, Attorney Gen., Cal. Dep't of Justice 14 (Feb. 25, 2020), https://www.networkadvertising.org/sites/default/files/nai_comment_letter_-_ccpa_modified_proposed_regulations_february_25_2020.pdf.
[16] CAL. CODE REGS. tit. 11, § 999.314(c)(3) (proposed March 11, 2020).
[17] *See* Letter from Kenneth M. Dreifach, Shareholder, ZwillGen, to Xavier Becerra, Attorney Gen., Cal. Dep't of Justice (Feb. 25, 2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-15-day-comments-022520.pdf.

Recommended Amendments to the Regulations:

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 to use in providing services to another business~~, or correcting or augmenting data acquired from another source~~.

W333-3 cont.

Part IV: Enforcement

A. The OAG should delay enforcement of the Regulations until March 1, 2021

The NAI appreciates the fact that the OAG has engaged so thoroughly with the CCPA rulemaking process by carefully considering several rounds of written comments and making modifications to the Regulations where appropriate, including a number of material changes that affect compliance obligations for businesses. However, an inevitable consequence of that deliberative process is a rapidly diminishing timeline for businesses to understand and implement the final regulations.

There are a mere 66 working days until the July 1st enforcement date for the CCPA as of the writing of this letter.[18] However, businesses cannot reasonably plan compliance with the complex requirements of the Regulations before they are finalized. Further, businesses will likely have far fewer than 66 business days to prepare, as the OAG will need time to review this round of comments (even assuming there are no further material modifications), and the Office of Administrative Law may take up to 30 working days to approve the final regulations.[19]

W333-4

Coming into material compliance with final regulations on such a short timeline would be extraordinarily difficult for businesses in ordinary times; however, the global COVID-19 pandemic has put unprecedented strain on the resources of NAI member companies and the entire global economy. The closing of physical workplaces has made collaboration difficult across and among product, legal and engineering teams, not to mention the human dimension of the pandemic. Concentrating resources into short-term compliance efforts would place further strain on businesses already struggling to maintain normal operations in the face of both office closures and increased childcare and education responsibilities of employees with children whose schools have closed.

Due to the already dwindling time until July 1st, and these uniquely difficult circumstances, the NAI respectfully requests a delay in the OAG's enforcement of the CCPA until March 1, 2021.

[18] *See* CAL. CIV. CODE 1798.185(c).
[19] https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-rulemaking-fact-sheet.pdf

Conclusion:

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

Message

From: Justina Sullivan [redacted]
Sent: 3/26/2020 4:30:29 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Andrew Yang [redacted]
Subject: Comments of Andrew Yang concerning Regulations under The California Consumer Privacy Act
Attachments: Letter to California AG 3.26.20 .pdf

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

Please see attached document with comments of Andrew Yang regarding the Proposed Regulations under the California Consumer Privacy Act ("CCPA").

Best regards,

Justina Sullivan
--
HUMANITY FORWARD
Justina E. Sullivan
c: [redacted]
e: [redacted]

HUMANITY FORWARD

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

Dear Ms. Kim:

On behalf of Humanity Forward, a 501(c)(4) non-profit organization that advocates for the core ideals of my presidential campaign, we first want to thank you for the extraordinary work you do on behalf of the people of California.

As some people in the California Office of the Attorney General ("Office") may know, one central focus of my presidential campaign was around the issue of data privacy and data as a property right for individuals (https://www.yang2020.com/policies/data-property-right/). That is why we are taking great interest in your work finalizing the interpretations of the regulations of the California Consumer Privacy Act ("CCPA"). In addition, Humanity Forward plans to advocate for similar pro-consumer legislation in all 50 states using CCPA as the gold standard.

In that light, we have closely reviewed the First set of modifications (as of February 10, 2020) and the Second set of modifications (as of March 11, 2020) (collectively the "Proposed Regulations"). We would like to offer the following comments regarding the Proposed Regulations, especially as they relate to the notice requirements for data brokers.

The CCPA (Cal. Civ. Section 1798.100 et seq.) states the following regarding data brokers:

- Section 1798.120 of the CCPA is unequivocal about the notice obligations of businesses, including data brokers: "(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." (Emphasis added).

- Section 1798.115 of the CCPA also contains a specific provision intended for data brokers: "(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.*" (Emphasis added). There are no exceptions to this requirement anywhere in the CCPA.

W334-1

Section 1798.99.88 of the California Data Broker Act ("CDBA") (Cal. Civ. 1798.99.80 et seq.) is consistent with the CCPA, and it does not give data brokers any exceptions. That section states, "[n]othing in this title shall be construed to supersede or interfere with the operation of the California Consumer Privacy Act of 2018," and there is no discussion of any less stringent notice requirements for data brokers before they may sell consumer data.

Unfortunately, we believe that the current Proposed Regulations directly contradict how data brokers are to be regulated under the CCPA. Specifically, Section 999.305(e) of the Proposed Regulations currently states:

> "A data broker registered with the Attorney General 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."

As currently drafted, Section 999.305(e) is inconsistent with the current text of the CCPA. The proposed language expressly contradicts the language of Cal. Civ. Section 1798.115(d). In fact, the original language of Section 999.305(e) (then 999.305(d)) shows that the Office's original interpretation was also that data brokers needed to provide notice under the CCPA by contacting the consumer directly to provide notice *before* selling the consumer's personal information. Unless clarified, data brokers may argue that under Section 999.305(e), their notice obligations are weaker than those of non-data brokers, which results in an absurd outcome.

W334-1 cont.

Moreover, we note additional textual conflicts created by Section 999.305(e). For example, Section 999.306(e) states 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 notice posted unless it obtains the affirmative authorization of the consumer." This language also arguably contradicts 999.305(e). Data brokers should be subject to the same notice requirements as non-data brokers, as Section 999.306(e) appears to require.

The language originally proposed for Section 999.305(e) (then 999.305(d)) is in accord with Cal. Civ. Section 1798.115(d). And we believe that Section 999.306(e) reinforces the Office's original reading of the notice requirement as it applies to data brokers, and the Office should adhere to the unequivocal language of Cal. Civ. Section 1798.115(d). Sections 999.305(e) and 999.306(e) must be consistent. The CCPA clearly requires that data brokers provide notice before they sell, and the Office's initial interpretation retained that notice requirement.

Hence, we strongly urge the Office to either (1) revert to the original language in the first draft (then Section 999.305(d)) requiring data brokers to "[c]ontact the consumer directly to provide notice" before they sell a consumer's personal information, or (2) delete the revised Section 999.305(e) so that data brokers are subject simply to Section 999.306(e). We strongly believe that interjecting any ambiguity whatsoever via the interpretations of the regulations will severely hurt, not help, the consumer.

Conclusion

In sum, we wholeheartedly thank the Office for your advocacy on behalf of all Californians. We urge the Office to reject any language that diminishes the data broker's notice obligations under the CCPA. Moreover, we demand that clarifications be made in favor of an individual's right to data privacy and ownership whenever an ambiguity in language may exist. By passing the CCPA, the people of California have clearly spoken, and the law should not be abridged or diluted.

HUMANITY FORWARD

Please feel free to reach me directly at Humanity Forward at [redacted]. I am happy to discuss further my position by video, or in person should the circumstances allow. Thank you for your time and consideration.

Sincerely,



Andrew Yang
Founder, Humanity Forward

Message

From: Abrahamson, Reed C.F. [redacted]
Sent: 3/27/2020 2:54:21 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Blenkinsop, Peter [redacted]
Subject: Comments of the IPMPC on the 2nd Set of Modifications to the Proposed CCPA Regulations
Attachments: IPMPC Comments on v3 of Revised CCPA Regulations.PDF

To Whom it May Concern:

Please find the IPMPC's written comments on the second set of revisions to the 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

Welcome to **Faegre Drinker Biddle & Reath LLP (Faegre Drinker)** – a new firm comprising the former Drinker Biddle & Reath and Faegre Baker Daniels. Our email addresses have changed with mine noted in the signature block. All phone and fax numbers remain the same. As a top 50 firm that draws on shared values and cultures, our new firm is *designed for clients*.

This message and any attachments are for the sole use of the intended recipient(s) and may contain confidential and/or privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message and any attachments.

IPMPC
International Pharmaceutical &
Medical Device Privacy Consortium

March 27, 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.

The IPMPC appreciates the revisions made by the Attorney General to the first and second drafts of the CCPA regulations. The changes in the third draft provide additional clarity to businesses, but contribute to uncertainty by removing key guidance. The IPMPC also wishes to reiterate its previous requests that the Attorney General clarify important aspects of the draft regulations. In particular, the IPMPC wishes to call the Attorney General's attention to its previous comments on §§ _.301(c); _.305(a)(3); _.306(e); _.313(d)(3); _.314(c); _.314(e); and _.317(g)(2). A copy of each of our previously submitted comments are attached as appendices for ease of review. W335-1

Further, the IPMPC reiterates its request from our initial and second 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.

§ _.302 The IPMPC believes the previous interpretative guidance on the definition of "personal information" provided by the Attorney General in this section should be restored. As the IPMPC noted in its February comments, that interpretative guidance offered needed clarity about the standard to be applied when determining whether data held by a business is "personal information."

As noted in prior comments, in many cases, IPMPC members collect data for medical or scientific research that includes information that member companies do not and could not link to a specific person. For example, an IPMPC member company might be engaged in epidemiological research to understand the scope and course of a rapidly emerging and spreading disease. To better understand where the condition has originated and how it is being treated, an IPMPC member company might partner with a public health or health care organization that has data about patient experiences and outcomes. To conduct its research and consistent with the ethical guidelines applicable in these scenarios, the IPMPC member would not receive this data in a reasonably identifiable format. However, the data may contain information which appears on the list of data elements included in the definition of "personal information" under the CCPA "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." IPMPC members need clarity about how such data elements should be treated where they are not reasonably identifiable but could possibly be viewed as "relating to" "particular" individuals. The removal of the Attorney General's interpretative statements creates uncertainty and confusion W335-2

around an important issue affecting research relevant to the health and well-being of Californians.

As noted before, the IPMPC believes that a clarifying statement about what information should be considered either deidentified or not personal information would be helpful. The IPMPC continues to urge 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. W335-2 cont.

§ _.308(c) In both § 999.308(c)(1)(d) and (2)(d), the proposed regulations call for the inclusion of a "general" description of the verification process that will be used when a consumer seeks to exercise their rights. However, the verification process used may vary significantly depending on who the consumer is, what information the business has about the consumer, the nature of the relationship between the business and the consumer, and the standard that needs to be satisfied to "verify" the consumer based on the data possessed by the business. The IPMPC believes that even with the addition of the modifier "general," the requirement to describe the process used to verify the consumer presents significant practical challenges. For example, verifying the identity of a patient-support program participant, where a member company may have repeated interactions over a period of years and the data includes sensitive health information, will follow a different process than verifying the identity of a consumer who signed up for a mailing list, but otherwise has no interaction with the company. W335-3

Consumers should be informed that there will be a verification process, but providing a description of that process that applies to all consumers will require either the use of unhelpful generic statements or presenting descriptions of several possible processes, most of which the consumer will not encounter. At a minimum, the requirement to describe the process should be moved to the first response to the consumer acknowledging their request, at which point the business may have a better idea of the nature of the process that will be required for that consumer.

§ _.313(c)(3) The IPMPC continues to urge the Attorney General to reconsider the deletion of text from the original draft regulations that occurred in the February draft. This text was not restored in the most recent draft. The IPMPC previously commented on this deletion but wishes to reiterate that the Attorney General would best serve W335-4

Californians by more explicitly permitting businesses to withhold information when disclosure would put other consumer's personal information or the business itself at risk. The initial draft of the regulations appropriately provided further clarity around Civil Code 1790.145(l). The current draft of the regulations creates unnecessary uncertainty as to whether a business is permitted to decline to disclose information to consumers when it reasonably believes that disclosure creates a risk of harm for other consumers or the business's employees—for example, where disclosure of negative profile information might cause retaliation or harassment. Such a standard is reasonable and consistent with other privacy and data protection regimes. W335-4 cont.

§ _.313(d)(7) The IPMPC opposes the requirement to offer unverified consumers the option of opting out of the sale of information. In many instances where verification cannot occur, the business will also lack the necessary information to implement an effective opt-out. Requiring that the business offer an opt-out it could not deliver would lead to consumer frustration without delivering tangible benefit to consumers. W335-5

§ _.317(e) The IPMPC appreciates that the Attorney General revised the restriction on sharing record-keeping information with third parties to explicitly acknowledge that such information may be shared where required by law. Nevertheless, we reiterate our previous request that the Attorney General also make it clear that the information may be shared when an exception to the CCPA applies—like in the course of defending a legal claim or when exercising an evidentiary privilege. W335-6

We thank you for the opportunity to provide these comments.

Sincerely,

Peter A. Blenkinsop
IPMPC Secretariat

Appendix 1:

IPMPC Comments on Initial Proposed Regulations

IPMPC
International Pharmaceutical &
Medical Device Privacy Consortium

December 6, 2019

Mr. Xavier Becerra
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street, First Floor
Los Angeles, CA 90013

By Email to: PrivacyRegulations@doj.ca.gov

Re: CCPA Proposed Regulations

Dear Attorney General Becerra,

The International Pharmaceutical & Medical Device Privacy Consortium ("IPMPC") welcomes the opportunity to provide comments on the proposed regulations under the California Consumer Privacy Act (CCPA).

The IPMPC is comprised of chief privacy officers and other data privacy and security professionals from a number of research-based, global pharmaceutical companies and medical device manufacturers.[1] The IPMPC is the leading voice in the global pharmaceutical and medical device industries to advance innovative privacy solutions to protect patients, enhance healthcare, and support business enablement.[2]

W335-1 cont.

The IPMPC is concerned that some of the requirements in the proposed regulations go beyond the requirements laid out in the statute and create burdensome obligations for businesses

[1] IPMPC members may also operate related businesses, including CLIA laboratories.

[2] More information about IPMPC is available at https://www.ipmpc.org/. This filing reflects the position of the IPMPC as an organization and should not be construed to reflect the positions of any individual member.

without creating proportional benefits for consumers. In particular, we are concerned with the following requirements related to the notice at collection of personal information:

- Section 999.305(b)(2) would require that the notice state the business or commercial purposes for which the information will be used "for each category of personal information." This requirement will lead to significant redundancy and unnecessary length of privacy notices. In many cases, all categories of information collected from a consumer are used for the same set of purposes. For example, a company providing voluntary patient support programs will require (at least) a patient's name, contact information, medical information, and health insurance information. Rather than permitting a company to say "We collect your name, contact information, medical information, and health insurance information to provide our voluntary patient support program," the regulations appear to require a company to provide the notice in this format:

  > We collect your name to provide our voluntary patient support program.
  > We collect your contact information to provide our voluntary patient support program.
  > We collect your medical information to provide our voluntary patient support program.
  > We collect your health insurance information to provide our voluntary patient support program.

  The amount of repetitive text required above would only increase once disclosures about sources of information and any information sharing are added.

  Businesses should be permitted to aggregate or group the categories of personal information when the information that must be disclosed is the same. Requiring differentiation by category of personal information will lead to long, repetitive notices that will be difficult for consumers to understand.

- 999.305(b)(4) requires that the notice include a link to the business's CCPA privacy policy or the web address of the policy. This paragraph should be amended to make clear that in the case of employees, this requirement can be satisfied by directing individuals to the relevant employee privacy policy, whether online (including on a company's internal extranet) or offline (e.g., in an employee manual).

W335-1 cont.

In addition to the above concerns with the notice at collection of personal information, the IPMPC is also concerned with the requirement that "[i]f the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose" (emphasis added). This requirement for explicit consent is unnecessary where the consumer's intentions are clear from his or her actions.

The IPMPC encourages the Department of Justice to publish samples of the various types of notices and responses to "requests to know" that would be required under the proposed regulations. This will aid businesses in their compliance efforts.

Finally, the IPMPC notes that there are various circumstances in which a business is not permitted to disclose specific pieces of information in response to a consumer's request to know. In particular, Section 999.313(c)(3) states that "[a] business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks" (emphasis added). We suggest modifying the underlined text to read: "a substantial and articulable, or otherwise unreasonable, risk." Moreover, we encourage the Department to add "medical information" and other data elements the unauthorized disclosure of which could trigger a breach notification requirement under California law to the list of data elements in Section 999.313(c)(4) that do not require disclosure in response to a request to know specific pieces of information. W335-1 cont.

We thank you for the opportunity to provide these comments.

Sincerely,

Peter A. Blenkinsop
IPMPC Secretariat

Appendix 2:

IPMPC Comments on First Modifications to Proposed Regulations



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.

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.

§ _.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. W335-1 cont.

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.

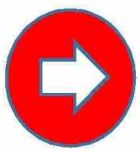
§ _.305(a)(3) The IPMPC appreciates the Attorney General's inclusion of additional examples, and requests that the Attorney General clarify § 999.305(a)(3)(d) to make it clear that, when a business collects information over the telephone or in person, in addition to the option of providing notice orally, 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).

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?

§ _.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.

§ _.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. W335-1 cont.

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

other buttons on the business's website" should be made conditional, and apply only when other buttons are present.

§ _.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.

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.

W335-1 cont.

§ _.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.

§ _.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.

§ _.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.

§ _.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. W335-1 cont.

§ _.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.

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. W335-1 cont.

We thank you for the opportunity to provide these comments.

Sincerely,



Peter A. Blenkinsop
IPMPC Secretariat

Message

From: Stacey Olliff [redacted]
Sent: 3/24/2020 11:36:18 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Legal [redacted]
Subject: comments on latest CCPA draft regulations

Ms. Kim,

Re-submitting the comments I made on February 28 in relation to the latest draft of the CCPA regs.

From: Stacey Olliff [redacted]
Sent: Friday, February 28, 2020 1:52 PM
To: 'PrivacyRegulations@doj.ca.gov' <PrivacyRegulations@doj.ca.gov>
Cc: 'Legal' [redacted]
Subject: Comments on revised CCPA regulations

Ms. Kim:

Our company, Prodege LLC, operates consumer-facing websites and mobile apps in California and we have the following comments on the revised CCPA regs: W336-1

1. In 999.312(a), it says you can use just email address if you "*operate exclusively online*" and have a direct relationship with a consumer, but that is too high a bar for almost anyone to meet. We are an online-only consumer-facing business, but obviously we have a physical office, have employees, meet with business partners, go to tradeshows, etc. and therefore, it isn't clear if we would "operate exclusively online" given the breadth of CCPA's coverage to include employees, business contacts, etc. So this needs to be clarified somehow. It would be useless to say that we can provide merely an email address for the 99% of the consumer information collection that we collect online, but we still have to create a toll-free number for our employees, business contacts, etc. because we may sometimes collect "consumer" information from them in the physical world. Not sure the best language, but ideally something like: "***For this purpose, a business will be considered operating exclusively online if it operates principally online and has no physical stores or other consumer-facing physical locations in the state of California, even if it does have an office with employees, interacts in person or by telephone with business partners, attends tradeshows, etc.***" If need be, to the extent a business considered operating exclusively online does *sometimes* get consumer information in the physical world from employees, in business meetings, at trade shows, etc., then *as to those "consumers" only*, a notice methodology like the provision in 999.306(b)(2) for opt-out requests should apply to requests to know (and requests to delete) as well.

2. Also in 999.312(a), it says if a business does operate exclusively online and has a direct relationship with a consumer, it shall only be required to *provide an email address* for submitting requests to know. But under 999.306(b)(1), a business is required to use an online link (*not an email address*) for requests to opt-out. Many CCPA compliance services like OneTrust, etc. use an online link/webform to submit all CCPA requests, rather than an email address. This allows for proper tracking of CCPA requests, improves compliance, tracks response times, allows for easy statistical reporting, etc. For some reason, if you are not an exclusively-online business, you can use a toll-free number plus a variety of other methods to meet the two-designated-methods requirement, and you can use an online link rather than an email address for the second method. **So in this regard, the regulation is actually inadvertently limiting/hurting online-only businesses by making it difficult or inefficient for them to use comprehensive services like OneTrust for compliance (although I doubt that was intended), because then they would then have to also maintain a completely unnecessary toll-free number that no one will likely use.** So the first sentence of 999.312(a) should be revised to read: *"A business that operates exclusively online…shall only be required to provide an email address* ***or a link or form available online through a business's website*** *for submitting requests to know."*

3. In 999.312(b), it says a business has to offer two or more designated methods for submitting requests to delete. **Why is there not a special one-method rule for online-only businesses for submitting requests to delete?** Shouldn't an online-only business be able to use the same method for both requests to know and requests to delete, and shouldn't that method be a *single* method, either via an email address or a link or form available online through a business's website? **It would be very confusing and unnecessarily complicated to require a consumer to use an online link to submit opt-out requests, an email address to submit requests to know, and possibly two different methods to submit requests to delete.** Services like OneTrust are designed to centralize all this in the single "link or form available online" approach, so that should be permitted for all types of CCPA requests (and online-only businesses should not be required to maintain an unnecessary second method that will seldom if ever be used and only complicate attempts to organize compliance efforts in a centralized fashion).

W336-1 cont.

Thank you if you can help get these comments considered in the finalization of the regulations. Please feel free to let me know if you have any questions.

Regards,

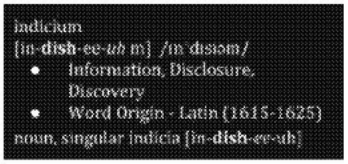
Stacey

Stacey Olliff, Esq.
SVP, Business & Legal Affairs | Prodege, LLC
Home of Leading Rewards Platforms: swagbucks.com | mypoints.com | shopathome.com | inboxdollars.com | mygiftcardsplus.com
o. [redacted] |c. [redacted] | [redacted]
100 N. Pacific Coast Highway, 8th Floor, El Segundo, CA. 90245
www.prodege.com

Message

From: Lynn Goldstein [redacted]
Sent: 3/27/2020 12:38:31 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments on Second Set of Modifications to Text of Proposed Regulations
Attachments: CCPA Proposed Regulations Comments.docx

Attached are the comments of Indicium LLC.



March 27, 2020

Lynn A. Goldstein
[redacted]

VIA E-MAIL (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

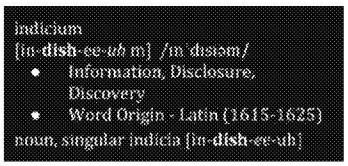
Re: Second Set of Modifications to Text of Proposed Regulations Regarding the California Consumer Privacy Act

Dear Ms. Kim:

Indicium LLC appreciates the opportunity to comment on the Second Set of Modifications to the text of the Proposed Regulations regarding the California Consumer Privacy Act (Proposed Regulations) and compliments the Office of the Attorney General on drafting very thorough Proposed Regulations. The founder of Indicium, Lynn A. Goldstein, was the Chief Privacy Officer of JPMorgan Chase for ten years and currently is a Senior Strategist for the preeminent global information policy think tank, the Information Accountability Foundation. Indicium is a privacy and data protection consulting firm whose clients include multi-national organizations that use Indicium to help build and improve privacy programs, explore privacy regulatory and compliance duties, and establish data governance and incidence response plans. Indicium writes solely to comment on a gap in the definition of "sale" in the California Consumer Privacy Act (CCPA) created by the expansion of the definition of "service provider" in the First and Second Set of Modifications to the Proposed Regulations.

Section 1798.140(v) of the CCPA defines a "service provider" as an entity "that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the purposes specified in the contract for the business . . . ." Section 999.314(b) of the Proposed Regulations was modified to provide: "To the extent that a business directs a second business to collect personal information directly from a consumer, or about 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."

W337-1



Section 1798.140(t)(2) of the CCPA provides: "a business does not sell personal information when: . . . (C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions is met: (i) The business has provided notice that information [is] being used or shared in its terms and conditions consistent with Section 1798.135 [the "Do Not Sell My Personal Information" link provisions in the CCPA]. (ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose." The definition of "sale" was not modified to correspond to the modifications in the First and Second Set of Modifications to the Proposed Regulations that deems a business's collection of personal information on behalf of another business to be in the capacity of a "service provider." W337-1 cont.

Indicium suggests that the Proposed Regulations need to be modified as follows: "a business does not sell personal information when the business directs a second business to collect personal information directly from a consumer, or about a consumer, on the first business's behalf if it is necessary to perform a business purpose as long as both of the following conditions is met: (i) the business has provided notice that information is being used or shared in its terms and conditions consistent with Section 1798.135 [the "Do Not Sell My Personal Information" link provisions in the CCPA]. (ii) The second business does not further collect, sell or use the personal information of the consumer except as necessary to perform the business purpose."

Thank you for the opportunity to comment on the Second Set of Modifications to the Proposed Regulations.

Sincerely,

Lynn A. Goldstein

Message

From: Walsh, Kevin [redacted]
Sent: 3/23/2020 6:41:35 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Levine, David [redacted]
Subject: Comments on the proposed California Consumer Privacy Act Regulations
Attachments: Spark CCPA Regulations Comment Letter 03172020v3.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

Notice: This message is intended only for use by the person or entity to which it is addressed. Because it may contain confidential information intended solely for the addressee, you are notified that any disclosing, copying, downloading, distributing, or retaining of this message, and any attached files, is prohibited and may be a violation of state or federal law. If you received this message in error, please notify the sender by reply mail, and delete the message and all attached files.

SPARK INSTITUTE
SHAPING AMERICA'S RETIREMENT

March 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 March 11, 2020 (the "Revised Proposal") to its proposed regulations under Chapter 20 of the California Code that had been published on October 11, 2019 and then initially revised on February 10, 2020 (the "Initial Proposals"). 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 appreciate the efforts the Attorney General's office has made to address concerns of employers and others providing benefits and continue to request that your office provide a model notice at collection for employers and that the regulations make it clearer that the collection and sharing of information gathered from identified fraudsters is acceptable, as it is a vital way of protecting participants and beneficiaries from the theft of their benefits. W338-1 W338-2

Today we write to emphasize the need to ensure that the employment and benefits specific pieces of CCPA do not sunset at the end of 2020. We believe it is a goal of all branches of California's government to protect employees, their families, and their beneficiaries by encouraging employers to provide benefits. We are already hearing concerns about the problems that would arise if these provisions were allowed to sunset. Given the unrelated economic disruptions that have already impacted employers this year, we ask that you ensure that the employment and benefits specific pieces remain in place beyond 2020. W338-3

* * * * *

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].

Sincerely,

Tim Rouse
Executive Director

Message

From: Aleecia M McDonald [redacted]
Sent: 3/27/2020 3:38:12 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments re: CCPA regulations - 2nd set of modifications
Attachments: McDonald-CCPA-Rulemaking-AG-Comments-Mar27.pdf

Thank you for the opportunity to comment.

Aleecia

Assistant Professor Aleecia M. McDonald // Carnegie Mellon's Information Networking Institute // [redacted]

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

[redacted]

March 27, 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.

Introduction

Thank you again for the opportunity for comment. COVID-19 enforces brevity.

Below, I make two points:

1. IP addresses are personally identifiable information (page 2,)
2. Suggestions of how to establish rules for the development of a CCPA button under Civil Code 1798.185(a)(4), also to include mature development of a header signal as currently described in 999.315.

Addressing IP Addresses

In section 999.302, it is suggested that not all IP addresses are "personal information" under Civil Code section 1798.140.

There are three reasons why I believe it is a mistake to treat IP addresses as anything less than personal information. The first two are technical, the final is legal.

W339-1

1. Static and stable assignment

IPv4 is the format most of us think of for IP addresses, for example 128.2.13.137. IPv4 addresses are assigned in one of two ways:

- Static, meaning a device has a stable address assigned uniquely to it over time. Just as a phone number is stable over time, a static IP address is rather straight-forward as a stable, persistent identifier for a device. It is personal information.
- Dynamic, meaning each time a device connects it is assigned a different number from a pool of available numbers. It is tempting to imagine that in this case, IP addresses do not identify people. In some circumstances that may be true, however:

- Personal information may leak from the IP address itself. To continue the example above, any IP address that starts 128.2 is from Carnegie Mellon. Especially combined with other seemingly non-identifiable information, IP address can very quickly re-identify specific people. IP address also strongly implies geographic location. This semester I assigned my students the task of trying an IP lookup on their own machines from home. Their location was usually pinpointed within a few blocks, just from their IP address without additional information.
- More concerningly in this context, many ISPs simply keep the same dynamic address for a device for an extended period of time. How long? It is up to the ISP to configure. As an anecdote, an online marketing firm described "…a patented technology of matching IP addresses to a database of names and physical street addresses and displaying your display or video ads only to those households (or businesses). It works without cookies and cannot be deleted or blocked. … Research has found that many households that have dynamic IP addresses (meaning the IP address is randomly assigned and can change) actually have held the same IP address for multiple years. We have found that the average household targeted by one of our IP Targeting campaigns has had the same IP address for nine months."[1] While I cannot verify this claim, it is entirely plausible.

W339-1 cont.

Most Californians have never heard of a DHCP lease, do not understand it has privacy implications, and cannot change the network management decisions of their ISPs. If Californians prefer not to be uniquely identified by IP address, they may have no practical options. An IP address can be as uniquely identifying as a phone number, and in many cases can be linked to their physical home address. This is personal information. Further, there is no way at first impression for a website operator to know if they have collected a customer's short-term dynamic IP address (perhaps an hour in a café) or a very long-term stable IP address (perhaps several years at home.) The only way to tell is after data collection, and after time elapses – after collection and use have occurred, and it is too late to be relevant.

2. Future IP format

Second, while IPv4 is the format of IP address most of us think of today, the future for the Internet depends up the longer IPv6 format. We are effectively out of new IPv4 address blocks, so now we need longer numbers with a different format. The transition is well in progress.

An IPv6 address can be assigned in privacy-preserving ways, but instead operating systems like Windows embed the device's unique MAC address.[2] Putting the MAC address into the IPv6 address is functionally like having a serial number for every piece of hardware that is included in all IP addresses. As new Internet of Things devices come online – cars, toasters, sensors, toothbrushes – the need for more IP addresses will accelerate the ongoing transition to IPv6. IPv6 is already heavily used by cell phones. For example, in 2018 Verizon used IPv6 for 80% of IP addresses issued and

[1] Dana Bojcic, "How often do IP addresses change? (Example)" *Vici Media*, May 8, 2017. Available from <https://www.vicimediainc.com/often-ip-addresses-change/>

[2] An address set in networking hardware, not to be confused with the Macintosh line of computers from Apple; a Mac has a MAC.

90% of their traffic used IPv6; T-Mobile announced plans to drop IPv4 entirely.[3] Any IPv6 address that includes a MAC address is personal information.

Again, citizens are not likely to know which version of IPv4 or IPv6 their providers choose, or even that there are different formats with different privacy characteristics. There are no practical opt outs for consumers who wish not to be identified by IP address.

For these two technical reasons, I strongly urge a decision that IP addresses are personal information.

W339-1 cont.

3. Consistency

Last, IP addresses are commonly held to be PII in other jurisdictions. I see no compelling reason to create regulatory burden on companies by establishing divergent legal standards in this area.

Recommendation: revise 999.302 to read in full: "For the purposes of the California Consumer Privacy Act, IP addresses are personal information."

Less Preferred Alternative: revise 999.302 from "a particular consumer or household" to "a particular consumer or household or device"

Button and header signal development

Thank you for taking the time to consider a thoughtful deployment of a privacy control button. In a prior regulation draft, section 999.315 had specifics of how a Do Not Sell My Info button would look. Under the legal code of 1798.185(a)4 the Attorney General's office is required to establish the rules for the development of a button.[4]

I suggest this is the right time to create those rules, with the particulars of a button to follow shortly. Similarly, a browser control such as a header signal can go through a parallel and perhaps even overlapping process.

From my experience with Do Not Track, and watching the multi-stakeholder processes from the Department of Commerce, I suggest the following approaches.

W339-2

1. Establish metrics for success and criterion for choosing between final fully-developed proposals for a button and browser-based signal. For example, you might consider:
   a. Top priority: usability tests demonstrate Californians are best able to enact their preferred privacy choices, with testing for under 13, 13 to 16, 16 to 70, and over 70 years old. Tests must take into account not just one setting once, but enacting multiple settings over time.
   b. Second priority: ease of implementation for companies. For systems that are equally usable for citizens, favor choices that reduce the burden on companies. Please note I do not propose this as a balancing test: designing a button to enact privacy

[3] "State of IPv6 Deployment 2018," *Internet Society* (June 6, 2018.) Available from <https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/>

[4] 1798.185(a)(4)(A) reads: ("…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…")

CCPA_2ND15DAY_00225

preferences is the goal and the statutorily required task at hand. It is often the case that ease of use is directly opposed to ease of adoption. That said, reducing barriers to implementation is an important secondary goal, when possible.

2. Solicit proposals in writing, similar to this comment process.
3. Encourage working demonstrations with open-source code and graphics. This allows groups to test what others submit as well as their own designs, for those who have the resources to do so. Note that absent an open-source license, the AG's office could inadvertently grant a company an intellectual property monopoly. In a world where Amazon could patent "1-Click," this is a real concern. The Apache open source license is one of the more popular choices.
4. Be able to ask questions and give feedback. If the AG's office is unable to do so, simple issues get much more difficult to sort out.
5. Strive for transparency and a public process to the extent practical. This might suggest something similar to an *ex parte* filing approach, but since there are not clear opposing sides, an ideal system strives for public notice to all rather than depending upon an adversarial framework.
6. Allow for partial submissions. For example, one proposal might reflect expertise on button size, placement, or other UI elements. Another proposal might focus on how to minimize network traffic on a header signal. The OAG's role becomes stitching different proposals together, and then seeing if the final quilt is harmonious (likely with rounds of comments.)
7. Establish guidelines on how the AG's office will hire contractors for subtasks if necessary. For example, a proposal might have a very good idea but the citizen submitting it may not have the resources to fully develop it.

W339-2 cont.

Alternatives to a multi-stakeholder process are to either hire an external group to perform all of these functions, or to develop a system entirely within the AG's office, both of which would take considerable resources. The downside to the sort of multi-stakeholder approach I outline above is that it can be simply awful. Keeping participants largely isolated from one another is one way to retain sanity. Yet there are also times getting everyone in a room (or Zoom call) is a much faster way to make progress. If you can reserve the ability to hold workshops or meetings as needed, you may be able to accelerate the pace.

As a final thought, a temptation is to say "let the marketplace sort it out," and to effectively have a set of experiments run. I strongly advise against this approach. Please create a framework to pick a standard for use online. For one thing, if the market were able to sort it out, we would not have the extraordinarily unusual legislative history that lead to CCPA. For another, it is an utter mess for typical citizens to need to learn different conflicting controls.

Thank you for your time and efforts.

Message

From: James Koons [redacted]
Sent: 3/20/2020 12:09:37 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments Regarding the Proposed CCPA Changes
Attachments: CCPA Comments - DPS Advisors - 200320.pdf

Hello Lisa B. Kim,

In accordance with the "Notice of Second Set of Modifications to Text of Proposed Regulations" (OAL File No. 2019-1001-05), we would like to submit the attached comments regarding the text of the second set of modifications to the proposed regulations.

Please let me know if you have any questions.

Thank you,
James

James Koons | Founding Partner
Data Privacy & Security Advisors LLC
[redacted]
www.DPSAdvisorsLLC.com
Washington DC | Philadelphia | New York | London

Data Privacy & Security Advisors LLC

March 20, 2020

VIA E-MAIL (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: March 11 Revisions to the Proposed Regulations Implementing the California Consumer Privacy Act ("Regulations")

Dear Lisa B. Kim:

Data Privacy & Security Advisors is a small company specializing in advising organizations around the world on global data privacy and information security challenges. Since the introduction of the California Consumer Privacy Protection Act on January 3, 2018, our heavily experienced and industry certified Privacy Experts have been counseling clients on how to interpret and prepare for demonstrating compliance with the CCPA. The following comments are an aggregation of comments collected from clients. They do not reflect the position of all our clients, or of Data Privacy & Security Advisors. However, we believe the issues raised are of high importance to many of our clients and the suggestions made are within the authority of the Attorney General ("AG") to adopt. We respectively submit the following for your consideration:

Delay in the Enforcement of the CCPA

We hereby request the Attorney General exercise the AG's authority under Civil Code Section 1798.185(b) and the inherent prosecutorial discretion of the AG to extend the date upon which the Attorney General may commence an enforcement action under the CCPA until the date that is six (6) months from the date the Regulations are final. This will allow the business community enough time to recover from the ongoing COVID-19 pandemic, as well as time to update procedures and processes to align with the final Regulations. The AG has authority under CA Civil Code Section 1798.185(b) to issue Regulations that further the purposes of the CCPA. The AG also has inherent authority to delay or defer prosecution when doing so would serve the interests of justice. Allowing businesses enough time to implement the final Regulations, and to do so after they have addressed the initial impact of COVID-19, serve the purposes of the CCPA, the interests of justice and the public interest. Further, the legislature did not preclude the AG's authority when it mandated the first enforcement delay by adding subsection (c) to CA Civil Code Section 1798.185. That subsection does not provide that the AG must start enforcing the CCPA on the later of six months after publication of the final Regulations, or July 1, 2020. Rather it says the AG must not do so until such dates. Accordingly, legislative amendment to the CCPA is not required to extend the enforcement delay.

W340-1

Ongoing Revisions to Regulations have Created Uncertainty and Confusion

The various changes to the Regulations over the last few months have created an undue burden on businesses. Businesses have had to revise protocols to implement details that have changed from the first version of the draft regulations in October 2019, to the second version in February, and now the third version on March 11, 2020. It is unclear when the Regulations will be final and what further changes may be made. Some clients are understandably waiting for final Regulations before fully developing a comprehensive compliance program.

W340-2

For certain new obligations, businesses will not be able to adequately prepare and effectuate the requirements as most recently set forth, or that may be later promulgated. For example, mobile apps cannot be revised without submitting a new update to Google or Android for approval and the just-in-time requirements for mobile apps were just put forth in the second version of the revised regulations and the third version did not provide any further clarity as requested in the over 100 comments submitted to the AG.

Further, the third version of the regulations removed the "Do Not Sell" button and businesses are unclear whether this will come back in the final version and require additional technical implementation close to the current July 1, 2020 enforcement date. However, since Section 1798.185(4)(C) of the CCPA requires the Attorney General to establish rules and procedures *"[f]or the development and use of a recognizable and uniform opt- out logo or button by all businesses,"* it is likely the guidance on the opt out button will come back in, it just won't be provided until the next set of draft Regulations.

W340-2 cont.

Lastly, many vexing questions remain unanswered by the third draft of the regulations, and provide, for many unexpected and difficult to implement compliance obligations. It will take considerable time for companies to prepare to do what will be ultimately necessary to launch a fully compliant program.

As such, additional time is needed to effectuate the proposed regulations due to the numerous changes released in the past three versions that impact businesses compliance obligations.

COVID-19 State of Emergency

The need for more time to respond to the final Regulations will be exacerbated by understandable diversion of businesses' resources due to the national state of emergency resulting from the COVID-19 pandemic. Businesses need concentrate their focus and resources on addressing business continuity challenges and consumer and employee safety during the national health crisis that is ongoing throughout California and the U.S. Further, many businesses will suffer economic hardships and staff shortages that will make a rush to meet the current July 1, 2020 deadline impractical or even impossible. Finally, it is reasonable to expect the AG's CCPA rulemaking process may be delayed as a result of the shelter at home approach to combating community spread of the virus.

W340-1 cont.

Governor Gavin Newsom issued Executive Order N-25-20 on March 12, 2020 to protect public health and the California economy, which will have a significant impact on companies doing business in California. As a result, the Attorney General should issue the six-month extension in order to alleviate the impact on CCPA covered businesses and allow all efforts to be focused on combatting COVID-19 and addressing the needs of their consumers and employees.

With the unparalleled public health crisis of coronavirus mounting, California should allow businesses to focus on keeping operations running, and protecting the health of their consumers and staffs, without fear of CCPA compliance enforcement actions.

Thank you for your consideration of these comments.

Respectfully submitted,

Data Privacy & Security Advisors, LLC
www.dpsadvisorsllc.com

Message

From: Colin Smith [redacted]
Sent: 3/27/2020 4:31:34 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Derek Schwede [redacted]; Todd Smithline [redacted]
Subject: Comments to Further Revised CCPA Implementing Regulations
Attachments: Comments to Further Revised CCPA Regulations 2020 03 27.pdf

Dear Sir/Madam,

We respectfully submit these comments regarding the Attorney General's CCPA Implementing Regulations.

Very truly yours,

Derek Schwede, Smithline PC
Todd Smithline, Smithline PC

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, Suite 1000 San Francisco, California 94104
Phone: (415) 834-1700 Fax: (415) 834-1720
www.smithline.com

March 27, 2020

By email to privacyregulations@doj.ca.gov

Re: Comments to Further Revised CCPA Regulations

We write on behalf of a CCPA working group composed of California and national in-house and law firm attorneys. This is our third letter of comments. With a nod to current circumstances we are not circulating this letter for participant signatures, but based on our group discussions we believe these comments do generally reflect the consensus of our enterprise SaaS provider participants.

We again thank the Attorney General and staff for the opportunity to submit these comments, particularly at this time. We believe this process has generally led to more cogent and helpful regulations, but ask you to please consider these last two items that are of critical importance to members of our working group.

A. *Service Providers and Businesses Need Freedom to Define the "Services" (§999.314(c)(1))*

1. Issue. The new draft of §999.314(c)(1) moves this clause to center stage in describing how service providers may use personal information. Unfortunately, the revisions shift control of this critical question from businesses and service providers to a one-size-fits-all regulation, which fails to account for the range of services received by businesses, erodes freedom of contract and is contrary to the CCPA itself. This change could cause significant economic harm to California companies by prohibiting them from providing routine enterprise services that their peers in other regions remain free to offer, without any additional benefit to consumer privacy. We agree that service provider contracts must be CCPA-compliant and that businesses must provide notices and meet their other obligations to consumers – but so long as these requirements are met, the regulations should not artificially limit the services for which businesses may engage service providers.

> §999.314(c): A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except:
>
> ***Prior Language from February Draft:*** (1) To perform the services specified in the written contract with the business that provided the personal information;
>
> ***Proposed New Language in March Draft:*** (1) To process or maintain personal information on behalf of the business that provided the personal information, or that directed the service provider to collect the personal information, and in compliance with the written contract for services required by the CCPA;
>
> (emphases added)

W341-1

2. Wide Range of Services. As the February draft recognized, businesses rely on service providers for a wide range of services involving a variety of uses of personal information. The proposed change is confusing and constraining – limiting the service provider to *processing or maintaining* information on behalf of a single business while the lead-in broadly restricts *retention, use and disclosure* – and imposes unnecessary limits on industry-standard services.

   For example, from accounting platforms to business intelligence tools, most online services allow the business to *disclose* their data to others as an essential feature (e.g., sharing accounting data with tax software also used by the business). The proposed change casts doubt on these standard disclosures requested by businesses.

   Further, the limit "*on behalf of the business that provided the personal information*" raises serious concerns for service providers that provide technology platforms to business consortiums. These platforms allow businesses to share data with one another to solve industry-wide problems such as supply chain logistics, transit system issues and protection against malware and other common risks – activities which directly benefit consumers.

3. Freedom of Contract. Given the range of services that power California's economy, businesses and service providers are best positioned to define how service providers use data and require freedom of contract to do so. This flexibility is especially needed for sophisticated and rapidly evolving technology services. So long as the contracts are CCPA-compliant and businesses meet their consumer obligations, the regulations should respect private contract.

4. Exceeds Statute. The proposed change is also contrary to the statute itself. The "*business purposes*" in §1798.140(d) expressly include operational purposes of service providers such as debugging, account maintenance, analytics and order processing. The change appears to ignore or restrict these uses. The regulations must not deprive entities of rights expressly granted by the legislature. W341-1 cont.

5. Request. We believe that the February draft of §999.314(c)(1) struck the correct balance. We request that the Attorney General restore the prior language allowing a service provider to retain, use and disclose information to "perform the services" under its contract with the business. Alternatively, we propose modifying the new proposed language as follows:

> "A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except:
>
> (1) ~~To process or maintain personal information~~ on behalf of the business that provided the personal information, or that directed the service provider to collect the personal information, ~~and~~ or otherwise in compliance with the written contract for services required by the CCPA..."

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

1. Issue. We reiterate the objections from our February 25 letter regarding §999.314(d), which provides:

> "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."

A service provider's use and disclosure of personal information is governed by its agreement with the business. But as the party with direct consumer relationships, the *business* is responsible for ensuring that its instructions to the service provider comply with the CCPA, including honoring any opt-outs relevant to its use of the services. The proposed regulation mistakenly places this obligation on the service provider, which distorts the CCPA's core compliance framework for businesses and could pressure service providers to second-guess or even violate the data processing instructions they receive from businesses. It is also unnecessary given that the CCPA already expressly limits how service providers may use personal information received from businesses (§1798.140(v) of the statute; §999.314(c) of the proposed regulations). W341-2

2. Request. We respectfully request that the Attorney General delete §999.314(d). It is not necessary and places an unrealistic and problematic burden on service providers.

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

Very truly yours,

Derek Schwede

Derek Schwede
Principal
Smithline PC

Todd Smithline

Todd Smithline
Managing Principal
Smithline PC

Message

From: Rustici [redacted]
Sent: 3/27/2020 12:30:58 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Comments to the text of the second set of modifications of the CCPA Regulations

For the Attention of the Privacy Regulations Coordinator
California Office of The Attorney General

Dear Sir/ Madam

I note the most recent amendments to the CCPA Regulations and would politely submit that, overall, this second amended version of the text reinforces the perception that the CCPA Regulations reserve a high level of scrutiny to the business practice of outright sale of personal information but shield from regulatory scrutiny the business practice of disclosing or licensing or allowing controlled access to personal information in a commercial venture that is short of outright PI sale.

W342-1

More specifically, may I politely draw your attention to the following definitions:

1)
Page 2

Definition of "Financial Incentive" at Art. 1 § 999.301. (j)
As the text currently reads at page 2, in order for something to fall under the definition of financial incentive for the purposes of the CCPA Regulations, it must relate to personal information collection, retention or sale. It would appear that if anything relates to **disclosure** or **deletion** of personal information, it no longer falls under the definition of financial incentive for the purposes of the Regulations.

As a result, two key business models are - to my mind unjustifiably - exempted from the obligation to provide notice of financial incentive (Art. 2 § 999.304(d)) and the obligation to use and document a reasonable and good faith method for calculating the value of the consumer's data (Art.6 § 999.337 (a)) or any other CCPA obligation relating to financial incentives:
- (a) any business which monetizes personal information not through direct sale of it to 3rd parties but through controlled **disclosure**, such as licensing access to it, or licensing access to inferences derived from personal information would not have to declare a financial incentive nor document the value of consumers' data (for example instead of selling gyroscopic data of individuals' devices at a given point in time to advertisers, a business might licence a feed of easily drawn inferences from gyroscopic data from all the devices that are being held by someone in a horizontal position - thus allowing precision targeting of advertisements to people reading in bed or in a horizontal position);
- (b) any business which monetizes individuals' privacy by offering to **delete** personal information in its possession or in its control in return for a financial incentive would also be under no obligation to declare a financial incentive nor document the value of consumers' data.

As I do not believe this result was part of the legislative intent for the CCPA, I would politely submit that the definition of "financial incentive" not only reinstates "disclosure" and "deletion" but includes reference to "**any current or future business model which offers benefits to a business' customers in return for that business' freedom to handle personal information in ways that exceed those strictly required for the offering of a paid product or service**" or analogous phrasing to the same effect.

2)
Page 3

A similarly unjustifiable result would follow unless "disclosure" and "deletion" are reinstated in the definition of "Price or service difference" (Art.1 § 999.301.(o)) and reference is made to **any current or future business model which offers benefits to a business' customers in return for that business' freedom to handle personal information in ways that exceed those strictly required for the offering of a paid product or service.** W342-2

Unless this is amended, the paradoxical outcome would be one where the Act imposes on businesses an obligation to describe any "disclosure" and "deletion" of personal information in their "Privacy Policy" as per definition of privacy policy at Art. 1 §999.301. (p), but no obligation to indicate if such disclosures or deletions are the *quid pro quo* for price or service differences.

In the same vein, at Art. 1 §999.301 (q) (6) the revised text should include "selling **and disclosing**" and a reference to **any current or future business model which offers benefits to a business' customers in return for that business' freedom to handle personal information in ways that exceed those strictly required for the offering of a paid product or service**. W342-3

Also, Art.1 §999.301 (s) currently reads: "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)." W342-4
May I politely submit that it should read instead: "Request to opt-out" means a consumer request that a business **neither sells, nor discloses** to third parties **nor in other way benefits commercially from sharing with third parties** the consumer's personal information **in ways that exceed those strictly required for the offering of a paid product or service**".

Lastly, Art.1 §999.301 (t) currently reads:
"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."
May I politely submit that it should read instead: W342-5
"Request to opt-in" means the affirmative authorization that the business may sell **or disclose or in other way benefit commercially from sharing with third parties** personal information about the consumer **in ways that exceed those strictly required for the offering of a paid product or service** 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 **or of the disclosure** of their personal information.

3) **Page 4**

While it is certainly true that legal definitions of what constitutes "personal information" are inherently imperfect and often of little practical help to businesses when discriminating between personal and non-personal information, the CCPA Regulations should not abdicate their duty to direct businesses and consumers to a core notion of personal information that is commonly understood, while allowing doctrine and scholarship to perfect the notion in lockstep with technological progress. W342-6

I politely submit that Art.1 §999.302 (a) should be reinstated and a definition reads: "**Personal information is information that describes, characterizes, singles out or relates to living individuals as both state of the art technology and common natural language allow**".

4) **Page 7**

Art. 2 §999.305 (d) currently reads: "A business that does not collect personal information directly from a consumer does not need to provide a notice at collection to the consumer if it does not sell the consumer's personal information".
For the same set of reasons given above, I politely submit that it should read instead: "A business that does not collect personal information directly from a consumer does not need to provide a notice at collection to the consumer if it **neither sells, nor discloses nor in other way benefits commercially from** the consumer's personal information" W342-7

May I conclude by stating none of the comments made above detract in any way from the admiration for the Office of the Attorney General of the State of California in its determination to meet the intended deadline for these Regulations despite the current hard working conditions.

With kindest regards,
Dott. Chiara Rustici
Independent EU privacy, GDPR and data regulation analyst

Sent with ProtonMail Secure Email.

Message

From: Jones, Erik [redacted]
Sent: 3/27/2020 3:04:48 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CompTIA Comment - Second Set of Modifications to CCPA Implementing Regulations
Attachments: CCPA Second Modified Regulations - CompTIA Comment.pdf

Please find attached CompTIA's comments on the Second Set of Modifications to the CCPA Implementing Regulations. Please let me know if you have any questions or issues accessing the document.

Sincerely, Erik Jones

Before the
CALIFORNIA DEPARTMENT OF JUSTICE
Los Angeles, CA 90013

In the Matter of	)	
	)	
Second Set of Modifications to	)	OAL File No. 2019-1001-05
the 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
515 2nd Street NE
Washington, DC 20002

March 27, 2020

CCPA_2ND15DAY_00237

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 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 second set of modifications to the regulations. CompTIA appreciates the changes the Department made related to the opt-out button graphic that had been proposed in § 999.306(f) and the indirect collection exception in § 999.305(d). While 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]

W343-1

[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.

CCPA_2ND15DAY_00238

DISCUSSION

I. § 999.302. The Guidance Regarding the Interpretation of CCPA Definitions Should Be Reinstated.

The language and guidance regarding the interpretation of CCPA definitions in § 999.302 of the first set of modifications to the regulations should be reinstated. CompTIA supported this guidance, as it provided businesses with important clarifications about what is considered personal information under the regulations. Information deemed as "personal information" under the regulations should depend on whether the business maintains the 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." As such, CompTIA strongly supports reinstating this language. W343-2

II. § 999.307. The Value of Consumer Data Disclosure Requirements Should Be Deleted.

We reiterate our request to delete the value of consumer data disclosure requirements. 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." W343-3

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~~."

W343-3 cont.

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.

We also recommend revising the updated definition of "financial incentive," which appears broader than the statute.

W343-4

Definition of Financial Incentive(j) Financial incentive means a program, benefit, or other offering, including payments to consumers, ~~related to~~ as compensation for the collection~~, retention~~, deletion or sale of personal information.

III. 999.308(c)(1)(e). The Requirement to Identify the Categories of Sources Should be Clarified.

W343-5

The additional language in section 999.308(c)(1)(e) could be read to imply that businesses need to describe the data collected from sources, and that reading is counter to the purpose of the addition. Accordingly, we recommend the following edits:

999.308(c)(1)(e) Identify the categories of sources from which the personal information is collected. The categories shall be described in a manner that provides consumers a meaningful understanding of the sources from which the information is ~~being~~ collected.

W343-5 cont.

IV. § 999.313. Businesses Should Not Be Required to Provide Substantially Similar or Duplicative Information to Consumers in Response to Their Requests to Know.

The Department should specify that businesses need not provide substantially similar or duplicative information to consumers in response to their requests to know. Providing consumers with substantially similar or duplicative data would be disproportionately burdensome on businesses and not useful for consumers. In responding to a consumer's request to know what personal information a business has collected, the business should need only to produce a single data point, and not multiple data points, to provide a consumer with a meaningful understanding of the category of personal information it has collected. Accordingly, we recommend the following addition:

W343-6

> 999.313 (c)(12) In responding to a verified request to know categories of personal information, a business shall not be required to produce substantially similar or duplicative specific pieces of personal information.

V. § 999.313(c)(3). The Security Risk Exception Should Be Reinstated.

As we requested in our comments on the first set of modifications, we reiterate our 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. Businesses should not be forced to choose between compliance and security. Accordingly, we request that this language be restored:

W343-7

> 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.

VI. § 999.313(c)(3). Subsection (c)(3) is Overly Restrictive and Does Not Sufficiently Address Privacy and Security Concerns.

CompTIA reiterates the request related to § 999.313(c)(3) in its comment on the first set of modified regulations. 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. The second set of modified regulations still require 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. W343-8

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. This is particularly true with data that the business has derived rather than collected. 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:

> A business shall not provide a consumer with specific pieces of personal information if the disclosure would: (1) create a substantial, articulable, and unreasonable risk to the privacy or security of that personal information, the

consumer's account with the business, or the security of the business's systems, networks, or consumers; (2) interfere with law enforcement, judicial proceedings, investigations, or efforts to guard against, detect, or investigate malicious or unlawful activity or enforce contracts; (3) disclose the covered entity's trade secrets or proprietary information; (4) would require the covered entity to re-identify or otherwise link information that is not maintained in a manner that would be considered personal information; or (5) violate federal, state, or local laws, including rights and freedoms under the United States Constitution.

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 information it collects:

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; or

c. The business does not sell the personal information and does not use it for any commercial purpose.

W343-8 cont.

VII. § 999.314. The Regulations Should Allow Service Providers to Process Personal Information for all Business Purposes Permitted Under the Statute and Should Provide Guidance on How to Use Personal Information for Data Security and Fraud Detection.

We request that the Department clarify that the regulations allow service providers to process personal information for any "business purpose," as that term is defined in the statute. Specifically, the regulations should make it clear that a service provider may use personal information for any "operational purposes" enumerated in Section 1798.140(d) of the statute without introducing non-statutory restrictions on service providers. Permitting service providers to use personal information for their own operational purposes is not only required by a plain reading of the statutory text, it is sound policy. To perform the contracted-for services on behalf of the business, service providers often *must* process personal information received from multiple businesses internally.

W343-9

The Attorney General should reinstate the deleted language in (c)(1) to clearly permit a service provider to use personal information for any permitted business purpose pursuant to the

written agreement between the business and the service provider. To clarify that the Department's regulations are meant to be consistent, and not in conflict, with the statute, we request that the Department further modify the draft regulations by adding the underlined language:

W343-9 cont.

W343-10

> 999.314 (c): A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except to the extent permitted by the statute, including

VIII. § 999.315(d)(1). The Privacy Controls Should Require the Consumer to Affirmatively Select Their Choice to Opt-Out.

The second set of modified regulations deleted the sentence that states that a pre-selected setting is not permitted. Removal of that sentence entirely is problematic. While the prior version of the provision and sentence was confusing, at a minimum, the first clause – "The privacy control shall require that the consumer affirmatively select their choice to opt-out" – must be reinstated. Without it, there is a risk that consumers will inadvertently make a selection to opt-out of sale without having had an opportunity to actually make that selection.

W343-11

Additionally, the proposed changes to (d)(1) contravene the statute by removing a consumer's right to opt-out and giving browser publishers significant power over consumer choice, thereby circumventing that choice. The statute contemplates consumers directing specific businesses not to sell data, and not having web browsers direct all businesses through a single opt out. The draft mandate of honoring user-enabled global privacy controls would have the likely effect of allowing browsers to subvert consumer choice. Accordingly, we recommend the following edit:

W343-12

> **§ 999.315 (d)** 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 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.

W343-12 cont.

IX. § 999.317(g). The Recordkeeping Requirements Should Be Deleted

As we requested in our prior comments, the reporting and recordkeeping requirement presented in §999.317(g) should be deleted. The requirement 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 CCPA, for various reasons, could be very different for different organizations. These differences could be based upon very legitimate reasons. However, the differences in these numbers could be misleading to consumers and needlessly cause reputational damages to businesses.

W343-13

X. § 999.319. Intellectual Property and Trade Secrets Should be Protected

The Department should issue a new regulation to protect businesses' intellectual property rights when complying with Sections 1798.110 to 1798.135. The CCPA requires the Attorney General to promulgate a regulation including "Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights…" 1798.185(a)(3). The Department has not yet issued draft regulations related to trade secrets and intellectual property rights.

W343-14

We request that – to comply with its obligations under the CCPA – the Department should issue a regulation establishing an exception to the requirements of the CCPA to protect against violations of intellectual property rights and the disclosure of trade secrets. Accordingly, we recommend the addition of the following provision:

999.319. Intellectual Property and Trade Secrets. The obligations imposed on businesses by Sections 1798.110 to 1798.135, inclusive, shall not apply where compliance with the title would violate the business's intellectual property rights or result in the disclosure of trade secrets.

W343-14 cont.

CONCLUSION

CompTIA and our member companies take consumer privacy issues very seriously. We believe that well-crafted privacy protections can 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, 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.

Message

From: Maureen Mahoney [redacted]
Sent: 3/26/2020 2:33:04 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CR comments on the second set of modifications to the proposed CCPA rules
Attachments: CR CCPA Comments 3.26.20 FINAL.pdf

Dear Ms. Kim,

Attached, please see Consumer Reports' comments on the second set of modifications to the proposed rules to implement the CCPA. Please let me know if you have any questions.

Best,
Maureen

--
Maureen Mahoney
Policy Analyst
o [redacted]
CR.org



PLEASE NOTE: My email address has changed. Please begin using [redacted] for all future correspondence.

***
This e-mail message is intended only for the designated recipient(s) named above. The information contained in this e-mail and any attachments may be confidential or legally privileged. If you are not the intended recipient, you may not review, retain, copy, redistribute or use this e-mail or any attachment for any purpose, or disclose all or any part of its contents. If you have received this e-mail in error, please immediately notify the sender by reply e-mail and permanently delete this e-mail and any attachments from your computer system.
***

March 26, 2020

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

Re: Second Set of Modifications to Proposed Regulations 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 second set of modifications to the proposed rules implementing the California Consumer Privacy Act (CCPA).[2] As consumers shift to working from home and spending even more of their time online in light of the COVID-19 crisis, now more than ever, they need baseline protections to protect their privacy and security. We appreciate that the AG has improved upon the previous draft rules, particularly by eliminating the exemption for IP addresses from the definition of personal information.[3] But other steps, such as a new provision that could allow service providers to build profiles to deliver targeted advertising, undermine existing protections.[4] We reiterate the requests from our previous comments, particularly to close targeted advertising loopholes by strengthening the definitions of sale and service provider, and to further limit pay-for-privacy;[5] and additionally call on the AG to: W344-1

- Deny the request from industry to delay enforcement of the CCPA;
- Maintain a strong, inclusive definition of personal information;

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.
[2] California Attorney General, California Consumer Privacy Act Regulations, Text of Modified Regulations (Feb. 25, 2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-redline-020720.pdf.
[3] § 999.302(a).
[4] § 999.314(c)(3).
[5] See, Consumer Reports Comments on Modified Proposed Rules Implementing the California Consumer Privacy Act (CCPA) (Feb. 25, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/02/CR-CCPA-Comments-2.25.20-FINAL.pdf.

- Ensure that Do Not Track signals are honored as opt-out requests;
- Tighten up service provider language; and
- Set up an appeals process for responses to access requests.

Companies are seeking to evade the letter and the spirit of the CCPA, and to avoid any punishment for doing so. By sending a clear message that companies need to respect the CCPA, the AG can better protect consumers' constitutional right to privacy.

The AG should deny the request from industry to delay enforcement of the CCPA.

The AG should reject the cynical attempt by many industry groups to use the recent coronavirus crisis to evade their responsibilities under the law. Dozens of companies and industry trade groups requested that the AG delay enforcement of the CCPA to January 2021.[6] This latest effort to avoid compliance with the CCPA comes as more and more consumers work from home, increasingly relying on online communications to work, stay in communication with healthcare professionals, and obtain access to necessary supplies. It is critical for policymakers to ensure fairness, safety, and transparency for consumers in the marketplace. Industry shouldn't exploit the health crisis to ignore consumer requests to companies to stop selling their data. W344-2

This most recent letter is just the latest in a series of attempts to evade the CCPA. Last year, industry supported a raft of bills to gut the CCPA. Thanks to the efforts of several legislators, the worst bills failed to advance. Lawmakers also held the line against a last-minute wave of lobbying from industry groups such as the California Chamber of Commerce and the Internet Association, which sought to introduce amendments to exempt additional consumer information from the law.[7] Though the CCPA went into effect in January, many companies have avoided complying with the law.[8] In late January, advertising groups also called on the AG to delay the effective date of the CCPA until January 2021.[9]

---

[6] Association of National Advertisers et al, Request for Temporary Forbearance from CCPA Enforcement (March 17, 2020), https://www.law360.com/articles/1255181/attachments/0.

[7] Consumer Reports et al., *Joint news release: Privacy groups praise CA legislators for upholding privacy law against industry pressure* (Sept. 13, 2019), https://advocacy.consumerreports.org/press_release/joint-news-release-privacy-groups-praise-ca-legislators-for-upholding-privacy-law-against-industry-pressure/.

[8] 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.

[9] 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.

Companies making a good faith effort to comply with the CCPA have nothing to fear. Compliance should be fairly straightforward—access, deletion, and opt-out of sale. Companies that don't collect and retain unnecessary data, and those that don't sell consumers' data, should have very little difficulty in complying. Unfortunately, even those not making a good faith effort may find themselves off the hook, due to weak enforcement provisions in the CCPA. The AG enforcement section includes a "right to cure" provision that ties the AG's hands from taking action if the company "cures" the violation in 30 days,[10] meaning that the AG can spend months building a case against a company that is flagrantly violating the law, only to find that it goes nowhere. Further, once a consumer's privacy has been violated by unauthorized disclosure of information, there's no way to cure the damage. On top of that, the California Attorney General has limited resources to protect the privacy of 40 million Californians; earlier, the AG's office noted that they only have the enforcement capabilities to bring a few cases per year.[11]

Consumers shouldn't lose their right to privacy in a crisis. As tech companies work to create new solutions to address the scarcity of health services, consumers need baseline protections for that data more than ever. For example, a Google subsidiary, Verily, has launched a new service in two counties in California to help consumers determine whether or not coronavirus testing is appropriate.[12] While they're offering a good service, there should be some reasonable limits on what they do with the data, as consumers are very vulnerable at this time.[13]

W344-2 cont.

Consumers working from home need protections too. Well before this most recent crisis, about 43% of Americans spent at least some time working from home.[14] Now, many more have joined them, and are relying on their internet service providers, Google platforms, and teleconferencing services to work, communicate with co-workers, and order office, medical, and sanitizing supplies. In fact, due to these societal shifts, tech companies are expected to profit financially from this crisis.[15] In light of the recent health crisis, Consumer Reports recently examined teleconferencing service Zoom's privacy policies, and found that, while Zoom isn't necessarily doing anything objectionable with consumer data, its privacy policy gives the company a lot of leeway to share details about the calls, including instant messages and the names of participants,

---

[10] Cal. Civ. Code §1798.155(b).
[11] Yuri Nagano, *California Attorney General Plans Few Privacy Law Enforcement Actions, Telling Consumers to Take Violators to Court*, SAN FRANCISCO PUBLIC PRESS (May 15, 2019), https://sfpublicpress.org/news/2019-05/california-attorney-general-plans-few-privacy-law-enforcements-telling-consumers-to-tak.
[12] Julia Carrie Wong, *Google's Coronavirus Testing Website Arrives – With Serious Privacy Concerns*, THE GUARDIAN (Mar. 16, 2020), https://www.theguardian.com/us-news/2020/mar/16/coronavirus-testing-website-trump-promised-verily.
[13] Katie McInnis, *Privacy Concerns Raised by Verily's Baseline COVID-19 Pilot Program*, CONSUMER REPORTS, (Mar. 23, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/03/Consumer-Reports-letter-to-Verily-Alphabet-3.23.20.pdf.
[14] Niraj Chokshi, *Out of the Office: More People Are Working Remotely, Survey Finds*, N.Y. TIMES (Feb. 15, 2017), https://www.nytimes.com/2017/02/15/us/remote-workers-work-from-home.html.
[15] Daisuke Wakabayashi et al., *Big Tech Could Emerge From Coronavirus Crisis Stronger Than Ever*, N.Y. TIMES (Mar. 23, 2020), https://www.nytimes.com/2020/03/23/technology/coronavirus-facebook-amazon-youtube.html.

with third parties, even for advertising.[16] Consumers are transmitting sensitive information through these channels, and without the CCPA, they have next to no protection over the sale of that data. The AG should reject industry's request to throw out basic consumer protections in response to the crisis.

W344-2 cont.

The AG should maintain a strong, inclusive definition of personal information.

We thank the AG for deleting the provision in the first revised proposed rules, § 999.302(a), that would have removed 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.[17] Consumers should retain opt-out rights in this case. IP addresses are explicitly included in the CCPA's definition of personal information,[18] and to remove them would clearly subvert legislative intent. Deleting this provision properly closed up a potential new loophole for targeted advertising. We urge you to not reinsert the provision or weaken the definition of personal information in any way.

W344-3

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 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.[19] 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.[20] 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.

---

[16] Allen St. John, *Zoom Calls Aren't as Private as You May Think. Here's What You Should Know*, CONSUMER REPORTS (Mar. 24, 2020), https://www.consumerreports.org/telecommunications/zoom-teleconferencing-privacy-concerns/.

[17] Cal. Civ. Code §1798.140(o)(1)(A).

[18] *Id.*

[19] 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.

[20] *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.

The AG should ensure that Do Not Track signals are honored as opt-out requests.

We appreciate that the AG has kept the requirement that companies must honor browser privacy signals as an opt-out of sale.[21] 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.

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 to clearly convey that it constitutes an opt-out of sale.[22] 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.[23] Consumers would reasonably expect that enabling Do Not Track would opt them out of sale to third parties. 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.[24] Currently, major web browsers do not have comparable CCPA-specific settings, and we are unaware of any concrete plans to offer them in the near future. If companies can ignore DNT and similar requests, consumers may have no scalable way to opt out of data sales across the hundreds of sites and apps with which they interact. W344-4

Do Not Track was developed in response to consumer outcry over the fact that cookies enabled companies to track consumers' behavior across the web.[25] While it makes sense that a company would be able to view a consumers' activity on its own site, consumers would not reasonably expect that a company could also see what they were doing on other sites as they searched the Internet. It is precisely this type of transfer of data between first parties and third parties over which the CCPA attempts to give consumers control. It is a reasonable assumption that a consumer signing up for DNT would be opting out of sale to third parties.

---

[21] § 999.315(d).
[22] § 999.315(d)(1).
[23] Glenn Fleishman, *How the Tragic Death of Do Not Track Ruined the Web for Everyone*, FAST COMPANY (Mar. 17, 2019), https://www.fastcompany.com/90308068/how-the-tragic-death-of-do-not-track-ruined-the-web-for-everyone. 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.
[24] 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.
[25] Electronic Frontier Foundation, Do Not Track (last visited Mar. 23, 2020), https://www.eff.org/issues/do-not-track.

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 reiterate our request that 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.

W344-4 cont.

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 recently improved that tool to further limit the information advertisers can receive when the setting is activated.[26] 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.

The AG should tighten up guardrails on use of data by service providers.

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. We appreciate that the AG has kept the proposed § 999.314(d), which provides 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." Nevertheless, the language should be tightened further, especially since many companies incorrectly claim that the data-sharing engaged in for targeted advertising purposes is not a sale.[27] We reiterate our calls for a new .314(d):

W344-5

> 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

[26] 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.
[27] 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/.

than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

W344-5 cont.

The AG should also delete the new proposed language in § 999.314(c)(3), which explicitly allows service providers to build profiles for its own purposes. Given that many companies are already exploiting vagueness in the CCPA to claim a service provider exemption to deliver targeted advertising outside of the consumer opt-out, this new language could significantly undermine the CCPA by allowing service providers to use browsing, geolocation, dating app activity, and health data to derive detailed insights into consumers' lives and to better target ads on their own and potentially others' sites. Service providers shouldn't have the right to create profiles with its customers' data for its own unrelated purposes. Unless this language is tightened, companies could interpret this language as carte blanche to deliver targeted advertising in spite of an opt-out.

W344-6

The AG should set up an appeals process for access requests.

Companies have an unfair advantage in deciding whether or not to honor access requests, because it's not always easy for consumers to tell whether or not the company has fully complied. Especially in light of the many confusing exemptions, it's difficult for a consumer to know whether a company has released all of the covered information it has collected about them—or whether their exemption claim is legitimate. For example, at least one company, Airbnb, has claimed a trade secret exemption for not releasing consumer data. To address this, the AG should set up a process for appealing access decisions.

Consumers may suspect that a company hasn't been fully forthcoming—for example, the *Washington Post* noted that Uber only released the data involved in some of their interactions with the company:

W344-7

> [R]equests under the new law reveal huge variance in the data the companies disclose. Uber reveals a customer's rating, but doesn't disclose some customer service calls, users' ratings of drivers or any inferences about its users that help shape its business decisions. The company also maintains other data undisclosed in CCPA requests, according to people familiar with the matter, such as whether a credit card is corporate or personal.[28]

Employees of Consumer Reports have also run into problems in attempting to access their data. When a journalist at Consumer Reports recently sought to access their personal information from Airbnb, the company claimed an exemption based on intellectual property grounds:

[28] Greg Bensinger, *So Far, Under California's New Privacy Law, Firms are Disclosing Too Little Data — Or Far Too Much*, WASH. POST (Jan. 21, 2020), https://www.washingtonpost.com/technology/2020/01/21/ccpa-transparency/.

Airbnb takes its responsibilities for privacy and data protection very seriously. For example, so as not to adversely affect the rights and freedoms of others, we have not included some information where the inclusion would adversely affect intellectual property or other rights, or the data protection rights of third parties.

Trade secrets have the potential to be a significant exemption, since a company could potentially try to exempt any information that they've submitted to processing on intellectual property grounds. The CCPA itself does not provide a trade secret exemption but instead directs the AG to develop rules.[29]

W344-7 cont.

In addition, Epsilon couldn't provide the requestor with information because it could not verify their name and address. While companies shouldn't release information if they can't verify the consumer's identity, there should be a process by which any errors or issues can be resolved, so that customers can access their data.

THERE WAS A PROBLEM

Thank you for contacting Epsilon. We can't verify the name and address submitted, so your request can't be completed. Please click the "Make another request" button below to resubmit your name and address.

Make another request

Additionally, the requestor was surprised to find that Gap could not locate any of their data, because they were a regular customer. Even though the requestor had shopped with Gap multiple times, Gap reported that:

We were unable to locate any data associated with the email address that you provided. If you would like to submit another request with an alternate email address, then please use the link below.

Similarly, Comcast shared only a small amount of information. Even for such categories as "Service Activity Information" and "Account Information," the response was: "No data found for this category."

As a result, the AG should require companies to establish an appeals process for consumers who have not received information that may be covered under the law. Companies should be required not only to perform a meaningful investigation, free of charge, and either provide the requested information or a thorough response to the consumer, similar to the process for reinvestigation under the Fair Credit Reporting Act,[30] but to also file their response with the Attorney General. Companies should also be required to forward any complaints about a company's failure to comply with the CCPA to the AG to aid in regulation and enforcement.

[29] Cal. Civ. Code § 1798.185(a)(3).
[30] 15 U.S.C § 1681(i).

Conclusion

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

Message

From: Lindsay Gullahorn [redacted]
Sent: 3/27/2020 2:52:11 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Rachel Michelin [redacted]; CA - Margaret Gladstein [redacted]
Subject: CRA Comment Letter - CCPA Regulations (2nd Set of Modifications)
Attachments: CCPA Regs v3 CRA Comment Letter 032620.pdf; PastedGraphic-1.tiff

Please see the attached comment letter from our client, the California Retailers Association, regarding the second set of modifications to the CCPA draft regulations.

Thank you.

Lindsay Gullahorn
Capitol Advocacy
1301 I Street
Sacramento, CA 95814
[redacted] direct
916-444-0400 main
[redacted]

March 26, 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: **California Consumer Privacy Act Regulations – Second Set of Modifications to Proposed Text**

Dear Ms. Kim,

On behalf of the California Retailers Association, I am writing to register comments on the second set of modifications to the proposed California Consumer Privacy Act (CCPA) regulations. We have a number of concerns with the draft regulations but would like to highlight two major concerns that, if not addressed, will negatively impact our members.

The California Retailers Association is the only statewide trade association representing all segments of the retail industry including general merchandise, department stores, mass merchandisers, fast food restaurants, convenience stores, supermarkets and grocery stores, chain drug, and specialty retail such as auto, vision, jewelry, hardware and home stores. CRA works on behalf of California's retail industry, which currently operates over 164,200 stores with sales in excess of $571 billion annually and employing 2,776,000 people—nearly one fifth of California's total employment.

We appreciate your ongoing efforts to make the CCPA regulations workable for all affected parties and believe the second set of modifications has made important steps in this direction. However, we respectfully ask that you further amend the draft regulations to address the following key items of concern to the retail community:

Clarify Definition of "Financial Incentive"
The amended definition of "financial incentive" in the second set of modifications reads: *"'Financial incentive' means a program, benefit, or other offering, including payments to consumers, related to the collection, retention, or sale of personal information."* This revised definition can be interpreted to be broader than the description of "financial incentives" in Section 1798.125 of the Civil Code. To avoid confusion and remain consistent with statute, we urge you to remove "related to" in the definition of "financial incentive." W345-1

Do Not Sell Signal
The second set of modifications deletes the following sentence from Section 999.315(d)(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.*" The first part of this sentence, regarding a consumer affirmatively making a selection, is consistent with the underlying principles of the CCPA - consumer choice. To ensure that it is clear that an affirmative act is required by the consumer, this verbiage should be restored. Further, this is important guidance for companies trying to comply with the CCPA. Without it, it is not possible for businesses to determine whether a consumer is just receiving a default signal or whether that consumer intended to opt out of sale. W345-2

Conversely, we agree that the second portion of the deleted sentence ("…and shall not be designed with any pre-selected settings") should remain deleted. It conflicts with the first part of the sentence, which emphasizes consumer choice. Removing this phrase with also prevent competing browser providers from

opting consumers out of their competitors' services. For these reasons, we urge you to restore language allowing businesses who are complying with the Do Not Sell signal to present consumers who have reasons to accept sale the option to do so. W345-2 cont.

Thank you for the opportunity to provide feedback on the second set of modifications to the draft CCPA regulations. Please do not hesitate to contact me at [redacted] or [redacted] if you have any questions.

Sincerely,



Rachel Michelin
President

Message

From: Melanie Tiano [redacted]
Sent: 3/27/2020 2:25:42 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CTIA Comment on 2nd Set of Modifications to Text of Proposed Regulations
Attachments: CTIA - Comment on March 11 CCPA Modified Regulations 3.27.20.pdf

To Whom It May Concern:

Attached are CTIA's comments in response to the 2nd Set of Modifications to Text of Proposed Regulations.

Please let us know if you have any questions.

Thank you,

Melanie Tiano

Melanie K. Tiano
Director, Cybersecurity and Privacy
1400 16th Street, NW
Washington, DC 20036
[redacted] (office)
[redacted] (mobile)
[redacted]

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

March 27, 2020

TABLE OF CONTENTS

INTRODUCTION 1

I. § 999.302 – Guidance Regarding the Interpretation of CCPA Definitions 2

II. § 999.313 – Responding to Requests to Know and Requests to Delete 3

a. The Removal of the Security Risk Exception in 919.313(c)(3) Endangers Consumers 3

b. The "Legal or Compliance Purposes" Condition Prevents § 999.313(c)(3) from Providing Meaningful Relief to Businesses While Still Protecting Consumers 4

c. The New "Sufficient Particularity" Requirement in § 999.313(c)(4) Unduly Burdens Businesses and Provides No Additional Consumer Benefits 6

III. § 999.314 – Service Providers 8

IV. § 999.315 – Requests to Opt-Out 8

V. § 999.326 – Authorized Agent 9

CONCLUSION 11

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 appreciates the opportunity to provide these comments on the California Attorney General's Second Set of 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 and February 25, 2020.[2] CTIA understands the demanding statutory deadlines governing this process – particularly in light of the ongoing Covid-19 pandemic – and appreciates the Attorney General's efforts to move towards issuing final regulations.

Nevertheless, CTIA remains concerned that many of the provisions included in the modified regulations remain: (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. To the extent the issues raised in CTIA's December 6 and February 25 comments remain unaddressed, CTIA renews those concerns.

---

[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 and February 25, 2019 (respectively, "CTIA's December 6" and "CTIA's February 25" comments).

CCPA_2ND15DAY_00263

Additionally, as the Attorney General continues to finalize the regulations, CTIA asks that you consider the burdens imposed on business by instituting new, structural compliance obligations so close to the July 1, 2020 enforcement date -- particularly the practical challenges facing businesses forced to try to implement these changes on an unrealistically short timeframe. As such, CTIA requests that the Attorney General delay the effective date of CCPA enforcement. W346-1

CTIA's most urgent concerns pertain to the following sections of the modified regulations:

- § 999.302 – Notice of Right to Opt-Out of Sale of Personal Information
- § 999.313 – Responding to Requests to Know and Requests to Delete
- § 999.314 – Service Providers
- § 999.315 – Requests to Opt-Out
- § 999.326 – Authorized Agents

Where appropriate, CTIA provides alternative regulatory language to address the issues identified herein.

I. § 999.302 – Guidance Regarding the Interpretation of CCPA Definitions

§ 999.302 Provides Helpful Guidance and Should Be Retained

As previously formulated, subdivision § 999.302 provided useful guidance about the types of information that constitute "personal information" under the CCPA. The Attorney General's proposed removal of this guidance operates against the development of a uniform compliance regime. W346-2

Specifically, section 1798.140(o)(1) of the CCPA states that "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."[3] However, that same provision also states that "Personal information includes, but is not limited to, the following [enumerated data types] ***if*** it identifies, relates to, describes, is reasonably capable of

[3] Cal. Civ. Code §1798.140(o)(1).

being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household."[4] Thus, the CCPA expressly contemplates that the types of data included in Cal. Civ. Code §1798.140(o)(1) may not constitute personal information in instances where that data fails to meet the above standard.

The Attorney General's inclusion of subdivision § 999.302 in the February 10 iteration of the modified regulations helpfully illustrated that data constitutes "personal information" only when a 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." W346-2 cont.

For this reason, CTIA asks that the Attorney General reinstate proposed subdivision § 999.302 in its entirety:

> **§ 999.302.** *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. § 999.313 – Responding to Requests to Know and Requests to Delete

a. The Removal of the Security Risk Exception in 919.313(c)(3) Endangers Consumers

W346-3

CTIA renews its request that the Attorney General reinstate former subdivision § 999.313(c)(3) which prohibited businesses from responding to requests for specific pieces of personal information when doing so posed an unreasonable risk to consumers. While a stringent

[4] Cal. Civ. Code §1798.140(o)(1) (emphasis added).

standard to meet, this provision acted as a final stopgap to protect consumers' privacy and generally served to limit the unforeseen consequences of the new CCPA regime.

As we pointed out previously, the lack of U.S. precedent for comprehensive privacy legislation like the CCPA, means that 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. 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, the Regulations should support efforts by businesses to respond proactively to changes in technology and criminal tactics, even when such changes are, as of now, wholly unforeseeable. W346-3 cont.

CTIA requests that the modified regulations continue to support businesses' efforts to protect consumers. Any concern that the prior iteration of this provision granted businesses too much leeway could be addressed by modifying the provision to require businesses to maintain a formalized record of their rationale for invoking this exception, rather than by eliminating it altogether.

For this reason, CTIA asks the Attorney General to include the following language in addition to (and not in lieu of) subdivision § 999.313(c)(3) as it is currently formulated:

> **§ 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. If a business does not provide specific pieces of information to consumers under this provision, the business shall document and maintain a written record of this determination for a span of 2 years.*

b. **The "Legal or Compliance Purposes" Condition Prevents § 999.313(c)(3) from Providing Meaningful Relief to Businesses While Still Protecting Consumers** W346-4

The current iteration of subdivision § 999.313(c)(3) creates an exception whereby businesses are not required to search for personal information in response to requests to know if each of the following four conditions are met:

W346-4 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; *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.

However, combined, conditions (a), (c), and (d) provide ample protection for consumers. The "legal or compliance purposes" condition in (b) should therefore be removed as it results in too narrow relief for businesses while simultaneously failing to offer additional benefits to consumers.

Specifically, it is unreasonably burdensome to require businesses that do not maintain personal information in a searchable or reasonably accessible format, do not sell such information, and provide appropriate consumer disclosures, to nevertheless engage in the costly and time-consuming exercise of searching through unstructured and archival databases simply because the information at issue is not maintained "solely for legal or compliance purposes." The mere fact that the information is stored for reasons other than legal or compliance purposes is irrelevant to the apparent purpose of subdivision § 999.313(c)(3) – relieving businesses from the obligation to search for inaccessible information which holds no value to consumers. Put another way, from a consumer perspective, there is no meaningful distinction between information "maintained for a legal or compliance purposes," and information maintained for other reasons.

Accordingly, CTIA renews its request for the Attorney General to revise the modified regulations 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*
> - *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."*

W346-4 cont.

c. **The New "Sufficient Particularity" Requirement in § 999.313(c)(4) Unduly Burdens Businesses and Provides No Additional Consumer Benefits**

W346-5

Subdivision § 999.313(c)(4) prohibits businesses from providing certain sensitive information including Social Security numbers, financial account numbers, medical identification numbers, account passwords, and unique biometric data, in response to requests to know under the CCPA.[5] However, the current iteration of the modified regulations introduces a new requirement that businesses "inform the consumer with sufficient particularity that it has collected the type of information." As an example, the modified regulations provide that a business that collects fingerprint scan data would not be required to disclose the actual fingerprint scan, but instead notify the consumer that it collects "unique biometric data including a fingerprint scan." This new requirement overly complicates the existing CCPA "category disclosure" framework and provides no additional benefits to consumers.

Specifically, the CCPA already requires businesses to respond to requests to know categories of collected information with a "reference to the enumerated category or categories . . .

[5] *See* Cal. Civ. Code §1798.100(d).

that most closely describes the personal information disclosed."[6] The new requirement in Subdivision § 999.313(c)(4) to describe sensitive types of data that cannot be shared with "sufficient particularity" runs contrary to the text of the CCPA by creating obligations beyond the scope of the statute. Furthermore, it needlessly complicates the disclosure framework established in Cal. Civ. Code § 1798.110(a)(2).

W346-5 cont.

Finally, many businesses have already dedicated immense resources and incurred significant costs developing their CCPA compliance programs. Adding a new requirement at this late date imposes additional burdens on businesses, and as noted above, offers no tangible benefits to consumers. For businesses that have already developed and implemented their CCPA compliance programs, this provision would necessitate costly reevaluation which cannot reasonably be accomplished prior to the scheduled enforcement date.

Accordingly, CTIA requests the Attorney General revise subdivision § 999.313(c)(3) as follows:

> **§ 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.* ~~*The business shall, however, inform the consumer with sufficient particularity that it has collected the type of information. For example, a business shall respond that it collects 'unique biometric data including a fingerprint scan' without disclosing the actual fingerprint scan data.*~~

[6] Cal. Civ. Code §1798.130(a)(3)(B).

III. § 999.314 – Service Providers

The Limitations on Service Providers in § 999.314(c) Conflicts with the CCPA

Subdivision § 999.314(c) prohibits service providers from retaining, using or disclosing personal information obtained in the course of providing services except for five enumerated purposes. However, in setting forth the concept of a service provider, the CCPA allows for broader uses of personal information.[7] By restricting service providers uses of personal information to those five exceptions enumerated in subdivision § 999.314(c), the modified regulations conflicts with the plain language of the statute. W346-6

IV. § 999.315 – Requests to Opt-Out

The Modifications to § 999.315(d)(1) Undermine Consumer Autonomy

For the reasons articulated in CTIA's February 25 comment, CTIA remains opposed to the global privacy control framework proposed in subdivision § 999.315(d). However, to the extent the Attorney General has already considered and declined to remove subdivision § 999.315(d)(1) in full, CTIA requests modifications to the provision for the reasons provided below. W346-7

In its former iteration, subdivision § 999.315(d)(1) reflected the principles of consumer autonomy that characterize the CCPA by explicitly requiring consumers to make an affirmative choice to opt-out before global privacy controls would become effective. The current version of the modified regulations removes this directive and instead permits operators of global privacy controls to implement default settings which may not reflect consumers' true choices. These unauthorized requests become especially problematic when a consumer has knowingly decided to

---

[7] *See* Cal. Civ. Code §1798.140(v)(allowing a service provider to retain, use or disclose personal information for the purpose of performing services specified in its contracts with businesses, 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***) (emphasis added).

opt-in to data sales (for instance, as part of a financial incentive program), only to have that decision undermined by a contradictory request from a global privacy control.

Additionally, in describing the right to opt-out, the CCPA states that consumers "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."[8] Thus, the right to opt-out is expressly tied to the notion of consumer direction. Allowing global privacy controls to exercise opt-out requests without the requisite consumer direction amounts to a fundamental and unauthorized expansion of the CCPA.

W346-7 cont.

For these reasons, CTIA asks the Attorney General to reinsert the following language into subdivision § 999.315(d)(1):

> **§ 999.315(d)(1).** *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.*

V. § 999.326 – Authorized Agent

The Authorized Agent Framework Creates an Unreasonable Risk of Fraud as Applied to the Power of Attorney Context

W346-8

As stated in CTIA's previous comment, the unauthorized agent framework creates an unreasonable risk of consumer fraud, particularly with respect to authorized agents who purport to hold consumers' powers of attorney. CTIA requests that the Attorney General clarify this process and implement greater safeguards to protect consumers.

Under subdivision § 999.326(b), the few existing safeguards intended to protect consumers during the authorized agent process may be disregarded if "the consumer has provided the authorized agent with power of attorney." The modified regulations allow businesses to take steps

[8] *See* Cal. Civ. Code§ 1798.120(a).

to verify the legitimacy of requests to know and requests to delete that come in through authorized agents, unless those authorized agents purport to possess a power of attorney. In those instances, businesses are not permitted to take the privacy protective measures outlined in subdivision § 999.326(a). This distinction creates a critical vulnerability.

CTIA is concerned that by hindering businesses from implementing simple, common-sense measures to verify all authorized agent requests, this provision creates incentives for fraudsters to create false power of attorney documents. Given the relative novelty of the CCPA's consumer request framework, it remains unclear how fraudsters might abuse CCPA requests for criminal purposes, including harassment, extortion, and identity theft. As such, CTIA urges that all authorized agent requests be subject to the same verification standards. W346-8 cont.

Moreover, it is illogical that businesses may deny opt-out requests made directly by consumers upon a "good faith, reasonable, and documented belief" that the request is fraudulent, but must comply with far more sensitive requests to know or delete from alleged authorized agents even where the evidence of fraud is identical. At the very least, requests to know and delete should be safeguarded with the same fraud protections afforded to requests to opt-out.

Accordingly, CTIA requests that subdivisions §§ 999.326(b) and 999.326(a) be amended as follows:

> **§ 999.326(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.*~~ *A business may deny a request from an authorized agent who fails to verify their identity directly with the business.*
>
> **§ 999.326(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.* ~~.~~ *or upon good-faith, reasonable, and documented belief that the authorized agent is attempting to fraudulently exercise a 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
(202) 736-3200

March 27, 2020

CCPA_2ND15DAY_00273

Message

From: Alex Propes [redacted]
Sent: 3/27/2020 3:02:18 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Interactive Advertising Bureau Comments on the Proposed Second Set of Modified CCPA Regulations
Attachments: IAB Comments on Second Set of Modifications to Proposed CCPA Regulations.pdf

Please find attached written comments by the Interactive Advertising Bureau in response to the proposed second set of modified CCPA regulations.

Kind regards,

Alex Propes
Vice President, Public Policy & International
Interactive Advertising Bureau
Office: 202-800-0770
Mobile: [redacted]

March 27, 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: Second Set of Modifications to California Consumer Privacy Act Proposed Regulations

The Interactive Advertising Bureau ("IAB") provides these comments on the second set of modifications to the proposed regulations issued by the California Attorney General ("AG") on March 11, 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 dated December 6, 2019 and February 25, 2020.[2] 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 advance it. IAB urges the AG to consider consumers' support for the ad-driven Internet model and asks the AG to update the modified rules in line with the suggestions in these comments so the regulations empower consumers by giving them increased choices and control over online data.

---

[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/.

[2] *See* IAB, *California Consumer Privacy Act Proposed Regulations*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-comments-45day-pt6.pdf at CCPA_45DAY_01296 - 01312; IAB, *California Consumer Privacy Act Proposed Modified Regulations*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-15-day-comments-022520.pdf at CCPA_15DAY_000179 – 000187.

IAB also asks the AG to consider postponing enforcement of the CCPA until January 2021. The draft regulations implementing the CCPA are still not final, leaving little to no time for businesses to implement the ultimate requirements before the CA AG may begin enforcing the law. In addition, the unique and extraordinary state of affairs brought on by the COVID-19 crisis has forced businesses to quickly adjust their priorities in order to appropriately address the needs of their employees and the world in this difficult time. Beginning to enforce the CCPA when the economic and public health situation is so dire and uncertain would harm rather than help consumers and the economy-at-large, and the AG should consider these unprecedented circumstances in developing its enforcement approach. W347-1

In the spirit of improving the CCPA's regulatory regime and providing privacy protections that benefit all Californians while enabling the business community to continue to support California's economy, IAB submits these comments. IAB below addresses specific provisions of the modified rules that should be updated or clarified to further consumer choice and privacy and enable business compliance with the law.

I. Commence Enforcement in January 2021 Instead of July 2020

The unfinalized nature of the draft regulations implementing the CCPA leaves minimal time for businesses to implement the rules' ultimate requirements prior to July 1, 2020, the date the AG may begin enforcing the law.[3] Making matters even more challenging, the COVID-19 health crisis has significantly changed everyday life as well as standard business operations. Resources businesses had been dedicating to CCPA compliance efforts have been diverted to assist workforces and ramp up remote work capabilities. Californians and others in myriad states are under mandatory "shelter in place" or "stay at home" orders, which have disrupted the economy as well as entities' ability to build brand-new processes and compliance systems in advance of the CCPA's enforcement date.[4] The World Health Organization has deemed the coronavirus to be a global pandemic, and President Trump has declared California to be a "major disaster" zone as one of the primary epicenters of the virus outbreak.[5] W347-1 cont.

During the present health emergency, businesses should remain vigilant and focused on doing everything they can to assist the fight against the coronavirus and maintain viability so they can continue to employ individuals and support the economy. Entities all over the country are doing their part to put workers, consumers, and the world-at-large at the forefront of their considerations as they navigate new requests from government entities to reoutfit operations and

---

[3] Cal. Civ. Code § 1798.185(c).

[4] Alicia Lee, *These states have implemented stay-at-home orders. Here's what that means for you,* CNN (Mar. 24, 2020), located at https://www.cnn.com/2020/03/23/us/coronavirus-which-states-stay-at-home-order-trnd/index.html.

[5] White House, *Proclamation on Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak* (Mar. 13, 2020) located at https://www.whitehouse.gov/presidential-actions/proclamation-declaring-national-emergency-concerning-novel-coronavirus-disease-covid-19-outbreak/; Office of Governor Gavin Newsom, *California Secures Presidential Major Disaster Declaration to Support State's COVID-19 Emergency Response* (Mar. 22, 2020), located at https://www.gov.ca.gov/2020/03/22/california-secures-presidential-major-disaster-declaration-to-support-states-covid-19-emergency-response/.

produce supplies to support hospitals and healthcare workers.[6] IAB members are providing their communities with connectivity, content, news, and services for free or at a reduced cost and partnering with groups such as the World Health Organization to provide timely information to American citizens through digital advertising.[7] Businesses should not be preoccupied with potential enforcement actions for technical violations of an entirely new legal regime when the world is facing such critical circumstances.

W347-1 cont.

In the face of immense challenges, the quickly approaching enforcement date of July 1, 2020 leaves businesses strapped to bring their procedures into compliance as they are attending to calamitous and pressing matters. The AG, like data protection authorities in other jurisdictions, should consider delaying or pausing enforcement until January 2021 so businesses are not distracted from the task of supporting the economy and fighting the coronavirus.[8] We therefore ask you to postpone enforcement of the CCPA until January 2021.

II. Update the Guidance Regarding the Definition of "Personal Information" to Encourage Privacy by Design

The March 11, 2020 version of modified regulations removed previously proposed language that stated "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."[9] The AG should re-insert this subsection as it provides beneficial guidance to companies. Furthermore, we would recommend modifying the language to better reflect privacy by design principles.

W347-2

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 re-inserting 999.302 as follows:

> *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*

---

[6] *See, e.g.,* Samantha Masunaga, *California companies jump in to supply ventilators needed in coronavirus fight,* LA TIMES (Mar. 23, 2020), located at https://www.latimes.com/business/story/2020-03-23/coronavirus-california-companies-medical-supplies.

[7] https://www.iab.com/blog/good-works/

[8] United Kingdom Information Commissioner's Office, *Data protection and coronavirus: what you need to know*, located at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/covid-19-general-data-protection-advice-for-data-controllers/.

[9] *Compare* Cal. Code Regs. tit. 11, § 999.302(a) (proposed Feb. 10, 2020) *with* Cal. Code Regs. tit. 11, § 999.302(a).

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."

W347-2 cont.

III. Revise the Proposed "Responding to Requests to Know and Requests to Delete" Regulations to Remove Undue Burdens for Business and Expressly Acknowledge That a Business May Withhold Specific Pieces of PI if Divulging Such Information Could Lead to Unreasonable Security Risks or Contravene Other Competing Public Policy Considerations

W347-3

Section 999.313(c)(3) is overly restrictive, creates undue burdens for business, and increases privacy and security concerns. 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 AG 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 collected about a consumer need be made available. We appreciate and agree with the recognition that an absolute access requirement is not desirable or consistent with privacy best practices.

Moreover, the proposed provision is too restrictive and does not sufficiently recognize privacy concerns or undue burdens. As currently drafted, (c)(3) contemplates a four-part test when, in practice, no information will meet all four prongs. For example, if a business maintains the personal information solely for legal or compliance purposes, then it necessarily has to maintain it in a searchable or reasonably accessible format. If it did not, it could not search or access the information for its legal or compliance obligations. Or, if a business maintains personal information "solely" for legal or compliance purposes, then it cannot sell the personal information because it maintains the information for discreet legal or compliance purposes. In these ways, (c)(3) does not meaningfully limit the scope of what must be provided in response to access requests. Each of the prongs, on their own, should provide a sufficient basis for not providing personal information covered by that prong.

The modified regulations also do not sufficiently address privacy and security concerns as they 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." 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.

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.[10] However, if a business is forced to divulge such the information it maintains anyway due to a legal requirement, this obligation could put the consumer, the consumer's information, and/or the business at unreasonable risk, such as unauthorized access to personal information. Such a requirement would be contrary to the intent of CCPA and less privacy protective for consumers. IAB therefore 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. Additionally, the draft regulations should recognize other important qualifications for when a business should not have to provide consumers with specific pieces of information.

W347-3 cont.

Finally, subsection (c)(3) creates undue burdens for businesses. Many businesses possess personal information that is not typically readily searchable (and able to be produced) on a user-level basis. For example, businesses may maintain property or sales records that contain personal information of prospective customers, sometimes in paper form. Retrieving personal information belonging to specific individuals in these records would be overly burdensome if the business lacks the technical ability to identify which records contain personal information from the user. Because that data is not readily searchable or in a reasonably accessible format, under that factor alone, businesses should not be required to search for personal information within that data. IAB suggests the following text for § 999.313(c)(3):

> *A business shall not provide a consumer with specific pieces of personal information if the disclosure would: (1) create a substantial, articulable, and unreasonable risk to the privacy or security of that personal information, the consumer's account with the business, or the security of the business's systems, networks, or consumers; (2) interfere with law enforcement, judicial proceedings, investigations, or efforts to guard against, detect, or investigate malicious or unlawful activity or enforce contracts; (3) disclose the covered entity's trade secrets or proprietary information; (4) would require the covered entity to re-identify or otherwise link information that is not maintained in a manner that would be considered personal information; or (5) violate federal, state, or local laws, including rights and freedoms under the United States Constitution.*
>
> - *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 information it collects:*
>
> *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; or*
>
> *c. The business does not sell the personal information and does not use it for any commercial purpose.*

[10] Cal. Code Regs. tit. 11, § 999.325(c) (proposed Mar. 11, 2020).

IV. Make Clear that Internally Generated Data and Inferences Are Not Responsive to CCPA Access Requests Because They Are Not "Collected"

W347-4

The CCPA states that in response to a consumer request to access personal information, a business must disclose "[t]he specific pieces of personal information it has *collected* about the consumer."[11] The AG recently revised the text of the draft rules to mirror this statutory language by specifically stating that a "request to know" means a "request that a business disclose personal information that it has *collected*," including "[s]pecific pieces of personal information that a business has *collected* about the consumer."[12] We ask the AG to clarify that the data a business generates or infers internally is not collected and therefore is not responsive to a consumer's request to access specific pieces of information. This interpretation is rational given the plain text of the CCPA and its implementing regulations. It would also protect businesses' intellectual property and trade secrets and enable them to provide understandable privacy disclosures to consumers. As such, it is appropriate for your office to update the draft rules to exempt internally-generated and inferred information from the scope of access requests under the CCPA.

Businesses internally generate inferences and derived data regularly, and many of these inferences constitute intellectual property or trade secrets that are subject to protections under various state and federal legal regimes. Businesses should not be forced to reveal their intellectual property or trade secrets due to an ambiguous requirement in state law. The CCPA itself acknowledges that certain information may need to be exempt from the law's bounds and instructs the AG to "[e]stablish any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights…."[13] Despite the mandatory nature of this requirement, to date, the Attorney General has not issued any draft regulations related to trade secrets and intellectual property rights. We request that, to comply with its obligations under the CCPA, the AG issue a regulation establishing an exception to the requirements of the CCPA to protect against violations of intellectual property rights and the disclosure of trade secrets. In so doing, we believe the Attorney General should take into consideration the proprietary nature of certain data, particularly internally generated or derived data, and the impact that may have on a business. To this end, IAB suggests the following text for § 999.319 on Intellectual Property and Trade Secrets:

> *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 the business's intellectual property rights or result in the disclosure of trade secrets.*

Internally generated inferences and inferred data are created by virtually every business in its normal course of operations, and much of this data is duplicative of other information maintained in enterprise systems. For example, connecting an individual's name with his or her email address involves an inference made by the business processing the data. If businesses are required to return each and every inference connected with a consumer in response to a consumer's request to access specific pieces of personal information, the consumer would be

[11] Cal. Civ. Code § 1798.110(a)(5) (emphasis added).
[12] Cal. Code Regs. tit. 11, § 999.301(q) (proposed Mar. 11, 2020) (emphasis added).
[13] Cal. Civ. Code § 1798.185(a)(3).

inundated with hundreds if not thousands of pages of data that could bury important disclosures like a needle in a haystack. Consumers would be fatigued by excessively voluminous notices that would impede their ability to access important information about businesses' privacy practices. This result would not further the CCPA's purpose of providing consumers with enhanced transparency. To this end, the Attorney General should specify that businesses need not provide substantially similar or duplicative information to consumers in response to their requests to know. The CCPA already permits a business to refuse to act on "manifestly unfounded or excessive requests," recognizing that there are limits to information that must be provided to consumers in response to requests to know. Similarly, there are other instances in which it would be useful to limit the information required to be provided to consumers. For example, providing consumers with substantially similar or duplicative data would be disproportionately burdensome on businesses and not useful for consumers. An illustrative example is useful here. A business might keep the following specific pieces of information about a consumer: (1) data indicating a consumer watched a video; (2) data indicating that a consumer watched at least 25% of a video; (3) data indicating that a consumer watched at least 75% of a video; and (4) data indicating that a consumer watched at least 90% of a video. In response to a consumer's request to know what personal information a business has collected about her, the business should need only to produce a single data point to provide a consumer with a meaningful understanding of the information it has collected. IAB suggestions the following text for § 999.313(c)(12):

W347-4 cont.

> *In responding to a verified request to know categories of personal information, a business shall not be required to produce substantially similar or duplicative specific pieces of personal information.*

Additionally, retrieving internally generated inferences from businesses' systems to return them to consumers is no small task; internally generated data is often housed in various disparate databases throughout an enterprise and is therefore excessively burdensome to amalgamate. Additionally, this information may be unstructured or not readable by the average consumer due to privacy-protective measures a business has taken to mask identifying information associated with the internal inference. Revealing such data would be meaningless to consumers and would provide them with no useful insights. The practical challenge of consolidating internal inferences coupled with the minimal privacy value it would offer to consumers if returned in an access disclosure warrants an interpretation from your office that such data is not responsive to consumer access requests for specific pieces of personal information.

The CCPA and its implementing regulations clearly require businesses to disclose inferences in responses to consumer requests for specific pieces of information if those inferences are actually collected or received by the business from another entity.[14] Additionally, if a business discloses or sells its internally generated inferences, the business must list the category of "inferences" in its response to a request to know pursuant to the requirement to provide the categories of personal information sold and disclosed.[15] However, internal inferences that are generated by a business and not received from another entity are not

[14] *Id.* at § 1798.110(a)(5); Cal. Code Regs. tit. 11, § 999.301(q) (proposed Mar. 11, 2020).
[15] Cal. Civ. Code §§ 1798.115(a)(2)-(3).

"collected", and therefore they should not be required to be returned in response to a consumer request to access personal information. We ask the AG to issue a regulation clarifying this interpretation, which would further legislative intent and better enable consumers to receive digestible and understandable privacy disclosures under the CCPA.

W347-4 cont.

V. The CCPA regulations should allow service providers to process personal information for all business purposes permitted under the statute

W347-5

In response to the initial draft CCPA regulations, several commenters raised concerns that the regulations' restrictions on service providers' use of personal information did not align with the text of the CCPA statute.[16] As many commenters recognized,[17] this creates regulatory uncertainty that frustrates businesses' ability to engage service providers to efficiently and effectively perform tasks critical to offering products and services to California consumers. We urge the Attorney General to further clarify (through the text of the regulations and the Final Statement of Reasons) that the regulations allow service providers to process personal information for any "business purpose," as that term is defined in the statute. Specifically, the regulations should make it clear that a service provider may use personal information for any "operational purposes" enumerated in Section 1798.140(d) of the statute permitted under the written agreement between the business and the service provider without introducing non-statutory restrictions on service providers.

The CCPA defines "service provider" as a for-profit entity "that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose, pursuant to a written contract."[18] Accordingly, a service provider's rights to use personal information received from a business depends on what constitutes a "business purpose" under the statute.

The statute defines "business purpose" as "the use of personal information for the business's *or a service provider's operational purposes*, or *other notified purposes.*"[19] As multiple commenters have explained, this statutory text plainly affords service providers flexibility to process personal information not only for the *business's* purposes, but also for the *service provider's* own purposes so long as those purposes are necessary to perform the services specified in the contract.[20]

The statute provides several examples of permitted operational purposes, such as "[p]erforming services on behalf of the business or service provider, including . . . processing

---

[16] *See, e.g.*, Written Comments Received During 45-Day Comment Period, Comments of NAI at 24-25; Comments of California Cable and Telecommunications Association at 8-11; Comments of Consumer Data Industry Association at 13; Comments of CCIA at 7; Comments of CTIA at 14-16; Comments of Engine Advocacy at 5-6; Comments of California Chamber of Commerce at 11-12.

[17] See, e.g., Written Comments Received During 15-Day Comment Period, pdf [last updated on March 9, 2020], Comments of the Department of Justice at 5; Comments of the Entertainment Software Association at 4; Comments of the State Privacy and Security Coalition at 4; Comments of NAI at 14.

[18] Cal. Civ. Code § 1798.140(v).

[19] Id. at § 1798.140(d) (emphasis added).

[20] *See, e.g.*, Written Comments Received During 45-Day Comment Period, Comments of Entertainment Software Association at 4; Comments of Google at 1; Comments of TechNet at 12; Written Comments Received During 15-Day Comment Period, pdf [last updated on March 9, 2020], Comments of Entertainment Software Association at 4.

orders and transactions . . . providing advertising or marketing services . . . providing analytic services, or providing similar services on behalf of the business or service provider."[21] Operational purposes also include, for instance, "auditing related to a current interaction with a consumer, including but not limited to verifying the positioning and quality of advertising impressions,"[22] and "undertaking internal research for technological development and demonstration."[23]

The plain language of the "business purpose" definition sensibly limits uses of personal information to those which are "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."[24] The written agreement between the business and service provider, along with the privacy notices that consumers receive under the statute, specify the purposes for which personal information is collected and processed and also inform what uses are compatible with the context in which personal information is collected. Personal information disclosed to a service provider must be "pursuant to a written contract," which must prohibit the service provider from processing the information "for any purpose *other than for the specific purpose of performing the services specified in the contract* for the business . . . including retaining, using, or disclosing the personal information *for a commercial purpose other than providing the services specified in the contract with the business*."[25] W347-5 cont.

Permitting service providers to use personal information for their own operational purposes is not only required by a plain reading of the statutory text, but also is sound policy: in order to perform the contracted-for services on behalf of the business, service providers often *must* process personal information received from multiple businesses internally. For example, a business may hire a consulting service to help it determine the best location for its next retail store. To facilitate this analysis, the business likely will need to provide the service provider with personal information (such as names and transaction history) about its existing customers, consistent with its privacy policy. The service provider likely will need to combine this information internally with similar information it has collected from other customers to analyze where these existing customers, and other potential new customers with similar interests or preferences, might shop. Without disclosing any personal information received from other customers to the business, the service provider would use this combined data to inform the recommendations it provides to the business on where to build a new store. If the consultant is not permitted to combine personal information received from its different customers and use that information to perform its services consistent with its written agreements with those different businesses, the consultant's recommendations to the retail store would be based on incomplete and less relevant information that ultimately could produce a worse outcome for consumers.[26]

---

[21] Cal. Civ. Code § 1798.140(d)(5).
[22] *Id.* at § 1798.140(d)(1).
[23] *Id.* at § 1798.140(d)(6).
[24] *Id.* at § 1798.140(d).
[25] *Id.* at § 1798.140(v).
[26] Relatedly, the store might decide not to engage a service provider at all for these services if it meant having to treat the disclosure as a "sale" of data, which would require the store to expend significant resources to update its privacy notice, build and maintain an opt-out mechanism, and provide additional information when responding to consumers' "right to know" requests. This alternative is particularly problematic because reasonable consumers are W347-5 cont.

Importantly, this interpretation also ensures the privacy of consumers' personal information remains protected at all times for at least two reasons. First, consumers must have received notice that their personal information may be shared with the service provider for business purposes. Second, the CCPA requires that the written agreements between the service provider and its business customers prohibit the service provider "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," which safeguards the data from unauthorized processing and ensures that all uses are compatible with the context in which the personal information was collected.[27]

W347-5 cont.

Moreover, this interpretation aligns the Attorney General's second modified draft regulations and the plain text of the enabling statute. The Attorney General cannot enact rules that are inconsistent with the statutory text, including by narrowing a statute.[28] And the California legislature also specified that the Attorney General's regulations must further the CCPA's purposes.[29] Accordingly, we ask that the Attorney General further clarify that the regulations allow service providers to process personal information received from a business for any "business purpose," as that term is defined in the statute. IAB proposes the following text for § 999.314(c):

- *The Attorney General should reinstate the deleted language in (c)(1) to clearly permit a service provider to use personal information for any permitted business purpose pursuant to the written agreement between the business and the service provider.*[30]
- *To clarify that the Attorney General's regulations are meant to be consistent, and not in conflict, with the statute, we request that the Attorney General further modify the draft regulations by adding the underlined language to § 999.314(c):*
    - *A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except <u>to the extent permitted by the CCPA, including</u>: . . .*

---

unlikely to consider such disclosures, where the recipient of the data is providing services to the business and is subject to contractual restrictions on how the personal information is processed, to be a sale of personal information.

[27] *See* Cal. Civ. Code §1798.140(v) (requiring service providers to receive personal information "for a business purpose" and to process personal information for "the specific purpose of performing the services specified in the contract for the business").

[28] *In re Edwards*, 26 Cal. App. 5th 1181, 1189, 237 Cal. Rptr. 3d 673, 679 (Ct. App. 2018) (quoting Gov. Code, § 11342.2). Agencies do not have the discretion to promulgate regulations that are inconsistent with the relevant statute. *See Ontario Community Foundations, Inc. v. State Bd. of Equalization* (1984) 35 Cal.3d 811, 816–817, 201 Cal.Rptr. 165, 678 P.2d 378, ("[T]here is no agency discretion to promulgate a regulation which is inconsistent with the governing statute.") (Emphasis, citations and internal quotation marks deleted.)

[29] Cal. Civ. Code §§ 1798.185(a)(1); (b)(2).

[30] Section 999.314(c)(3) permits service providers to process personal information for internal purposes but includes the limitation "provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business." For the reasons discussed above, this example must be in alignment with the permissions service providers enjoy under the statute. Therefore, we understand the limitation to apply *only if* the written agreement between the business and the service provider does not permit the service provider to process personal information to build or modify profiles for other businesses.

W347-5 cont.

VI. Remove the Obligation for Businesses to Comply with Global Privacy Controls, Such as Browser Settings

The modified regulations state that "[i]f a business collects personal information from consumers online, the business shall treat 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… for that browser or device, or, if known, for the consumer."[31] W347-6

IAB asks that the AG remove the requirement to comply with browser and device-level privacy controls, as these obligations are not contemplated by the CCPA itself, impose new substantive requirements on businesses that the legislature has previously considered and elected to not include, and impede the development of new opt out tools. IAB believes this proposal is based on an inaccurate understanding of today's Internet ecosystem and existing browser controls, and the outcome of this proposal will have dramatic negative impacts on competition in the state of California.

a. The AG has instituted new substantive requirements on businesses that the legislature has previously considered and elected to not include.

The AG's mandate that businesses must treat browser settings and global privacy controls as valid requests to opt out of personal information sale is nowhere in the text of the CCPA itself. Despite the numerous amendments to the CCPA that were enacted in 2018 and 2019, none of those legislative vehicles included a requirement to honor browser settings or global privacy controls.[32] Additionally, the California legislature considered global privacy controls and browser setting mandates in the past and elected not to enact such legislation. As such, the AG's institution of a browser mandate in the draft regulations contravenes legislative intent and exceeds the scope of the CCPA.

In 2011, California Senator Alan Lowenthal introduced SB 761, instructing the AG to adopt regulations allowing consumers to opt out of online tracking. This bill failed to pass after careful consideration by the legislature. SB 761's failure to be enacted by the legislature demonstrates how technical tools that send a single signal to the entire Internet marketplace have been at legislators' disposal for years. Though legislators in California are well aware of these tools, they have specifically declined to make them the law of the land in the state. No new developments have arisen to prompt the AG to infer any intent on behalf of legislators to enact such tools now or support them. To the contrary, past experience in the state suggests that its representatives would not and do not approve of a wholesale browser signal or global privacy control requirement.

The legislature again considered a blanket Do Not Track ("DNT") requirement when it amended the California Online Privacy Protection Act in 2013.[33] However, that proposal made clear that it merely required the disclosure of whether a business honors such DNT signals and

---

[31] Cal. Code Regs. tit. 11, § 999.315(d) (proposed Mar. 11, 2020).
[32] *See* SB 1121 (2018); AB 25 (Cal. 2019); AB 874 (Cal. 2019); AB 1146 (Cal. 2019); AB 1355 (Cal. 2019); AB 1564 (Cal. 2019).
[33] AB 370 (Cal. 2013).

did not include an express mandate to respect the signals themselves. The California legislature declined to impose a one-size-all technical-based solution to effectuating consumer opt outs to personal information transfers in 2011 as well as 2013. The AG should not usurp that careful calculation by instituting a brand new and unprecedented requirement in California to respect such signals under the CCPA.

W347-6 cont.

b. The privacy controls mandate will have negative consequences for consumers by interfering with business relationships and consolidating market power.

W347-7

Requiring businesses to honor global 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, or whether the user is a California resident. 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 would thwart the aim of the CCPA to give consumers' control over personal information as well as have a negative revenue impact on the publishers and services consumers rely on and trust.

Concerns about concentrating power in the hands of intermediaries and consolidation of market power are not unfounded. There are four browser manufacturers that control over 90 percent of the browser market in the United States and three device manufacturers that control nearly 80 percent of the mobile phone market.[34] Examples of browsers interfering with consumer privacy preferences to the advantage their own revenue models have already been revealed.[35] The proposed rules' mandate that businesses must respect global privacy controls and browser settings stands to entrench these already deeply ingrained market players, and it places control in their hands rather than in the hands of consumers, effectively making these few companies gatekeepers to the Internet economy.

Moreover, the requirement advantages certain entities in the ecosystem over others. The AG's draft regulations note that if a browser control or global privacy setting conflicts with a setting set directly with the business, the business can contact the consumer to find out which signal should be respected.[36] Third parties that do not have a direct way to communicate with consumers will be disadvantaged over first party publishers who can serve notices and choices directly to consumers. This term therefore stands to distort the marketplace by providing

---

[34] *See Browser Market Share Untied States of America*, STATCOUNTER GLOBALSTATS, *located at* https://gs.statcounter.com/browser-market-share/all/united-states-of-america; *US Smartphone Market Share: By Quarter*, COUNTERPOINT RESEARCH, located at https://www.counterpointresearch.com/us-market-smartphone-share/.

[35] *See* Kimber Streams, *Internet Explorer 10 first browser to have Do Not Track as default*, THE VERGE (June 1, 2012), located at https://www.theverge.com/2012/6/1/3057265/internet-explorer-10-windows-8-do-not-track-default

[36] Cal. Code Regs. tit.11, § 999.315(d)(2) (proposed Mar. 11, 2020).

avenues for relief for certain entities at the expense of others, which likely would reduce revenue for independent publishers and online journalism.

The opportunity for intermediaries to interfere with consumer choices is magnified by the modified regulations' removal of the requirement that privacy controls shall not be designed with any pre-selected settings. The AG struck this provision from the draft rules, which stated: "[a]ny 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."[37] As a result, intermediaries have been given complete license to set default opt out signals that may not align with consumers' expressed choices and preference regarding sales of personal information. W347-7 cont.

The California Privacy Rights Act Ballot initiative recognizes the concern that businesses could leverage opt-out controls to gain unfair advantages over competitors, rather than to protect consumer privacy. As a result, the ballot initiative requires regulations for an opt-out preference signal that, among other things, ensures that platforms or browser device that sends the opt-out preference signal cannot unfairly disadvantage another business and must "clearly represent a consumer's intent and be free of defaults constraining or presupposing such intent[.]"[38] Consequently, privacy initiatives on the horizon in California address the concern that intermediaries will set default signals without consulting consumers. The AG's draft rules should similarly address this issue. If the AG decides to include browser controls, IAB asks that the AG include previously proposed language that prevents interference with consumer choice signals and signals that may be set by intermediaries without first consulting the consumer.

c. Claims in favor of browser controls such as DNT ignore the many outstanding problems with such browser-level controls.

Those advocating for and referencing the World Wide Web Consortium's DNT proposal as an example of the benefits of global privacy settings have ignored the real-world implications of this standard and its well documented unintended consequences.

For one, some have argued that DNT improves consumer experience by reducing the number of privacy choices consumers must make to protect their privacy. There is no evidence to support this. 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, a universal opt-out will prevent consumers from receiving a wide variety of services they expect and would not consider to be a sale or harmful to their privacy. As a result, consumers will be inundated with whitelisting requests, further deteriorating the consumer experience without providing enhanced privacy.

Others have argued that the DNT standard accommodates granular controls. These arguments ignore the reality of how browser makers have implemented the DNT mechanism in their software. Today, browsers only offer a binary choice to consumers in their privacy settings

---

[37] *Compare* Cal. Code Regs. tit. 11, § 999.315(d)(1) (proposed Feb. 10, 2020) *with* Cal. Code Regs. tit. 11, § 999.315(d)(1) (proposed Mar. 11, 2020).

[38] Ballot Initiative 19-0021 (Nov. 4, 2019), California Privacy Rights Act of 2020, § 1798.185(19)(A).

pages. This blunt instrument fails to provide the flexibility and granular privacy preferences that consumers need and expect, and that is required by other laws, such as the GDPR.

An additional concern with browser-level toggles is that they assume the consumer understands the browser's relationship with other applications and services on their devices. Consumer expectations around what a browser-level DNT toggle would do vary widely, which leads to confusion about what selling activities are impacted. This increases consumer confusion and can lead to a false sense of security.

The unintended consequences of requiring browser signals have been documented at length in Europe with respect to the proposed ePrivacy Regulation. Due to the significant concerns with mandating such a system, subsequent drafts of the ePrivacy Regulation have removed browser and device level privacy settings.[39] Even lead developers of the DNT mechanism have acknowledged the risks and unintended consequences of requiring by force of law the use of such global privacy signals, and have recommended not including this requirement in the regulations until after further deliberation.[40]

W347-6 cont.

d. The AG should provide businesses more flexibility and encourage innovative approaches to providing privacy preferences in line with consumer expectations.

The AG takes the position that in the absence of mandatory support for privacy controls, "businesses are likely to reject or ignore consumer tools."[41] While it is true that adoption of certain existing privacy controls has varied across publishers and platforms (*i.e.*, adoption of the DNT standard), IAB urges the AG to recognize that the CCPA is without precedent and represents a fundamental shift in California privacy law. As the CCPA comes into effect in 2020, IAB expects to see market forces leading to 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 global privacy controls could impede the development of various helpful tools and solutions for consumers to use to exercise choice in the marketplace.

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 global signal developed to facilitate CCPA compliance. We therefore respectfully ask the AG to remove the requirement to treat global privacy controls as valid requests to opt out of personal information sale and update the draft rules so that businesses

---

[39] Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications* (Feb. 20, 2020), located at https://data.consilium.europa.eu/doc/document/ST-5979-2020-INIT/en/pdf.

[40] See, e.g., Written Comments Received During 15-Day Comment Period, pdf [last updated on March 9, 2020], Comments of Aleecia M. McDonald at 14-15.

may respect such global 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. W347-6 cont.

* * *

We appreciate the opportunity to submit these comments. If you have questions, please contact me at [redacted].

Respectfully submitted,

Alex Propes
Vice President, Public Policy & International
Interactive Advertising Bureau

Message

From: Robert Callahan [redacted]
Sent: 3/27/2020 1:59:20 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Elizabeth Banker [redacted]
Subject: Internet Association comments on the Second Set of Modifications to Text of Proposed CCPA Regulations
Attachments: IA-Comments-on-Second-Set-of-Modified-Proposed-Regulations-CCPA_03272020.pdf

To Whom it May Concern:

Please find attached Internet Association's comments on the Second Set of Modified Proposed Regulations for the California Consumer Privacy Act of 2018. Please do not hesitate to reach out if you have any questions.

Thank you,
Robert
--

Robert Callahan
Senior Vice President, State Government Affairs

O: [redacted]

INTERNET ASSOCIATION
1303 J Street, Suite 400, Sacramento, CA 95814

March 27, 2020

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

Re: *Internet Association Comments on Second Set of Modified Proposed Regulations for the California Consumer Privacy Act of 2018*

To Whom It May Concern:

Internet Association (IA) appreciates the opportunity to review and provide the Attorney General's Office (AGO) feedback on the Text of the Second Set of Modified Regulations (Second Set) for the California Consumer Privacy Act (CCPA). 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 complying with applicable laws, and advocating 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.

IA appreciates that the Attorney General's Office provided the public an additional opportunity to provide comments on the changes to the text of the regulations for the CCPA, as well as the AGO's efforts to revise the regulations based on the feedback received. In particular, IA was pleased to see that the proposed design for the opt-out button has been deleted from the Second Set. IA had significant concerns that the design would confuse consumers, likely hindering their efforts to exercise choice under the CCPA.

[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/).

IA continues to have concerns on several provisions of the proposed Regulations which, in the interest of brevity, will not be fully reiterated here. However, IA believes it is important to note that our comments with regard to the initial Proposed Regulations[3] and the Modified Proposed Regulations[4] remain largely unaddressed. This round of comments is primarily directed at changes to the proposed regulations made in this latest set of revisions. In addition to feedback on the Second Set, IA also asks that the AGO fulfill the rulemaking mandate in CCPA related to intellectual property and trade secrets.

Comments On Changes Made In The Second Set

There are a few changes in the Second Set of Proposed Regulations that IA would like to highlight because they introduce new problems, aggravate existing problems, or raise a concern that had previously been addressed but is now once again problematic. These comments relate to:

1. Consumer notices and requests
2. Service providers
3. Anti-discrimination provisions
4. Intellectual property and trade secrets
5. Calculating value of consumer data

Each of these is addressed in more detail below.

1. Consumer Notices And Requests

Consumer notices and the processes by which consumers can exercise the rights created by the CCPA are the heart of the CPPA. For this reason, in advance of the January 1, 2020 effective date of the CCPA, businesses focused on designing and building the mechanisms for providing the required notices and processing consumer requests. Almost three months after the CCPA took effect there are still proposals being made that fundamentally change the requirements and which companies may not be able to comply with before, or even after, July 1, 2020 when enforcement begins. IA, as stated in our prior comments, urges the AGO to limit the CCPA regulations to only those needed to give the CCPA effect.

[3] Available at: https://internetassociation.org/files/ia_comments-on-proposed-ccpa-regulations_12062019_privacy/.
[4] Available at: https://internetassociation.org/files/ia_comments-on-proposed-modified-ccpa-regulations_02252020_privacy/.

The changes to the Second Set that are needed to make the regulations clear and in line with the CCPA include:

- **Clarification Of § 999.306(b)(1)**

This subsection should provide clearer guidance to mobile applications on the required location of the Do Not Sell My Information link. It would be helpful if the AGO could make it clearer which locations for the opt-out link are required and which are discretionary. It appears the language intended to require the opt-out link on the download/landing page and to make placing a link within the settings menu of an app discretionary. If either location fills the notice requirement, this should be clarified. W348-1

- **Clarification Of § 999.308(c)(1)(e)**

The draft regulations introduce a new requirement that when identifying categories of sources of personal information, "the categories shall be described in a manner that provides consumers a meaningful understanding of the information being collected." Section 999.308(c)(1)(e). It is unclear why this provision requires a meaningful understanding of the information collected, when the primary purpose of the provision is to provide notice and transparency around sources of information. Section 999.306(c)(1)(c) is directed towards providing consumers notice about personal information collected. The text for Subsection 999.308(c)(1)(e) should be modified to make clear that consumers should be able to develop a meaningful understanding of the "categories of sources" listed in the privacy policy by revising it to read: "Identify the categories of sources from which the personal information is collected. The categories shall be described in a manner that provides consumers a meaningful understanding of the sources from which the information is ~~being~~ collected." W348-2

- **§ 999.313 Responding To Requests To Know And Requests To Delete**

Subsection (c)(3). Subsection (c)(3) does not adequately take into account burdens for business and privacy and security concerns. The consumer rights created by the CCPA were not intended to be absolute. This is clear from exceptions that exist in specific provisions, such as exceptions to the right to delete in Section 1798.105(d), and general exceptions in Section 1798.145. In addition, 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). IA appreciates that subsection (c)(3) of Section 999.313 of the Second Set recognizes that not *all* personal information a business has collected about a consumer needs be made available to comply with a consumer's request for access. However, the practical effect of the four-part test in subsection (c)(3) is far too restrictive and little, if any, information will be able to satisfy it. For example, if a business maintains the personal information solely for legal or compliance purposes, then it necessarily has to maintain it in a searchable or reasonably accessible format. If it did not, it could not search or access the W348-3

information for its legal or compliance obligations. In addition, many businesses possess personal information that is not typically readily searchable (and able to be produced) on a user-level basis. For example, businesses may maintain property or sales records that contain personal information of prospective customers, sometimes in paper form. Retrieving personal information belonging to specific individuals in these records would be overly burdensome if the business lacks the technical ability to identify which records contain personal information from the user. Because that data is not readily searchable or in a reasonably accessible format, under that factor alone, businesses should not be required to search for personal information within that data. As written, subsection (c)(3) does not meaningfully limit the scope of what must be provided in response to access requests. Each of the prongs, on their own, should provide a sufficient basis for not providing personal information covered by that prong.

Subsection (c)(3) also does not sufficiently address privacy and security concerns. As currently drafted subsection (c)(3) will result in businesses creating new searchable databases of personal information for the single purpose of being able to comply with a consumer request under the CCPA. Having to create systems that enable searching user-level data is not only burdensome, but actually reduces individual privacy and security of personal information. For example, log data stored in a data warehouse may not be stored in a centralized profile, making it difficult to retrieve data about a single user without (a) scanning potentially billions of lines of warehoused data, or (b) making copies of the data and centralizing it, thus raising privacy risks by requiring businesses to centralize disparate data and index it by user identifiers. There may be specific pieces of personal information that businesses collect and maintain that, if disclosed externally, could pose security risks to either the business's systems or networks or consumer personal information by allowing bad actors to exploit systems or networks. W348-3 (cont.)

The initial Proposed Regulations appropriately recognized these scenarios and prohibited businesses from providing consumers with specific pieces of personal information when doing so would present "substantial, articulable, and unreasonable" security risks to the personal information, the consumer's account with the business, or the security of the business's systems or networks. This prohibition should be added back to the final regulations to protect both consumers and businesses alike. Additionally, the draft regulations should recognize other important qualifications for when a business should not have to provide consumers with specific pieces of information.

The text of § 999.313(c)(3) should be revised as follows: A business shall not provide a consumer with specific pieces of personal information if the disclosure would: (1) create a substantial, articulable, and unreasonable risk to the privacy or security of that personal information, the consumer's account with the business, or the security of the business's systems, networks, or consumers; (2) interfere with law enforcement, judicial proceedings, investigations, or efforts to guard against, detect, or investigate malicious or unlawful activity or enforce contracts; (3) disclose the covered entity's trade secrets or proprietary information;

(4) would require the covered entity to re-identify or otherwise link information that is not maintained in a manner that would be considered personal information; or (5) violate federal, state, or local laws, including rights and freedoms under the United States Constitution.
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 information it collects:

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; or
c. The business does not sell the personal information and does not use it for any commercial purpose.

W348-3 (cont.)

Subsection (c)(12)[Proposed new regulatory provision]. The Attorney General should specify that businesses do not need to provide substantially similar or duplicative information to consumers in response to their requests to know. This will help to avoid overwhelming consumers with voluminous data and imposing burdens on businesses without any justification in terms of privacy benefit. A single data point could be housed in multiple systems across a business. For many of the same reasons explained above regarding subsection (c)(3), having to make all such systems searchable would actually have a negative effect on consumer privacy and security. It also creates a significant burden for businesses.

IA proposes the addition of new suggested text for § 999.313 (c)(12): In responding to a verified request to know categories of personal information, a business shall not be required to produce substantially similar or duplicative specific pieces of personal information.

W348-4

Intersection of § 999.313 with § 999.302. To avoid confusion for consumers and burdens to businesses associated with the right to know, the Attorney General should re-insert § 999.302 Guidance Regarding the Interpretation of CCPA Definitions from the Modified Proposed Regulations and issue guidance regarding information that is generated internally by a business about a consumer, provided such personal information is not transferred or disclosed to any third parties. Specifically, it would be appropriate to exclude information generated internally from disclosure in response to access requests because providing such information would impose significant burdens on businesses without corresponding benefits to consumers, who are likely to be confused by receiving such information. For example, businesses often generate internal information for reporting and other mundane business reasons. This internal information is not provided by a consumer or acquired from third parties, nor is it shared externally. It is used only for internal business reasons.

The CCPA appropriately limits access rights to "collected" data and, in defining "collected," specifically excluded language from the CCPA ballot initiative that defined "collect" more broadly, to include "buying, renting, gathering, obtaining, storing, using, monitoring, accessing,

W348-5

or making inferences based upon, any personal information pertaining to a consumer by any means." If the CCPA required businesses to return *all* generated data, including inferences, in response to consumer access requests, in many instances, businesses would have to build new systems for searching for them and collecting them in a centralized way. This is because this type of data is commonly not maintained in a human-readable way.

W348-5 (cont.)

Subsection 999.313(d)(7). This requires that for any consumer making a deletion request, if a company cannot verify the consumers identity, the company 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." The reasons why consumers may choose to delete data and opt-out of the sale of personal information are often quite different. Thus, when a consumer asks for personal information to be deleted, they should not be confused by receiving information on how to opt-out. This could lead the consumer to believe that opting-out of sale will accomplish the same objective as the request to delete, when in fact they are wholly unrelated.

W348-6

There is also no compelling reason why the availability of the right to opt-out of sale needs to be flagged to consumers if their request to delete is refused. Putting aside concerns about a legal requirement to prompt an individual who has failed verification to take any action on an account, the CCPA makes opt-out of sale the most prominent consumer right. The right to opt-out of sale is the only one of the CCPA rights that requires specific placement, in addition to the privacy policy, on webpages, mobile app download pages, and elsewhere. The privacy policy must contain information on how to exercise the right to delete and the right to opt-out. It is therefore unlikely that a consumer who chooses to request deletion is unaware of the right to opt-out of sale, and more likely that the consumer chooses deletion because it accomplishes what they desire. And 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.

The requirement should be struck from the regulations. If that is not possible, a more efficient approach would be to require the business to point the consumer to the privacy notice that explains how to exercise all of their privacy rights so that they can review all of their options.

- **Remove § 999.315. Requests To Opt-Out**

IA has previously described its concerns with the language in the prior two versions of the Proposed Regulations regarding the AGO's choice to create a new requirement for online services to re-engineer their systems to recognize and process automated opt-out of sale signals sent by browsers, devices, or other mechanisms.[5] This provision has grown even more

W348-7

[5] *See* pp. 17-18, IA Comments on the Modified Proposed Regulations for CCPA (available at: https://internetassociation.org/files/ia_comments-on-proposed-modified-ccpa-regulations_02252020_priva

troubling by allowing a default setting to override affirmative indications of a consumer's choices.

IA reiterates its objection that this new requirement exceeds the AGO's rulemaking authority. It has no basis in the CCPA, and in fact, is in stark contrast to the very deliberate choices that the legislature made in the CCPA regarding the details of how the opt-out of sale should work. It is even more troubling that this requirement lacks precision, specificity, or any detail that would provide clear notice of what types of signals a business must be prepared to receive and how it should respond. The requisite lack of clarity has been one of the reasons why the Do Not Track browser signal has not been widely adopted. The AGO should look at the precedent of Do Not Track, not as a model, but as a warning of the significant challenges of putting such a system into operation. For example, if a website receives an opt-out sale signal from a browser from a user who is not logged in, how is the website to implement and track that signal and what should happen if the users logs into their account, receives a notice from the business about their choice to opt-out and the user affirmatively declines to opt-out, but does not change the browser setting. Tracking and implementing signals will be very difficult without much more direction. There is no barrier or vetting process for browser plug-ins that may promise consumers that they will be opted-out of sale, but behind the scenes be collecting consumer data for their own nefarious purposes. The burdens on business could be immense because this low barrier to entry will allow a virtually unlimited number of potential signals to be developed.

W348-7 (cont.)

The draft rules mandate that businesses treat user-enabled global privacy controls that communicate or signal a consumer's choice to opt-out of the sale of personal information as a valid request. The proposed changes to (d)(1) contravene the statute by removing a consumer's right to opt-out and give browser publishers significant power over consumer choice, thereby circumventing that choice.

The statute contemplates consumers directing specific businesses not to sell data; not browsers telling that to all businesses through a single opt out. The draft mandate of honoring user-enabled global privacy controls would have the likely effect of allowing browsers to subvert consumer choice.

IA is particularly troubled by the choice in the Second Set to delete the following language from Section 999.315(d)(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." The lack of affirmative consumer choice to use an automated opt-out is concerning in part because it would essentially allow a default setting in a browser to override affirmative choices a consumer has made in situations where they had significantly more notice and, thus, a better understanding of the choice. Subsection (d) requires that a business "respect" the default

cy/); pp. 34-35, IA Comments on the Proposed Regulations for CCPA (available at: https://internetassociation.org/files/ia_comments-on-proposed-ccpa-regulations_12062019_privacy/).

opt-out signal, but allows the consumer to be contacted by the business. CCPA does require that the opt-out process be easy for consumers, but it also anticipates that the consumer will "direct" a business to opt-them out. The removal of this language regarding pre-selected settings directly conflicts with the CCPA's grant to consumers of "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." 1798.120(a).

This opt-out is at the heart of the delicate balance that the CCPA creates between a consumer's control over personal information and business' legitimate interests in relying on such information to offer personalized services. The prior draft of the regulations, the Modified Proposed Regulations, was more consistent with this statutory structure, requiring users to affirmatively make the choice to enable browser-based opt-out signals, rather than having such decisions made by pre-selected settings.

The regulations, in their current form, make a significant economic/policy decision to upend that balance, substantially altering the operation of the law's primary requirement - one that was vigorously and repeatedly debated in the legislature. As common, widely-used web browsers implement these settings, opt-out rates in the nation's most populous state (if not across the world) could soar, with significant effects on businesses of all sizes. The AG should at least conduct further study on the operation of these controls and associated economic impacts before scaling back these important limitations.

W348-7 (cont.)

Additionally, by removing the prohibition that the privacy control shall not be designed with any pre-selected settings, the draft rules appear to give browser publishers significant power by allowing them to unilaterally turn on an opt-out or even do it selectively for certain companies. The California Privacy Rights Act ballot measure contemplates a scenario where businesses could leverage opt-out controls for competitive advantages and in response requires regulations for an opt-out preference signal that, among other things, ensures that platforms or browser device that sends the opt-out preference signal cannot unfairly disadvantage another business and "clearly represent a consumer's intent and be free of defaults constraining or presupposing such intent[.]"

In addition, IA objects to the AGO creating yet more requirements that require time to be designed and implemented if a business wants to communicate with consumers about the opt-out signal and the impact on the consumer's account or online experience. The CCPA has already taken effect and enforcement is scheduled to begin in just a few months. The AGO should not require any significant changes to the fundamentals of the technology for consumers to exercise their right to opt-out, such as building new pop-up window functionality. This introduces new burdens and costs on businesses that have already built CCPA-complaint opt-out functionality.

IA continues to believe that the entirety of Section 999.315 should be removed for all of the reasons cited above. If the AGO will not remove Section 999.315, IA recommends the following changes:

(d) ~~(c)~~ 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 interest in potentially opting-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 as a~~as an expression of interest in opting out and shall provide the consumer with an opportunity to opt out under Civil Code section 1798.120. For example, the business may show the consumer a pop-up window that, when clicked, redirects the consumer to the business's Notice of right to opt out, or provide the consumer with other similar methods designed to facilitate the consumer's right to opt out.

W348-7 (cont.)

(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.
(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 provide the consumer with the opportunity to confirm existing settings or manage those settings when consumers direct themselves to the business's site. ~~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.~~ For example, the business may show consumers a pop-up window that, when clicked, redirects the consumer to a page where consumers may manage their privacy settings, or provide the consumer with other similar methods designed to facilitate the management of the consumer's privacy settings.

2. Service Providers

Section 999.314 of the CCPA regulations should allow service providers to process personal information for all business purposes permitted under the statute. In response to the initial proposed regulations, several commenters raised concerns that the regulations' restrictions on service providers' use of personal information did not align with the text of the CCPA statute.[6]

W348-8

[6] *See, e.g.*, Written Comments Received During 45-Day Comment Period, Comments of NAI at 24-25; Comments of California Cable and Telecommunications Association at 8-11; Comments of Consumer Data Industry Association at 13; Comments of CCIA at 7; Comments of CTIA at 14-16; Comments of Engine Advocacy at 5-6; Comments of California Chamber of Commerce at 11-12.

As many commenters recognized,[7] this not only makes the regulations susceptible to judicial challenge, but also creates regulatory uncertainty that frustrates businesses' ability to engage service providers to efficiently and effectively perform tasks critical to offering products and services to California consumers. The Second Set presents similar difficulties as the initial draft. IA urges the Attorney General to further clarify (through the text of the regulations and the Final Statement of Reasons) that the regulations allow service providers to process personal information for any "business purpose," as that term is defined in the CCPA. Specifically, the regulations should make it clear that a service provider may use personal information for any "operational purposes" enumerated in Section 1798.140(d) of the statute that are permitted under the written agreement between the business and the service provider without introducing non-statutory restrictions on service providers.

The CCPA defines "service provider" as a for-profit entity "that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose, pursuant to a written contract."[8] Accordingly, a service provider's rights to use personal information received from a business depends on what constitutes a "business purpose" under the statute.

W348-8 (cont.)

Section 1798.140(d) defines "business purpose" as "the use of personal information for the business's *or a service provider's operational purposes*, or *other notified purposes*." As multiple commenters have explained, this statutory text plainly affords service providers flexibility to process personal information not only for the *business's* purposes, but also for the *service provider's* own purposes so long as those purposes are necessary to perform the services specified in the contract.[9]

The statute provides several examples of permitted operational purposes, such as "[p]erforming services on behalf of the business or service provider, including . . . processing orders and transactions . . . providing advertising or marketing services . . . providing analytic services, or providing similar services on behalf of the business or service provider."[10] Operational purposes also include, for instance, "auditing related to a current interaction with a consumer, including but not limited to verifying the positioning and quality of advertising

[7] *See, e.g.*, Written Comments Received During 15-Day Comment Period, pdf [last updated on March 9, 2020], Comments of the Department of Justice at 5; Comments of the Entertainment Software Association at 4; Comments of the State Privacy and Security Coalition at 4; Comments of NAI at 14.
[8] Cal. Civ. Code § 1798.140(v).
[9] *See, e.g.*, Written Comments Received During 45-Day Comment Period, Comments of Entertainment Software Association at 4; Comments of Google at 1; Comments of TechNet at 12; Written Comments Received During 15-Day Comment Period, pdf [last updated on March 9, 2020], Comments of Entertainment Software Association at 4.
[10] Cal. Civ. Code § 1798.140(d)(5).

impressions,"[11] and "undertaking internal research for technological development and demonstration."[12]

The plain language of the "business purpose" definition sensibly limits uses of personal information to those which are "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."[13] The written agreement between the business and service provider, along with the privacy notices that consumers receive under the statute, specify the purposes for which personal information is collected and processed and also inform what uses are compatible with the context in which personal information is collected. Personal information may only be disclosed to a service provider "pursuant to a written contract," which must prohibit the service provider from processing the information "for any purpose *other than for the specific purpose of performing the services specified in the contract* for the business . . . including retaining, using, or disclosing the personal information *for a commercial purpose other than providing the services specified in the contract with the business*."[14]

W348-8 (cont.)

Permitting service providers to use personal information for their own operational purposes is not only required by a plain reading of the statutory text, but also is sound policy: in order to perform the contracted-for services on behalf of the business, service providers often *must* process personal information received from multiple businesses internally. For example, some service providers may be specifically retained by businesses because of their ability to combine information across different businesses, in order to assist each of the businesses to better perform their business by providing insights, but not actual personal information.

Importantly, consumers' personal information remains protected at all times consistent with the CCPA and regulations. First, consumers must have received notice that their personal information may be shared with the service provider for business purposes. Second, the CCPA requires that the written agreements between the service provider and its business customers prohibit the service provider "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," which safeguards the data from unauthorized processing and ensures that all uses are compatible with the context in which the personal information was collected.[15]

---

[11] *Id.* at § 1798.140(d)(1).
[12] *Id.* at § 1798.140(d)(6).
[13] *Id.* at § 1798.140(d).
[14] *Id.* at § 1798.140(v).
[15] *See* Cal. Civ. Code §1798.140(v) (requiring service providers to receive personal information "for a business purpose" and to process personal information for "the specific purpose of performing the services specified in the contract for the business").

Moreover, this interpretation aligns the Attorney General's second modified draft regulations and the plain text of the enabling statute. The Attorney General's Office cannot enact rules that are inconsistent with the statutory text, including by narrowing a statute.[16] And the California legislature also specified that the Attorney General's regulations must further the CCPA's purposes.[17] Accordingly, we ask that the Attorney General further clarify that the regulations allow service providers to process personal information received from a business for any "business purpose," as that term is defined in the statute.

W348-8 (cont.)

IA proposes the text for § 999.314(c) be revised by reinstating the deleted language in (c)(1) to clearly permit a service provider to use personal information for any permitted business purpose pursuant to the written agreement between the business and the service provider.[18] To clarify that the Attorney General's regulations are meant to be consistent, and not in conflict, with the statute, IA also requests that the Attorney General further modify the draft regulations by adding the underlined language to § 999.314 (c): A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except to the extent permitted by the CCPA, including: . . .

3. Anti-Discrimination Provisions

The Second Set makes changes to definitions and provisions that impact the anti-discrimination provisions of CCPA and how they are implemented. All of the versions of the proposed regulations are confusing in how they seek to implement this element of the CCPA. First, IA would like to note that the legislature only charges the AGO with establishing rules and guidelines regarding "financial incentive offerings" rather than "financial incentives."[19] In the context of the full text of Section 1798.185(a)(6), this should be read as relating to the

W348-9

[16] *In re Edwards*, 26 Cal. App. 5th 1181, 1189, 237 Cal. Rptr. 3d 673, 679 (Ct. App. 2018) (quoting Gov. Code, § 11342.2). Agencies do not have the discretion to promulgate regulations that are inconsistent with the relevant statute. *See Ontario Community Foundations, Inc. v. State Bd. of Equalization* (1984) 35 Cal.3d 811, 816–817, 201 Cal.Rptr. 165, 678 P.2d 378, ("[T]here is no agency discretion to promulgate a regulation which is inconsistent with the governing statute.") (Emphasis, citations and internal quotation marks deleted.).

[17] Cal. Civ. Code §§ 1798.185(a)(1); (b)(2).

[18] Section 999.314(c)(3) permits service providers to process personal information for internal purposes but includes the limitation "provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business." For the reasons discussed above, this example must be in alignment with the permissions service providers enjoy under the statute. Therefore, we understand the limitation to apply *only if* the written agreement between the business and the service provider does not permit the service provider to process personal information to build or modify profiles for other businesses.

[19] "Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter." Section 1798.185(a)(6).

notice of financial incentives, and not inclusive of financial incentives generally — and certainly not inclusive of price of service differences tied to the value of a consumer's data. Thus the entirety of Section 999.336 of the Regulations is not required by the CCPA, is arguably inconsistent with the CCPA, and creates unnecessary confusion for businesses and consumers about its intent and operation.

The purpose of non-discrimination provisions is to allow consumers to exercise rights created by the CCPA without fear of retaliation in the form of unnecessary restrictions on access to or quality of products and services. The rights created by the CCPA are correctly reflected in Section 999.336(c) which states: "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." (*emphasis added*). They are also very clearly delineated by the text of the CCPA, which creates only the following rights:

W348-9 (cont.)

- Section 1798.100 states: (a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.
- Section 1798.105 states: (a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.
- Section 1798.110 states: (a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following...
- Section 1798.115 states: (a) A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer...
- Section 1798.120 states: (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.

Thus in Section 1798.125(a) (1), where it states "A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title," CCPA refers to specific rights created in Sections identified above. These rights are the right to know or right to access, the right to delete, and the right to opt-out. Nothing in the CCPA authorizes the AGO to create new rights via regulations, but this is what the AGO's proposed regulations seek to do.

The expansion of the definition of "price or service difference" through the various iterations of the proposed regulations is problematic due to the way the term is used in Section 999.336. That draft regulatory provision appears to collapse subsections (a) and (b) of Section 1798.125 into one. The Second Set states in Section 999.336(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." This does not accurately reflect the structure of the CCPA's non-discrimination provision which has two distinct parts. The first part bars discrimination against consumers who exercise a right created by the CCPA — the right to know or access, the right to delete, and the right to opt-out — by denying a service, providing a different price, or providing a different quality. The first part continues by making clear that a price or service difference is not discriminatory if it is reasonably related to the value of the consumer's data to the business. Specifically, it states, "Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data." Section 1798.125(a)(2). Thus, Section 999.336(a) of the regulations seems to contradict the CCPA by declaring any price and services difference "discriminatory" if it treats a consumer differently because the consumer exercised a right under the CCPA. The CCPA makes clear that price and service differences would only be discriminatory and prohibited if the difference is triggered by a consumer's exercise of a right created by the CCPA and is not reasonably related to the value of the customer's data. Section 999.336(a) is overly broad as written and contradicts the plain language of Section 1798.125(a)(2) of the CCPA. W348-9 (cont.)

The second part of the CCPA non-discrimination provision specifically allows the use of the financial incentives without taking a position on whether they are discriminatory. The financial incentives provisions of CCPA are better understood as an affirmative authorization to compensate or encourage consumers to refrain from exercising rights created by the CCPA. Such programs, without this authorization, might be viewed as discriminatory and so the CCPA creates incentives for following the rules for financial incentive programs by providing regulatory clarity about what is allowed and under what conditions. In addition, subsection (b)(1), Section 1798.125 of the CCPA reiterates that, "A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data." This language is almost identical to the language in (a)(2) of the Section. Thus, the CCPA specifically authorizes businesses to do two things: (1) offer financial incentives including payments as compensation for collection, sale, or deletion of personal information; and (2) offer different prices or quality of goods or services if tied to the value of the information.

By collapsing the concepts "financial incentives" and "price or service differences" in subsection (a), Section 999.336, the Second Set regulates price of service differences in a way unsupported by the CCPA — essentially treating them in the same way as financial incentives. IA also notes that this section purports to allow the AGO the authority to create new rights beyond those identified in the CCPA. This is unsupported by the text of the CCPA. The CCPA does not make any allowance in the provisions on anti-discrimination or in the rulemaking

section for the creation of new rights by the AGO. Section 999.336(a) should be modified to strike "financial incentives" and "or these regulations." W348-9 (cont.)

Section 999.336(b) also treats financial incentives and price or service differences as though they are equivalent. But the CCPA treats the two concepts differently, regulating how "financial incentives" are offered but not similarly regulating price or service differences. Thus, subsection (b) should also be modified, in this case to strike the reference to "price or service differences." This subsection also requires that financial incentives be related to the value of the consumer's data to the business. This is not a requirement of the CCPA. Section 1798.125(b)(1) says a business "may offer financial incentives" and in the next sentence says, a "business may *also* offer a different price." (*emphasis added*). The requirement that a price difference or difference in quality be tied to the value of the consumer's data is only present for the price or service difference. The remainder of subsection (b) refers only to "financial incentives." Financial incentives may not be, "unjust, unreasonable, coercive, or usurious in nature." Second Set, Section 999.336(b)(4). W348-10

Subsection 999.336(b) overreaches yet another way by creating a new affirmative obligation to determine a value of consumer data for purposes of offering a financial incentive or a price or service difference. For the reasons explained above, this requirement should not be read as being applicable to financial incentives. Under the CCPA a business could pay a consumer more than the value of their data as long as it is not "unjust, unreasonable, coercive, or usurious in nature." Likewise, the CCPA does not support applying any obligations to how price or service differences are implemented. As IA has recommended before, Subsection (b) should be struck, and with it Section 999.337 regarding determining the value of consumer information, an obligation that has no foundation in the CCPA.[20] Section 999.336(e) should also be revised to delete the reference to price or service differences. W348-11

For these reasons explained above, the recent addition of the word "collection" to the definition of price or service difference also should be deleted. This definition has evolved with each successive round of proposed regulations as follows:

<u>Definition of Price or Service Difference, Section 999.301:</u>

Proposed Regulations:
"Price or service difference" means (1) any difference in the price or rate charged for any goods or services to any consumer, 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, including denial of goods or services to the consumer. W348-12

Modified Proposed Regulations:

[20] Section 999.337 is further discussed on pages 6 and 16.

(o) "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.

Second Set Modified Proposed Regulations:
"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 collection, retention, 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 collection, retention, or sale of personal information, including the denial of goods or services to the consumer.

W348-12 (cont.)

This definition has been expanded far beyond what is necessary to elaborate on the CCPA. The definition applies language to price or service differences that only appears in the CCPA in connection with financial incentives. Part of one of the various definitions appears to be intended to describe financial incentives which the Second Set defines as: "a program, benefit, or other offering, including payments to consumers, related to the collection, retention, or sale of personal information." Despite appearing to define a financial incentive as a type of price or service difference, the proposed regulations use both terms side by side. This is confusing and not supported by the CCPA. The proposed regulations attempt to create new rights around the collection and use of data that do not exist in the CCPA by tying price or service differences to collection and use of data. That radically alters the balance struck by the Legislature between giving consumers choice and allowing data-dependent businesses to continue to exist subject to the specific requirements spelled out in the CCPA.

The definition of "price or service difference" is not necessary for the regulations if they are appropriately modified to no longer treat price and service differences as though they should be regulated the same as financial incentives, as IA recommends above. Thus, the definition should be struck from Section 999.301(j). At the very least, it should be returned to the original definition in the initial Proposed Regulations.

IA continues to believe that Section 999.337 on calculating the value of data should be struck. It attempts to articulate standards by which businesses can calculate the "value" of consumer data. However, as IA and other commenters have noted before, no specific piece of data has a fixed value. The perceived value of data is subjective, in constant flux, and depends on context. Value is "in the eye of the beholder." Because data lacks clear, objective value, academics have come up with wildly different estimates for the value of certain services to people and the value of a consumer's data to a business. Specifically with respect to free, ads-based, personalized services, people don't give up or exchange data for their experience; instead the

W348-13

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. To make this clearer the definition of Financial Incentive should also be adjusted to read, "Financial incentive means a program, benefit, or other offering, including payments to consumers, ~~related to~~ as compensation for the collection, ~~retention,~~ deletion or sale of personal information." This aligns the definition with the language of the CCPA.

W348-13 (cont.)

4. Intellectual Property And Trade Secrets

The CCPA requires the Attorney General to promulgate a regulation including, "Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights…" 1798.185(a)(3). Despite the mandatory nature of this requirement, to date, the Attorney General has not issued any draft regulations related to trade secrets and intellectual property rights. We request that, to comply with its obligations under the CCPA, the AG issue a regulation establishing an exception to the requirements of the CCPA to protect against violations of intellectual property rights and the disclosure of trade secrets. In so doing, we believe the Attorney General should take into consideration the proprietary nature of certain data, particularly internally generated or derived data, and the impact that may have on a business.

W348-14

IA suggests the addition of new text to the CCPA regulations stating:

§ 999.319 Intellectual Property and Trade Secrets
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 the business's intellectual property rights or result in the disclosure of trade secrets.

5. Calculating Value Of Data

Subsection 999.337(b) of the Second Set allows businesses to determine the value of consumer data based on customer segments for "consumers," which is defined to be California residents, or "natural persons in the United States." The "United States" is a recent addition and welcome. As recommended above, IA believes that Section 999.337 should be deleted from the regulations. However, if it is retained, this provision would be further improved by not requiring businesses to segment their customers at all and allow global determinations of the value of consumer data. For many services, not only is segmentation of their audiences potentially difficult, but for online services that operate on a global scale the vast majority of a business' user base may be outside the United States. Thus, the value of any single consumer's data can only be understood by looking at the value with respect to the whole of the global user base.

W348-15

Message

From: Monticollo, Allaire [redacted]
Sent: 3/27/2020 9:25:32 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Signorelli, Michael A. [redacted]
Subject: Joint Ad Trade Comments on Second Set of Modifications to the Proposed CCPA Regulations
Attachments: Joint Ad Trade Comments on Second Set of Modifications to Proposed CCPA Regulations.pdf

Dear Attorney General Becerra:

Please find attached joint comments from the following advertising trade associations on the content of the second set of modifications to the proposed regulations implementing the California Consumer Privacy Act: the American Advertising Federation, the American Association of Advertising Agencies, the Association of National Advertisers, the Digital Advertising Alliance, the Interactive Advertising Bureau, 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

****
This electronic mail transmission may contain confidential or privileged information. If you believe you have received this message in error, please notify the sender by reply transmission and delete the message without copying or disclosing it.
****

March 27, 2020

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

RE: Second Set of 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 proposed regulation included in 999.315(d) of the March 11, 2020 release of the second set of modifications to the text of the proposed regulations implementing the California Consumer Privacy Act ("CCPA").[1] This requirement exceeds the scope of the OAG's ability to regulate in conformance with the CCPA, runs afoul of free speech rights inherent in the United States Constitution, and impedes the ability of consumers to exercise granular choices in the marketplace. We ask that it be struck or modified per the below comment.

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.[2] We and our members strongly support the underlying goals of the CCPA, and we believe consumer privacy deserves meaningful protections in the marketplace. However, as discussed in our previous submissions and in the sections that follow below, the draft regulations implementing the law could be updated to better enable consumers to exercise meaningful choices and to help businesses in their efforts to continue to provide value to California's consumers and its economy.[3]

Despite businesses' best efforts to develop compliance strategies for the CCPA, current events coupled with the unfinalized nature of the draft rules stand in the way of entities' earnest work to facilitate compliance with the law. As we have discussed in our prior submissions, the draft rules' onerous terms concerning global controls and browser settings stand to impede consumer choices as well as access to various products, services, and content in the digital ecosystem. More urgently, the novel coronavirus known as COVID-19 has shaken businesses' standard operating procedures as well as the development of policies, processes, and systems for the CCPA. In this period of crisis facing the world-at-large, entities should be focused on dedicating funds, time, and efforts to supporting their employees and the response to

---

[1] *See* California Department of Justice, *Notice of Second Set of Modifications to Text of Proposed Regulations* (Mar. 11, 2020), located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-second-mod-031120.pdf?.

[2] IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at http://www.ana.net/getfile/23045.

[3] Our organizations have submitted joint comments throughout the regulatory process on the content of the OAG's 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; *Revised Proposed Regulations Implementing the California Consumer Privacy Act*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-15-day-comments-022520.pdf at CCPA_15DAY_000554 – 000559.

the coronavirus outbreak rather than diverting resources to prepare for an ever-evolving set of regulations under the CCPA. Therefore, we support the request made earlier this month by a group of sixty-six (66) trade associations, organizations, and companies to your office asking you to delay enforcement until January 2, 2021.[4] W349-1

Our members are committed to offering consumers robust privacy protections while simultaneously maintaining their ability to support California's employment rate and its economy in these unprecedented times as well as access to ad-funded news. We believe a regulatory scheme that enables strong individual privacy protections alongside continued economic development and advancement will best serve Californians. The suggested updates we offer in this letter would improve the CCPA implementing regulations for Californians as well as the global economy.[5]

I. Give Businesses the Option to Honor Browser Settings and Global Controls

The revised proposed rules require businesses that collect personal information from consumers online to treat user-enabled global controls, such as a browser plugin or setting, device setting, or other mechanism that purports to carry signals of the consumer's choice to opt out of the sale of personal information, as a valid request submitted for that browser, device, or consumer.[6] This requirement exceeds the scope of the OAG's authority to regulate pursuant to the CCPA, runs afoul of free speech rights inherent in the United States Constitution, and impedes consumers of the ability to exercise granular choices in the marketplace. For these reasons, we ask the OAG to remove this requirement, or, at a minimum, to give businesses the option to honor such controls or decline to honor such settings if the business offers another, equally effective method for consumers to opt out of personal information sale.

a. The Browser Setting and Global Control Mandate Exceeds the OAG's Regulatory Authority Pursuant to the CCPA

W349-2

Requiring businesses to honor such controls and browser settings is an obligation that has no support in the text of the CCPA itself and extends far beyond the intent of the California Legislature in passing the law. Under California administrative law, when an agency is delegated rulemaking power, rules promulgated pursuant to that power must be "within the lawmaking authority delegated by the Legislature," and must be "reasonably necessary to implement the purposes" of the delegating statute.[7] The CCPA gives the OAG power to "adopt regulations to further the purposes of [the CCPA]," but not to adopt regulations that contravene the framework set up by the Legislature when it passed the law.[8]

The CCPA was plainly structured to provide consumers with the right to opt out of sales of personal information.[9] However, the requirement to respect the proposed controls and browser settings effectively transforms the CCPA's opt-out regime into an opt-in regime by enabling intermediaries to set opt-out signals through browsers that apply a single signal across the entire Internet marketplace. Individual businesses will consequently be forced to ask consumers to opt in after receiving a global opt-out signal set by an intermediary, thereby thwarting the granular opt-out structure the California Legislature purposefully enacted in passing the CCPA. The OAG's regulation mandating that businesses

---

[4] *Joint Industry Letter Requesting Temporary Forbearance from CCPA Enforcement* (Mar. 20, 2020), located at https://www.ana.net/getfile/29892.

[5] These comments are supplementary to filings that may be submitted separately and individually by the undersigned trade associations.

[6] Cal Code Regs. tit. 11, § 999.315(d) (proposed Mar. 11, 2020).

[7] *Western States Petroleum Assn. v. Bd. of Equalization*, 304 P.3d 188, 415 (Cal. 2013) (quoting *Yamaha Corp. of America v. State Bd. Of Equalization*, 960 P.2d 1031 (Cal. 1998)).

[8] Cal. Civ. Code § 1798.185.

[9] *Id.* at § 1798.120.

obey such controls and browser signals therefore exceeds the scope of the OAG's authority to issue regulations under the CCPA.

The requirement to obey such 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 for browser signals or global controls. Additionally, the California Legislature considered a similar requirement in 2013 when it amended the California Online Privacy Protection Act ("CalOPPA"), 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.[10] The Legislature did not intend to institute a requirement to mandate global controls or browser signals when it amended CalOPPA in 2013, and it similarly did not intend to do so when it passed the CCPA in 2018. The obligation to honor such signals in the draft rules therefore thwarts legislative intent and is an impermissible exercise of the OAG's ability to issue regulations under the law.

b. The Browser Setting and Global Control Mandate Contravenes Constitutional Rights to Free Speech

W349-2 (cont.)

The OAG's proposed rule regarding such controls and browser signals violates the First Amendment to the United States Constitution by converting the CCPA's opt-out structure into a de facto opt-in structure and by improperly restricting free speech. Businesses' dissemination of the data they collect constitutes constitutionally protected commercial speech.[11] A regulation restricting commercial speech is unconstitutional unless the state has a substantial interest in restricting this speech, the regulation directly advances that interest, and the regulation is narrowly tailored to serve that interest.[12] While there may be a substantial state interest in protecting consumer privacy,[13] the OAG's directive to respect such controls and browser settings does not advance the government's substantial interest. Moreover, this rule is not narrowly tailored to advance such an interest. The regulatory requirement therefore violates the First Amendment.

Commercial speech is entitled to protections under the United States Constitution. Regulations that provide ""ineffective or remote support for the government's purpose'" impermissibly burden constitutional protections afforded to commercial speech.[14] The wide-ranging opt-out structure set forth by the California Legislature and the OAG particularly focus on a consumer's relationship with an individual business. This structure enables consumers to express opt-out preferences in the context of their unique relationships with individual entities. By contrast, the global controls mandate obligates businesses to figure out consumers' individual preferences regarding data disclosures from a singular browser setting. Moreover, requiring businesses to defer to such controls as a way to understand consumers' true preferences is less effective and less direct than the opt-out methods employed by the rest of the OAG's regulations. If the state's interest is in stopping the disclosure of specific data that a consumer wishes to restrict from sale, such a proposal does not adequately further this aim. It provides no way for businesses

---

[10] *See Assembly Committee on Business, Professions and Consumer Protection*, Hearing Report on AB 370 (Cal. 2013) (Apr. 16, 2013), located at https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201320140AB370# ("According to the California Attorney General's Office, 'AB 370 is a transparency proposal – not a Do Not Track proposal. When a privacy policy discloses whether or not an operator honors a Do Not Track signal from a browser, individuals may make informed decisions about their use of the site or service.')

[11] *See Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001); *Boetler v. Advance Magazine Publishers Inc.*, 210 F. Supp. 3d 579, 597 (S.D.N.Y. 2016).

[12] *Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001).

[13] *Verizon Northwest, Inc. v. Showalter*, 282 F. Supp. 2d 1187, 1192 (W.D. Wash.).

[14] *Id.* (quoting *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980)).

to divine that a consumer wishes to keep personal information within the confines of a specific business relationship, and instead compels businesses to guess at consumers' preferences from an indirect signal that may not accurately reflect a consumer's wishes.

In addition, the AG's proposed rule is not narrowly tailored to serve the state's interest. Instead, it senselessly restricts the commercial speech of businesses without supporting the efficacy of the existing opt-out framework. Narrowly tailored regulations are not disproportionately burdensome. Additionally, they must "signify a careful calculation of the costs and benefits associated with the burden on speech imposed."[15] The existing opt-out regime implemented by the California Legislature offers businesses more exact information about specific, granular preferences of individual consumers than the global controls mandate. The global controls requirement serves no purpose that is not already served by existing opt-out rules in the draft regulations and the law itself, and it could potentially restrict speech by requiring businesses to act on inaccurate information about a consumer's individual preferences.

The proposed regulations note that businesses may contact consumers to ascertain their true intent regarding personal information sales if a global control conflicts with a choice the consumer individually set with the business. However, the rules require the business to defer to the global controls in the meantime, thus mandating a potentially incorrect expression of user preferences at the expense of specific choices the consumer indicated to the contrary. In addition, businesses bear the burden of ascertaining the consumer's true intent after receiving a global signal that does not align with an individual consumer's preferences. In contrast, the opt-out privacy framework set forth in the CCPA itself and bolstered by the draft rules is both more precise and less burdensome. It enables businesses to assess specific preferences of users in the context of each unique consumer relationship, and it restricts commercial speech only if that speech is known to contravene consumer preferences. The global controls mandate consequently does not further the goals of the existing framework, but it does needlessly restrict commercial speech. The global controls rule therefore does not pass constitutional muster because it burdens commercial speech without appropriately balancing those burdens with benefits. W349-2 (cont.)

c. The Browser Setting and Global Control Mandate Impedes Consumer Choice

The revised proposed rules' imposition of a requirement to honor such controls would result in broadcasting a single signal to all businesses, opting a consumer out from the entire online ecosystem. This requirement would obstruct consumers' access to various products, services, and content that they enjoy and expect to receive, and it would thwart their ability to exercise granular, business-by-business selections about entities that can and cannot sell personal information in the digital marketplace.

In the March 11, 2020 updates to the draft rules, the OAG removed the requirement for a consumer to "affirmatively select their choice to opt-out" and the requirement that global controls "shall not be designed with any pre-selected settings."[16] The removal of these provisions entrench intermediaries in the system and will advantage certain business models over others, such as models that enable direct communications between consumers and businesses. It will also enable intermediaries to set *default* signals through browsers without consumers having to approve of them before they are set. This outcome risks causing businesses to take specific actions with respect to consumer data that the consumer may not want or intend. The OAG should take steps to ensure that default privacy signals may not be set by intermediaries without the consumer approving of the signals set and the choices they relay to businesses.

Moreover, the draft rules do not address how businesses should interpret potentially conflicting signals they may receive directly from a consumer and through a global control or a browser setting. For

[15] *Id.* at 1194.
[16] Cal. Code Regs. tit. 11, § 999.315(d)(2) (proposed Mar. 11, 2020).

example, if a business directly receives a consumer's permission to "sell" personal information, but later receives a global control signal through a browser set by default that indicates the consumer has opted out of such sales, which choice should the business follow? The CCPA itself allows businesses to contact consumers asking them to opt in to personal information sales after receiving opt-out signals only once in every twelve month period.[17] As such, the business's ability to communicate with the consumer to ascertain their true intentions may be limited despite the draft regulations' statement that a business may notify consumers of conflicts between setting and give consumers the choice to confirm the business-specific setting.

W349-2 (cont.)

To preserve consumers' ability to exercise granular choices in the marketplace, to keep the regulations' requirements in line with constitutional requirements and legislative intent in passing the CCPA, and to reduce entrenchment of intermediaries and browsers that have the ability to exercise control over settings, we ask the OAG to remove the requirement to obey such 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.

* * *

Thank you for the opportunity to submit input on the content of the revised proposed regulations implementing the CCPA. 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

Lou Mastria
Executive Director
Digital Advertising Alliance

[17] Cal. Civ. Code § 1798.135(a)(5).

Message

From: Monticollo, Allaire [redacted]
Sent: 3/20/2020 12:43:54 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Jaffe, Dan [redacted]
Subject: Joint Industry Letter Requesting a Delay in CCPA Enforcement - Updated 3.20.2020
Attachments: Joint Industry Letter Requesting a Delay in CCPA Enforcement - Updated 3.20.2020.pdf

Dear Attorney General Becerra:

Please find attached an updated letter from sixty-six (66) trade associations, organizations, and companies requesting that your office delay its enforcement of the California Consumer Privacy Act until January 2, 2021.

If you have any questions, please feel free to contact Dan Jaffe 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

****
This electronic mail transmission may contain confidential or privileged information. If you believe you have received this message in error, please notify the sender by reply transmission and delete the message without copying or disclosing it.
****

** UPDATED **


ANA
CalChamber
HR Expert & Business Advocate
AIMS
ACCLAMATION INSURANCE MANAGEMENT SERVICES
AdvaMed
Advanced Medical Technology Association
ALLIANCE FOR AUTOMOTIVE INNOVATION
ALLIED MANAGED CARE INCORPORATED
AAF
ACLI
Financial Security...for Life.
American Property Casualty Insurance Association
INSURING AMERICA
apci.org
ACLHIC
acp
association of claims professionals
MPA
THE ASSOCIATION OF MAGAZINE MEDIA
BizFed
Los Angeles County Business Federation
Strengthening the Voice of Business Since 2008
CALASIAN
chamber of commerce
CAPA
CALIFORNIA ATTRACTIONS AND PARKS ASSOCIATION
cabbi
California Business Properties Association
CCTA
California Cable & Telecommunications Association
California
CREDIT UNION LEAGUE
CALIFORNIA FSA
CALIFORNIA FINANCIAL SERVICES ASSOCIATION
cga
CALIFORNIA HOTEL & LODGING ASSOCIATION
CLTA
California Land Title Association
CNCDA
California New Car Dealers Association
CNPA
CALIFORNIA RESTAURANT ASSOCIATION
CALIFORNIA RETAILERS ASSOCIATION
CALIFORNIA TRUCKING ASSOCIATION
We drive for a living. Safety is our priority.
CardCoalition
A STATEWIDE ORGANIZATION
CIVIL JUSTICE
ASSOCIATION OF CALIFORNIA
Coalition of Small & Disabled Veteran Businesses
CompTIA
CDIA
CONSUMER DATA INDUSTRY ASSOCIATION
eta
ELECTRONIC TRANSACTIONS ASSOCIATION
ESPC
Email Sender & Provider Coalition
Innovative Lending Platform Association
FELD
ENTERTAINMENT
FLASHER BARRICADE ASSN.
Hotel Association of Los Angeles
insights
ASSOCIATION
IRI
Insured Retirement Institute
iab.
INTERNET COALITION
ICI
INVESTMENT COMPANY INSTITUTE
LONG BEACH HOSPITALITY ALLIANCE
MOTION PICTURE ASSOCIATION - AMERICA
NAMIC
NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES
SHAPING OUR MUTUAL FUTURE
National Business Coalition on E-Commerce and Privacy
NMMA
National Marine Manufacturers Association
NPRC
National Payroll Reporting Consortium
NEWS MEDIA ALLIANCE
NFIB
aaa
Out of Home Advertising Association of America
PIFC
pmi
PLUMBING MANUFACTURERS INTERNATIONAL
SBCA
sifma
SOUTHERN CALIFORNIA EDISON
An EDISON INTERNATIONAL Company
SILICON VALLEY LEADERSHIP GROUP
TECHNET
THE VOICE OF THE INNOVATION ECONOMY
the toy association
Inspiring Generations of Play
ups
VICA
SINCE 1949

**** UPDATED ****

March 20, 2020

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

RE: Request for Temporary Forbearance from CCPA Enforcement

Dear Attorney General Becerra:

The undersigned trade associations, companies, and organizations collectively represent a broad cross-section of the United States business community spanning various industries including advertising and marketing, magazine publishing, Internet and online services, financial services, package delivery, cable and telecommunications, transportation, retail, utilities, real estate, insurance, entertainment, auto, technology, and others. Together, we include thousands of companies that do business in California, employ millions of residents in the state, and deliver goods and services that benefit and provide substantial value to the economy and consumers across California and the country.

We strongly support the underlying purpose and goals of the California Consumer Privacy Act ("CCPA"). We believe consumer privacy is an important value that deserves meaningful protections in the marketplace. However, we are concerned that given current events and the presently unfinished status of the regulations implementing the CCPA, businesses will not have the operational capacity or time to bring their systems into compliance with the final regulatory requirements by July 1, 2020.[1] We therefore respectfully request that you forebear from enforcing the CCPA until January 2, 2021 so businesses are able to build processes that are in line with the final regulations before they may be subject to enforcement actions for allegedly violating the law's terms. W350-1

I. The Current Health Crisis Hinders Businesses' Attempts to Develop Processes for CCPA Compliance

Recent events have encumbered businesses in their earnest efforts to operationalize the draft rules prior to July 1, 2020. The World Health Organization recently announced that the spread of the novel coronavirus known as COVID-19 has risen to the level of a global pandemic, and President Trump has declared that the United States is under a state of national emergency due to the outbreak.[2] The undersigned organizations employ millions of individuals who are

[1] "The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 20202, whichever is sooner." Cal. Civ. Code § 1798.185(c).

[2] World Health Organization, *WHO characterizes COVID-19 as a pandemic* (Mar. 11, 2020), located at https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen; White House, *Proclamation on Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19)*

faced with this crisis and are doing their best to manage their personal and professional lives in the face of uncertain times. Many companies have instituted mandatory work-from-home measures to limit community spread of the virus, meaning that the individuals who are responsible for creating processes to comply with CCPA are not present in the office to undertake such tasks. Developing innovative business procedures to comply with brand-new legal requirements is a formidable undertaking on its own, but it is an especially tall order when there are no dedicated, on-site staff available to build and test necessary new systems and processes.

The public health crisis brought on by COVID-19 juxtaposed with the quickly approaching enforcement date for the CCPA places business leaders in a difficult position. They are forced to consider tradeoffs between decisions that are best for their employees and the world-at-large and decisions that may help the organizations they lead avoid costly and resource intensive enforcement actions. Now is not the time to threaten business leaders with premature CCPA enforcement lawsuits, particularly when the legal regime is not yet in its final form. A temporary deferral in enforcement of the CCPA would relieve many pressures and stressors placed on organizations due to COVID-19 and would better enable business leaders to make responsible decisions that prioritize the needs and health of their workforce over other matters.

W350-1
(cont.)

II. Businesses Need Time to Implement Final CCPA Regulatory Requirements

The draft regulations interpreting the CCPA are still not settled and likely will not be for some time. Equally importantly, they contain a number of requirements and implementation obligations that are not present in the text of the law itself. These new mandates will materially impact how the CCPA is operationalized and will place extensive strain on companies attempting to achieve full compliance before enforcement may begin. Creating procedures and processes to comply with a law like the CCPA takes time, testing, and significant planning and foresight. Even in the most favorable of circumstances, presuming that companies will be able to achieve full compliance with brand-new substantive obligations within mere months of those obligations becoming final is an unrealistic and daunting expectation.

Because the CCPA became effective on January 1, 2020, the draft rules' new requirements beg the question of how the regulations' mandates will impact the baseline obligations that became operative when the CCPA went into effect. It is unclear whether businesses will be held accountable for their failure to abide by entirely new regulatory requirements before they became final or were even proposed. In addition, the lack of time for companies to implement the CCPA prior to enforcement may engender incongruous compliance mechanisms that will look and feel different to consumers on the receiving end of CCPA rights requests. The CCPA's incomplete legal regime risks confusing and frustrating consumers with multiple inconsistent processes for submitting rights requests, thereby potentially discouraging them from submitting such requests altogether. While we understand that your office is working to finalize the draft rules as quickly as reasonably possible, precious time is slipping away from businesses in their efforts to develop consistent and workable compliance processes for consumers before enforcement may begin.

Outbreak (Mar. 13, 2020) located at https://www.whitehouse.gov/presidential-actions/proclamation-declaring-national-emergency-concerning-novel-coronavirus-disease-covid-19-outbreak/.

Moreover, the content of the draft rules continues to evolve, and with each update made by the Office of the Attorney General, businesses' compliance responsibilities materially and substantially change. With less than four months before enforcement is scheduled to start, your office has revealed a second set of modifications to the proposed rules and has initiated a third comment period for interested parties to submit input on the content of the latest changes.[3] This third comment period will further delay the ultimate finalization of the rules until at least the end of April 2020, leaving very little time for entities to understand what is required of them under the final regulatory scheme and to build those requirements into their business processes. W350-1 (cont.)

The limited and rapidly dwindling time before CCPA enforcement may begin will place business in a compromising position. Without final regulatory requirements, businesses will be unable to make operational changes to their systems with any certainty that such changes will be compliant with the final form of the law. This reality will significantly delay businesses in crafting their ultimate CCPA compliance programs. Businesses should have a reasonable period of time to understand and implement the final regulations before being subject to enforcement.

* * *

The undersigned companies, organizations, and trade associations fully support California's efforts to provide consumers enhanced privacy protections, but the ever-evolving nature of the CCPA's proposed rules, especially in light of the current global crisis, makes the current enforcement date of July 1, 2020 a problematic deadline for both businesses and consumers. Though the CCPA commands the Office of the Attorney General to refrain from bringing an enforcement action before July 1, 2020, the statute does not restrict the office from providing an appropriate period of additional time for businesses to implement the final regulations before enforcement begins. As a result, we ask that you delay enforcement of the CCPA until January 2, 2021. This short forbearance will allow businesses to absorb the shock to the system presented by the current health crisis and will give businesses the time they need to understand and effectively operationalize the rules helping ensure consumers have consistent access to the rights afforded under the new law.

Thank you for your consideration of this request.

Sincerely,

Association of National Advertisers (ANA)
CalChamber
Acclamation Insurance Management Services
Advanced Medical Technology Association (AdvaMed)
Alliance for Automotive Innovation
Allied Managed Care Incorporated
American Advertising Federation (AAF)
American Association of Advertising Agencies (4As)

[3] *California Department of Justice*, Notice of Second Set of Modifications to Text of Proposed Regulations (Mar. 11, 2020), located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-second-mod-031120.pdf?.

The American Council of Life Insurers (ACLI)
American Property Casualty Insurance Association (APCIA)
Association of California Life & Health Insurance Companies (ACLHIC)
Association of Claims Professionals (ACP)
The Association of Magazine Media (MPA)
BizFed – Los Angeles County Business Federation
California Asian Pacific Chamber of Commerce
California Attractions and Parks Association (CAPA)
California Association of Boutique and Breakfast Inns
California Association of Licensed Investigators
California Business Properties Association (CBPA)
California Cable & Telecommunications Association (CCTA)
California Credit Union League (CCUL)
California Financial Services Association
California Grocers Association (CGA)
California Hotel & Lodging Association
California Land Title Association (CLTA)
California New Car Dealers Association (CNCDA)
California News Publishers Association (CNPA)
California Restaurant Association
California Retailers Association (CRA)
California Trucking Association (CTA)
Card Coalition
Cemetery and Mortuary Association of California
Civil Justice Association of California (CJAC)
Coalition of Small & Disabled Veteran Businesses
CompTIA
Consumer Data Industry Association (CDIA)
Electronic Transaction Association (ETA)
Email Sender & Provider Coalition (ESPC)
Feld Entertainment
Flasher Barricade Association
Hotel Association of Los Angeles
Innovative Lending Platform Association (ILPA)
Insights Association
Insured Retirement Institute (IRI)
Internet Coalition (IC)
Interactive Advertising Bureau (IAB)
Investment Company Institute (ICI)
Long Beach Hospitality Alliance
Motion Picture Association – America
National Association of Mutual Insurance Companies (NAMIC)
National Business Coalition on E-Commerce and Privacy
National Marine Manufacturers Association (NMMA)
National Payroll Reporting Consortium
News Media Alliance

NFIB California
Out of Home Advertising Association of America (OAAA)
Personal Insurance Federation of California (PIFC)
Plumbing Manufacturers International
Satellite Broadcast Communications Association (SBCA)
Securities Industry and Financial Markets Association (SIFMA)
Southern California Edison
The Silicon Valley Leadership Group
TechNet
The Toy Association
United Parcel Service (UPS)
Valley Industry & Commerce Association

Message

From: Monticollo, Allaire [redacted]
Sent: 3/5/2020 9:52:44 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Signorelli, Michael A. [redacted]
Subject: Letter to Attorney General Becerra Regarding ANA Guidance for CCPA Compliance
Attachments: Letter to Attorney General Becerra Regarding ANA Guidance for CCPA Compliance(48727724.1).pdf

Flag: Follow up

Dear Attorney General Becerra:

Please find attached a letter from the Association of National Advertisers (ANA) asking you to confirm particular guidance that members of the ANA set forth to comply with Cal. Civ. Code 1798.110 under the California Consumer Privacy Act. ANA requests your confirmation of this interpretation or other guidance from you by March 13, 2020.

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

****
This electronic mail transmission may contain confidential or privileged information. If you believe you have received this message in error, please notify the sender by reply transmission and delete the message without copying or disclosing it.
****

March 5, 2020

California Attorney General Xavier Becerra
California Department of Justice
Office of the Attorney General
ATTN: Privacy Regulations Coordinator
300 South Spring St., First Floor
Los Angeles, CA 90013

Request for Guidance Under the California Consumer Privacy Act

Dear Attorney General Becerra:

The Association of National Advertisers ("ANA"), a trade association serving the nation's largest leading consumer facing companies, through this letter seeks your confirmation regarding particular guidance that members of the ANA set forth to comply with Cal. Civ. Code 1798.110 under the California Consumer Privacy Act ("CCPA").[1] We request your confirmation of this interpretation or for other guidance from you by March 13, 2020.

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.

Our members have for decades sought to improve consumer privacy practices and give consumers advertising choices. For nearly two years, our members have worked to enhance and develop new processes, policies, and systems with the goal of furthering compliance with the CCPA. To help support efforts to enhance consumer privacy and businesses in meeting their CCPA obligations, a working group of our members convened to develop consistent approaches to complying with the CCPA.

In one of the areas where we developed guidance, the law and proposed regulations remain unclear. Under section 1798.110 of the CCPA, a consumer may request that a business disclose to them personal information that the business has collected about the consumer. For most businesses, providing access is both an important and costly aspect of complying with CCPA. Providing access presents challenges because many businesses do not maintain information about an individual in a centralized way, so complying with access requests often involves a manual process of searching through various storage locations to build a centralized

W351-1

[1] "Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title." Cal. Civ. Code § 1798.155(a).

collection of data that can be provided to a consumer. Against this backdrop, it is critical that businesses have clarity around what data should be disclosed under CCPA.

As further described in this letter and the included exhibit, the ANA guidance states that a business should return to the consumer the specific pieces of personal information it has collected about the consumer, but not the personal information it independently generated or derived from such data. This approach reflects a logical reading of the law and aligns with consumer expectations as to the types of data that could be "collected" from and sold about them. This interpretation also protects the intellectual property of businesses in their inferences and provides clear guidance that allows them to practically provide information about consumers that is readily understandable.

Significantly, a broader interpretation that would require the disclosure of inferences or decisions made tied to a consumer would in many cases infringe on the intellectual property of businesses. Companies compete on providing consumers with the best consumer experience, including pricing, customer support, product offering scope and many other factors. In the digital age, consumer experience is driven by trade secrets regarding computing and efficiencies. The CCPA specifically recognizes and enumerates that information that amounts to intellectual property or a business's trade secrets should be exempt from the law. The statute instructs your office to "establish… any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights…."[2]

W351-1
(cont.)

The ANA effort to develop consistent approaches to CCPA compliance culminated in the enclosed guidance for members, which helps members understand CCPA's use of the term "collect" as it relates to providing consumers access to personal information, attached hereto as **Exhibit A**. As we explain, we believe that businesses' *internally-generated* data are not required to be disclosed in response to a consumer access request for specific pieces of information because such information was not "collected" consistent with the law's definition of the term. In the instances where a business receives or buys inferred data from another entity, the business should include such data as part of its response to a verified consumer access request. Additionally, if a business sells its proprietary inferences to a third party or discloses such inferences for a business purpose, the business should disclose that it has sold and/or disclosed the category of inferences pursuant to the CCPA requirement to provide the categories of personal information that the business sold and disclosed about the consumer for a business purpose.[3] This reading of the CCPA is supported by the text of the law itself as well as your office's recent revisions to the regulations implementing the CCPA.

In today's day and age, nearly every entity—from corporations and nonprofits to sole proprietorships and start-ups—processes in some manner information about individuals and generates internal data, like internal inferences, which would be both time-consuming to collect and of little privacy value to consumers. For example, businesses generate information when they validate a consumer's name and customer relationship. Businesses also may generate lists of, or models that enable identification of, products and services that they may want to

[2] *Id.* at § 1798.185(a)(3).
[3] *Id.* at §§ 1798.115(a)(2), (3).

recommend to people in the future. Or they may maintain information to protect against information security threats, fraudulent activity, or noncompliance with their policies. These records are generally not maintained in a centralized consumer profile, and so responding to access requests typically requires businesses to search for and collect them in a centralized way. Likewise, because generated data is commonly not maintained in a human-readable way, both for computing efficiency and to protect the consumer's privacy, providing access to them may not provide meaningful information to consumers.

CCPA appropriately scoped the access obligations to "collected" data to avoid imposing undue burden on California businesses and ensure the data provided to consumers is meaningful and intelligible. If the CCPA were to require businesses to return *all* generated data, including inferences in response to a consumer access request, consumers would be burdened by the delivery of excessively detailed and potentially incomprehensible information, including internally-generated inferences—basic computing connections, like validating a name, that businesses must undertake in order to sustain day-to-day operations. Businesses ultimately would have difficulty or impossibility in complying. A business's provision of this data to a consumer would do nothing but hinder the consumer's ability to access meaningful information about the information collected from or about the consumer, thereby thwarting the aim of the CCPA to provide consumers with enhanced transparency. W351-1 (cont.)

The approach listed in the enclosed interpretation represents a logical reading of the law that takes into account consumer desires as well as practical realities. We request that you confirm this interpretation is satisfactory to you and your office so that our members can ensure that they are compliant with this section of the law. Please contact us with any questions.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
[redacted]

EXHIBIT A

CCPA GUIDANCE
PERSONAL INFORMATION COLLECTION AND INFERENCES

This guidance considers whether business-generated, modeled, and inferred data businesses create, receive, and sell or disclose about consumers are subject to an access request under the California Consumer Privacy Act ("CCPA").[1] While not clear under the text of the law, a reasonable reading of the law, consumer expectations, business proprietary information, and operational practicalities suggest that internally-generated inference-related data should not be returned to a consumer under the CCPA's obligation to provide the categories and specific pieces of personal information collected about the consumer because these sections of the CCPA are tied to the *collection* of personal information, not just any personal information held about a consumer.[2] However, if a business "collects" inference-related data, such as receiving or buying inferred data from another entity, the business should include such data as part of its response to a verified consumer access request. Additionally, if a business sells its proprietary inferences to a third party or discloses such inferences for a business purpose, the business should disclose that it has sold and/or disclosed the category of inferences pursuant to the CCPA requirement to provide the categories of personal information that the business sold and disclosed about the consumer for a business purpose.[3]

I. Inferences Businesses Create Themselves Are Not "Collected." Businesses create modeled data, business-generated data, and inferences about consumers from the personal information they collect about consumers in the regular course of business. A reasonable interpretation of the CCPA is that this inferred data need not be returned to a consumer in the context of a CCPA access request for information collected by the business because the inferences are created by the business itself and are not "collected".

"Personal information" under the CCPA is "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."[4] Such information explicitly includes "[i]nferences drawn from any [consumer personal] information to create a profile about a consumer reflecting the consumer's preference, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[5] However, the CCPA access right requires a business to give a consumer access to the "categories of personal information it has *collected* about that consumer" and the "specific pieces of personal

---

[1] Cal. Civ. Code §§ 1798.100, 110, 115, 130. Proposed CCPA regulations refer to the access right as a "request to know." Cal. Code Regs. tit. 11, § 999.301(q) (proposed Feb. 10, 2020). When the California Attorney General most recently updated the draft regulations, he added the term "collect" into the definition of "request to know" to conform the regulatory language with the text of the CCPA. *Id.* This change further bolsters the analysis that only information that is *collected* must be returned in response to a consumer access request.
[2] Cal. Civ. Code §§ 1798.110(a)(1), (5).
[3] *Id.* at §§ 1798.115(a)(2), (3).
[4] *Id.* at § 1798.140(o)(1).
[5] *Id.* at § 1798.140(o)(1)(K).

information it has *collected* about a consumer."[6] The CCPA defines "collects" as "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior."[7] This definition suggests that the CCPA requirement to give consumers access to the categories and specific pieces of personal information a business has collected about a consumer does not include the inferred data a business may have created from the personal information the business receives in its normal course of business.

A reasonable interpretation of the term "collect" is that it does not include modeled data, inferred data, or other business-generated data, because the definition implies that a business *received* data from the consumer or a third party and did not generate the data on its own. The definition of "collect" suggests that to engage in collection, the personal information must already have existed or have been generated by an entity and obtained by the covered business. The descriptive verbs that define "collect" do not appear to include the concept of generating new data from personal information that a business has already accumulated. As a result, a reasonable interpretation under the law is that business-generated, modeled, and inferred data created from the personal information the business already possesses does not constitute "collection" of personal information under the CCPA. Because such inferences were made by the business itself and were not collected, under this reading the inferences need not be returned pursuant to the CCPA obligation to provide the categories and specific pieces of personal information collected about a consumer. Additionally, there are public policy reasons that support not providing such internally-generated inferences under the access right. For example, inferences may reveal information that is subject to intellectual property protection. Also, certain kinds of inferred data could be meaningless to consumers, and providing inferred data could result in an unreadable, unwieldly, or exceedingly voluminous access disclosure.

II. Inferences Businesses Receive from Another Business Are Collected. If a business receives inferred, modeled, or business-generated data from another business, such data would likely be subject to a CCPA access request served on the business because such information is now "collected" under the CCPA.[8] To "collect" personal information under the CCPA is to receive it by any means, including by receiving such personal information from other businesses. As such, any entity that "collects" inferred data from another business should return that data in response to a consumer's CCPA request pursuant to the CCPA requirement to provide the categories and specific pieces of personal information collected about a consumer.[9]

III. Inferences Businesses Sell or Disclose for a Business Purpose Are Subject to a CCPA Access Request. In addition to disclosing the categories and specific pieces of personal information the business has collected about a consumer, the CCPA requires a business also to provide a list of "[t]he categories of personal information that the business sold about the consumer…" and "[t]he categories of personal information that the business disclosed about the

[6] *Id.* at §§ 1798.110(a)(1), (5) (emphasis added).
[7] *Id.* at § 1798.140(e).
[8] *Id.* at §§ 1798.100, 110, 115, 130, 140(e).
[9] *Id.* at §§ 1798.110(a)(1), 110(a)(5), 140(e).

consumer for a business purpose" in response to a CCPA access request.[10] If a business sells the proprietary inferences, modeled, or business-generated data that it created internally to third parties or discloses such data for a business purpose, the business should disclose that it has sold or disclosed the category of inferences for a business purpose in a CCPA access response.

Because of the CCPA requirement to provide a list of the categories of personal information sold about a consumer and the categories of personal information disclosed about the consumer for a business purpose, it is possible that businesses may need to list inferences in the sale-related sections of a CCPA access response and not the collection-related sections of the response. For example, a business that creates its own modeled, business-generated, or inferred data about consumers internally and sells that data to other parties would not have to disclose that it has collected inferred data, but would have to disclose that it sold or disclosed the category of inferred data for a business purpose in a CCPA access response.[11]

[10] *Id.* at §§ 1798.115(a)(2), (3).
[11] *Id.* at §§ 1798.100, 110, 115, 130, 140(e).

Message

From: John Kabateck [redacted]
Sent: 3/27/2020 3:59:58 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Letter to Attorney General re: CCPA - Small Business Data Privacy Committee
Attachments: Letter to AG re revised regulations 3.27.20.pdf

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

Attached please find a 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 in response to the new unexpected costs from the COVID-19 pandemic with a request to delay enforcement. It is signed by twelve 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].

March 27, 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:

Last month, the Small Business Data Privacy Committee provided our comments regarding the Revised Proposed Regulations for the California Consumer Privacy Act (CCPA). In that letter we expressed our support for consumer privacy protections and our support for the improvements contained in the first amended regulations. We also expressed our continuing concern about the costs of implementing the regulations and the lack of clarity that remained in many aspects of the law and regulations. Given the current COVID-19 crisis, we joined other business organizations in requesting that you delay enforcement until January 1, 2021.

The comments below reflect our surprise and concern that some of the regulations have backtracked. Rather than making compliance easier and reducing regulatory burdens in this period of crisis, the new draft regulations add more confusion. More urgently, they fail to address the fact that owners of most small business enterprises have been ordered to shelter in place to contain the spread of COVID-19 and cannot hire the lawyers and technology services they need to comply with the CCPA even if they are able to financially weather the crisis.

We respectfully request that the Attorney General withdraw the proposed regulations, consider the impact of the crisis on small business, and work with businesses that are required to comply to develop regulations that will facilitate compliance. We renew our request that you delay enforcement until January 1, 2021.

W352-1

Below are our comments on the second amended regulations.

First, we support the clarifications in the notice requirements but are concerned that the notice requirements in general require a costly and complex process for sorting out information that small business cannot afford (and that our customers are not requesting). Given that there can always be future modifications, we ask that in this environment you consider the burden of their totality and minimize the notice requirements that business must meet. W352-2

Second, regarding potential consumer requests, the new regulations eliminate the guidance for determining the data that is considered personal information. In discussing privacy with our customers, those concerned about privacy do not want their personal information shared but they are not asking for all data to be completely restricted. In fact, they utilize and rely on services that rely on IP addresses and other data that does not identify the consumer. The previous draft regulations provided that IP addresses that do not link to a person or household would not be "personal information." We request that the AG include the more restrictive guidance from the previous version of the final regulations. W352-3

Third, the Small Business Data Privacy Committee is concerned with the increased requirements for disclosures of sources from which a business collects personal information or the need to identify business or commercial purpose for collecting and selling the personal information. We are unclear whether these requirements will be imposed on small business. But we are concerned, especially in a post COVID-19 business environment, that internet advertising which we heavily rely upon will be degraded unnecessarily by these and other requirements. W352-4

Finally, we support the increase in the threshold that requires a business that buys, sells, receives, or shares the personal information to maintain and report certain data from four to 10 million customers. The 10 million threshold will narrow the number of smaller businesses required to comply. W352-5

Thank you for your consideration of our comments. We are happy to elaborate on any of the above.

Sincerely,

Coalition members:

Latin Business Association
Los Angeles County Business Federation (BizFed)
California Small Business Association
Coalition of Small & Disabled Veteran Businesses
California Hispanic Chambers of Commerce
California Asian Pacific Chamber of Commerce
National Federation of Independent Business, CA
Small Business California
Valley Industry & Commerce Association (VICA)
Flasher Barricade Association
Allied Managed Care
Acclamation Insurance Management Services

Message

From: Tom Lee [f[redacted]
Sent: 3/24/2020 11:25:31 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Kathleen Lu [redacted]
Subject: Mapbox comments re CCPA second set of modifications
Attachments: Mapbox - CCPA Rulemaking Comments Mar 27 2020.pdf

Attached, please find comments regarding the most recent revisions to the draft regulations concerning the California Consumer Privacy Act.

50 Beale Street, Ninth Floor
San Francisco, CA 94105

27 March 2020

The following comments are submitted on behalf of Mapbox, a leading provider of map and location services, in response to a call for comments by the California Office of the Attorney General (OAG) regarding rulemaking associated with the California Consumer Privacy Act of 2018 (CCPA).

Mapbox considers the responsible stewardship of the data in our possession to be among our most important duties. We strongly believe that a well-designed system of privacy regulation will benefit both companies and consumers. This responsibility prompted us to submit comments in advance of initial CCPA rulemaking as well as in response to the first draft regulations and their subsequent modifications.

Although we believe that the OAG's work toward a final set of CCPA regulations continues to proceed in a generally productive direction, we were disappointed to see that the most recent regulatory draft removes the February 10, 2020 document's guidance regarding internet protocol (IP) addresses (§999.302 (a)). This guidance provided valuable clarity to businesses seeking to comply with the CCPA and resolved a tension related to the CCPA's definition of "personal information" that we have highlighted since the law's passage.

The CCPA defines "personal information" as a category of information that triggers elevated compliance obligations when it is collected from consumers. The CCPA further identifies IP addresses as a type of personal information. Because internet communications necessarily include IP addresses, it could be argued that the practical effect could be to trigger elevated "personal information" protections for all internet-based collections of information. It seems absurd to suppose that the CCPA's authors intended for all information collected from consumers over the internet to qualify as personal information. We believe this is not an intended consequence of the CCPA, and that any final regulation should clearly preclude any such interpretation. W353-1

The §999.302 (a) guidance present in the modifications published February 10, 2020 provided a reasonable means of resolving this defect while preserving consumer privacy. We urge your office to consider reinserting the §999.302 (a) guidance as present in the February 10 draft. If

this is not possible, some other means of addressing the above ambiguity related to IP addresses is necessary.

This is doubly true given the additional questions raised by the removal of the §999.302 (a) language: observers have been left to guess what this deletion means for the CCPA and its enforcement. Without clarification, we believe that businesses will face an undesirably high level of uncertainty concerning their IP address-related obligations under the CCPA. W353-1 (cont.)

In closing

We welcome the OAG's attention to this matter and thank you for your consideration of these comments.

Thomas Lee
Policy Lead, Mapbox
[redacted]

Kathleen Lu
Senior Counsel, IP and Open Data, Mapbox
[redacted]

Message

From: Ilias Chantzos [redacted]
Sent: 3/26/2020 1:44:38 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: modifications to proposed CCPA Regulations - Broadcom comments
Attachments: Comments to the Second Set of Modifications-CCPA-Regs.pdf

Dear Madam, Sir,

attached to this email you will find Broadcom's comments to the proposed modifications to CCPA regulations.

For any questions, clarification or additional information please feel free to contact me directly.

Sincerely yours

Ilias Chantzos, LLM, MBA
Global Privacy Officer and Head of EMEA Government Affairs
Broadcom Inc.
Office: [redacted]
Mobile: [redacted]
Email: [redacted]
Twitter: @ichantzos
Jabber: [redacted]
Linkedin:https://www.linkedin.com/in/ilias-chantzos-a50121/

--

Ilias Chantzos, LLM, MBA
Global Privacy Officer and Head of EMEA Government Affairs
Broadcom Inc.
Office: [redacted]
Mobile: [redacted]
Email: [redacted]
Twitter: @ichantzos
Jabber: [redacted]
Linkedin:https://www.linkedin.com/in/ilias-chantzos-a50121/

BROADCOM

Comments to the Second Set of Modifications on the California Consumer Privacy Act Regulations Proposed Text of Regulations

Global Privacy Office
March 2020

Broadcom Inc

Web: www.broadcom.com
Corporate Headquarters: San Jose, CA
© 2020 by Broadcom All rights reserved.

Introduction

The California Consumer Privacy Act Regulation is now up for a second round of comments. We believe that cybersecurity and fraud prevention is a global objective on which privacy and critical infrastructure depend.

Both as an organization in our own right, and as a provider of payment security services and cybersecurity technologies and services, it is in our and our customers interest to collect and process personal information to the extent strictly necessary and proportionate for the purposes of preventing fraud and ensuring the security of our own, and of our customers' payment transactions and information networks and systems. This includes the development of payment transaction records and of threat intelligence resources aimed at maintaining and improving on an ongoing basis our ability to detect fraudulent payment transactions, and the ability of networks and systems to resist unlawful or malicious actions and other harmful events affecting information networks and systems.

We believe this merits a regulatory approach which serves to protect the digital ecosystem and ensures privacy, cyber safety and fraud prevention.

We would therefore like to support an approach that allows such protection.

Our comments in more detail

Service providers of cybersecurity and fraud prevention ("Service Providers") under CCPA

In order to work effectively Service Providers require so-called secondary processing. To be able to protect customers, Service Providers need to be aware of the threats throughout the ecosystem. This involves protecting customers from the threats they see affecting others, as well as protecting others from the threats affecting customers. It involves an iterative process whereby a security provider while protecting one customer is made aware of a new threat. The detection of the new threat or the threat itself may require the processing of personal information. Once that threat is detected the security provider is able to learn from it, improve its service and protect not only the customer in the environment of whom the threat was detected but the entire customer base as well as third parties by taking actions such as disclosing the threat information to a Computer Emergency Response Team (CERT).

We understand the cybersecurity use case to have been addressed by the First round of modifications, allowing for such secondary processing of personal information for Service Providers in section 999.314.c.4 in page 20 of the proposed Regulations:

(c) A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except:

(4) To detect data security incidents, or protect against fraudulent or illegal activity;

It is important to note that all security technologies work in this way and aim to create a condition of digital "herd immunity" akin to the biological one when a new threat appears. The processing of personal information in such a scenario to the extent necessary and proportionate to achieve the desired security result, i.e. the detection of the threat and the dissemination of the relevant security information does not constitute a sale of data in any way but a necessary precondition for the security technology to work. Any valuable consideration takes place with the purchasing of the technology and the delivery of the service as a result of the purchase. Any exchange of data that happens is an aspect of the essential functionality of the technology in order to deliver the protective result that the customer has purchased, and by no means a distinct sale of any kind. W354-1

Article 1798.140 section t.1 needs to be understood in that context when considering cybersecurity use cases because otherwise any security tool risks being perceived as "selling" personal information while in reality it simply processes such information for the purpose of providing the service that the customer purchased without any additional consideration. We would welcome language in the Regulations that would provide clarity and elaborate on this point along those line.

Interpretation of CCPA Definitions

In addition, Service Providers like other parts of the digital ecosystem rely on different types of data such as metadata and content data to detect and block malicious attacks. Detecting an email as spam may require scanning its metadata to identify whether it is originating from a known spam distributor or not. Scanning its content may be necessary to determine whether it has malicious attachments or links pointing to infected websites.

CCPA needs to strike the right balance between extending the protection to cover all personal information while enabling different businesses, including cybersecurity and fraud prevention service providers, to operate in a business conducive environment. In the digital age there is a plethora of data and digital traces available for organizations to access. The important policy decision is whether CCPA will go down the direction of treating pretty much anything as personal information (which is what the deletion of 999.302.a would signify) or will take a more granular approach that will ensure a level of protection that is both reasonable and flexible. W354-2

To achieve that the ability to identify and "single out" an individual based on data that is either available or easily/readily available to a business is a key differentiator. Another key differentiator is whether the business model i.e. the purpose of collection is to identify or single out a particular individual. Unlike other jurisdictions, such as GDPR countries, we do not believe in the desirability or the effectiveness of the approach whereby any data should always be considered as potentially personal, no matter how difficult it would be to collect, or correlate, just because a particularly well resourced and/or sufficiently motivated third party (e.g. a law enforcement or intelligence agency) could theoretically achieve that correlation and thus identify a consumer. This is the current interpretation in Europe which de facto has led to all data being treated as personal, even when that interpretation is so disproportionate as to make little or no practical sense.

Instead it would be more appropriate to have a reasonableness test that is based on:

- The proximity of the data to an individual consumer (i.e. can an individual be easily singled out?); and
- the ease of access to the data to be correlated (is the data readily available in the organization? Can additional data be easily found by a simple online search?); and
- finally, whether it is in the business model of an organization to use the data for the purpose of identifying or singling out an individual (e.g. to advertise or build and monetize profiles).

For the specific aspects of the cybersecurity and fraud prevention business a single online identifier especially as prolific to all kind of devices as an IP address is not sufficient to identify an individual. Equally correlation between an Internet Service Provider that can identify the individual in question is not evident nor is the purpose of a cybersecurity service to identify an individual, but rather to block a threat.

We therefore strongly support re-introducing the interpretation of Personal Information in relation to IP addresses as proposed in the first round of modifications:

§ 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."

W354-2 (cont.)

Where it qualifies as Personal Information, CCPA also regulates the processing of metadata, content data, terminal equipment information and IP addresses to which Service Providers need to have access for the benefit of protecting their entire user population, i.e. consumers, companies, critical infrastructure and governments. IP addresses may be of web servers and connected devices involved in the generation, distribution, conveyance, hosting, caching or other storage of cyber threats such as malicious or otherwise harmful contents. Processing of such data allows protecting customer environments, collecting threat data information and using it for security research or using threat detection information of a particular customer for the benefit of all customers in the digital ecosystem. It is important to note that the purpose of Service Providers is not to single out or target consumers based on IP addresses. Neither is such information disclosed to anyone for any such purposes.

The data used does not relate to customer organizations or to their users or consumers, but to the threat agents such as cybercriminals or fraudsters who are trying to attack customers and create and spread vulnerability within the ecosystem. It is used for the overall protection of a system that otherwise would suffer severely from malicious attacks.

Such interpretation is not uncommon in other privacy protective regulations, where it is a requirement that the business needs to have access to both the data and other information, which then allows identification of an individual. Where an IP address cannot be reasonably linked to a particular consumer or household, but is used to

protect against cyber attacks or fraudulent activity, it should not qualify as Personal Information.

W354-2
(cont.)

Anonymization

It is important to stress the fact that cybersecurity and fraud prevention is primarily about detecting and blocking known or suspected threats and locations on the internet. To do that the information needs to be accurate and precise otherwise it may cause damage to innocent parties or render parts of the internet inaccessible. Anonymization that could work in other instances is impractical in cybersecurity. A Service Provider needs to know which specific email address to treat as a source of spam or which IP address to block in order to resist the DDoS attack it is use to orchestrate. Trying to mask this information does not benefit privacy (except perhaps that of the attacker) and creates potential incompatibilities or risks that an innocent party will be blocked or inadvertently affected.

Message

From: Emery, Emily [redacted]
Sent: 3/27/2020 3:21:21 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Emery, Emily [redacted]
Subject: MPA Comments on the Modifications to the Proposed Text on CCPA
Attachments: MPA Comments on the Second Set of Modifications to the Proposed Text on CCPA 03.27.2020.pdf

Attached, please find comments on the second set of modifications to the 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.

Emily Emery
Director of Digital Policy
MPA - The Association of Magazine Media
Cell: [redacted]
Office: [redacted]

March 27, 2020

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 the Second Set of Modifications to the Text of Proposed 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 the following comments on the second set of modifications to the proposed text of the regulations implementing the California Consumer Privacy Act (CCPA). MPA is pleased to offer 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.

Readers trust magazine media brands to provide them informative, enriching, educational, and entertaining content. Delivering trusted content is an especially vital resource in times of public crisis. The responsible use of consumer data is one crucial way that magazine publishers create and maintain the high levels of the reader trust that sustain magazine media brands' relationships with their readers.

The responsible use of consumer 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. In turn, businesses, including magazine publishers, require clarity and certainty in regulatory requirements to develop the internal systems and processes meant to protect consumer data.

MPA appreciates the effort undertaken by the California Office of the Attorney General (OAG) to clarify several regulatory requirements in its recent modifications to the proposed rules implementing the CCPA. However, MPA believes that further clarification from the OAG is required to protect consumer privacy and data security and uphold the trusted relationship of magazine media brands with their readers.

Accordingly, MPA raises three areas of concern in the second set of proposed modifications to the regulatory text where clarification from the OAG would be welcome. MPA then asks the OAG to allow a reasonable amount of time for magazine publishers and others to adjust their practices under the proposed rules' new requirements before bringing enforcement actions under the CCPA.

I. The OAG should restore language in section 999.315(d)(1) that recognizes that consumer choice should prevail over default browser behavior.

MPA urges the OAG to restore the language removed from section 999.315(d)(1) that states: "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."

The requirement for businesses to honor default global privacy controls, including browser plugins or privacy settings, without the affirmative confirmation of the consumer, stands in the way of consumers' ability to make individualized choices about their own personal preferences, including determining which magazine publishers or businesses can and cannot sell their personal information.

In the current technological environment, default browser settings broadcast a single opt-out signal to the entire internet marketplace. Because individual businesses, including magazine publishers, would be required to ask consumers to opt-in to the sale of personal information after receiving a global privacy setting broadcast, the effect of this requirement is to inadvertently turn the CCPA's opt-out system into a *de facto* opt-in system. Striking the affirmative selection language result is clearly outside of the scope of what the California legislature intended in providing an opt-out right in the CCPA.

Even if users 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. W355-1

MPA respectfully asks the OAG to remove the global privacy control requirement entirely, 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.

At a minimum, the affirmative selection language should be restored. It is an important tool for respecting consumer choice based on preferences that reflect their direct relationship with magazine publishers and other websites.

II. Given the OAG's proposed modifications to Section 999.315(d), the OAG should modify Section 999.315(f) to create a reasonable grace period for requiring the notice of a consumer opt-out request to third parties.

Particularly given the uncertainty caused by the new language proposed in Section 999.315(d), the notification to third parties that a consumer has exercised their right to opt-out imposes new, significant operational challenges with a very short time frame for implementation.

MPA appreciates the clarification in the previous modifications to 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.

However, the additional added 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. W355-2

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.~~"

III. The OAG should again remove the privacy policy disclosure requirements added to section 999.308(d) and 999.308(e) that create significant new technical architecture requirements and could expose proprietary information.

MPA is troubled by the OAG's re-insertion of the previously deleted requirement that privacy policies must identify the categories of sources from which personal information is collected and the business or commercial purpose for collecting or selling personal information. W355-3

The CCPA statutory requirement in Cal. Civ Code § 1798.110(a)(2) allows an individual consumer the right to request a business disclose to the consumer the categories of sources and business or commercial purpose, specifically responsive to a consumer's request. The statutory language does not require businesses to include these in the publicly posted privacy policy, and the OAG should not either.

From a technical perspective, the re-introduction of such disclosure requirements creates an entirely new technical process for the collection, analysis and reporting of such information, with very little time for implementation.

In addition to the disclosure requirements being operationally burdensome, the latter definition "business or commercial purpose" is subject to interpretation. Without further clarification from the OAG, disclosure language could be perceived as overly broad, or if required to be overly specific, could lead to the disclosure of proprietary business information or trade secrets. W355-3 (cont.)

MPA urges the OAG to again remove the requirement to identify categories of sources of personal information and the business or commercial purpose for collecting or selling personal information where the requirement set forth in section 999.308(d) to identify "the categories of personal information the business has collected about consumers" should suffice.

IV. The OAG should add language in section 999.323 that affirmatively permits businesses to first engage directly with consumers to verify the validity of access and deletion requests made by authorized agents before any fees for verification are incurred.

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 as a potential and significant risk vector for fraudulent activity and data security concerns.

While MPA appreciates the additional clarifications made by the OAG in section 999.323 in the previous round of modifications, the OAG's addition of language indicating that an authorized agent should not be required to pay a fee requires further language to safeguard requests from likely fraud and abuse. MPA urges the OAG to further clarify that a business may revert to the consumer directly before any verification costs can be incurred by an authorized agent in order to confirm that the request is legitimate and that the consumer has, in fact, authorized the agent's request on their behalf. W355-4

The second round of modifications clarifies that a business may not charge a consumer or a consumer's authorized agent a fee for verification, including associated with notarization, but the new language does not anticipate potentially abusive or fraudulent requests purportedly made on behalf of consumers. Without further clarification from the OAG of adequate technological methods for making direct consumer verifications of such requests, businesses may be inundated with demands from authorized agents that seek reimbursement for proof of authorization, while lacking a clear mechanism to confirm such requests have been legitimately issued by a consumer to the requestor.

First, the OAG should clarify that a business may directly confirm with the consumer that they have authorized the agent to issue an access or deletion request before an authorized agent can incur or seek reimbursement for any costs that might be directed to a business in obtaining proof of authorization.

Second, the OAG should clarify that an authorized agent should not incur or seek reimbursement for proof of authorization where a business offers an alternative verification method that is free to the consumer. For example, if an entity that acts as an authorized agent routinely gathers

notarized identification from consumers, and the authorized agent submits a notarized document to a business that does not require a notarized document to process the underlying consumer request, the authorized agent should not be able to seek reimbursement from the business where the verification was not requested or required by the business in order to comply.

W355-4 (cont.)

Finally, in light of this proposed modification, MPA again notes the important role that direct first-party engagement with consumers can have in preventing fraudulent activity. Accordingly, MPA again urges the OAG to allow businesses discretion in section 999.315(h) by including language to permit the business to notify the consumer directly, and not merely the requestor, in instances where there exists a good-faith belief that the request made by an authorized agent to opt-out is fraudulent. Such a change would help ensure it is consumers themselves who 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.

V. The OAG should postpone enforcement in order to provide a reasonable amount of time for businesses to update their practices for the revised regulations.

The CCPA became operative on January 1, 2020. However, regulated entities still do not have access to finalized regulations to implement the law, and additional technical clarifications are needed to maximize the success of businesses making good-faith efforts to comply with the regulations. Simultaneously, the global coronavirus (COVID-19) pandemic has had a dramatic impact on the day-to-day operations of businesses, including the departments tasked with the legal, operational and technical preparations required for CCPA compliance efforts.

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. In light of shelter in place requirements like those issued by Governor Gavin Newsom, these efforts are now taking place remotely across distributed workforces.

W355-5

Even absent the challenges presented to businesses responding to the coronavirus (COVID-19) pandemic, the CCPA is complex, and the implementing rules could materially change again in further revisions before the law's enforcement date of July 1, 2020. The magnitude of uncertainty and complexity strongly suggests that despite making significant investments toward good-faith efforts to uphold consumer data protection, many businesses may not have sufficient time to operationalize the final rules before enforcement.

MPA urges the OAG to 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.

Extra implementation time will enable businesses like magazine publishers to understand and effectively operationalize the rules, helping consumers to more seamlessly exercise the rights afforded under the new law.

MPA members strongly support the underlying goals of the CCPA. However, given the enormous logistical challenges faced by businesses in the current environment, and the outstanding uncertainty of the final regulatory text, the OAG should postpone enforcement of the CCPA until January 1, 2021. W355-5 (cont.)

* * *

MPA appreciates the OAG's continued efforts to solicit feedback on proposed modifications to the CCPA rulemaking and the office's efforts to address outstanding CCPA implementation concerns. We appreciate the opportunity to provide our views on areas needing further guidance and the need for postponed enforcement. Greater clarity is needed from the OAG to ensure that businesses like magazine publishers can successfully implement these new and expanded requirements, uphold reader trust, and preserve the viability of the magazine media brands that consumers enjoy.

Sincerely,

Brigitte Schmidt Gwyn
President & CEO
MPA – The Association of Magazine Media

Emily Emery
Director, Digital Policy
MPA – The Association of Magazine Media

Message

From: Mark Smith [redacted]
Sent: 3/27/2020 9:39:48 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: NMMA comments on 2nd set of modifications to CCPA
Attachments: NMMA comments on 2nd CCPA modiciations 3.27.2020.pdf

Attached.

Thank you.

SMITH
POLICY GROUP

MARK SMITH
Smith Policy Group
1001 K Street, 6th Floor
Sacramento, CA 95814
[redacted]
[redacted]
smithpolicygroup.com

NMMA National Marine Manufacturers Association

March 27, 2020

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

On behalf of the National Marine Manufacturers Association (NMMA), I am again writing to request that you consider amending the proposed regulations implementing the California Consumer Privacy Act (CCPA) to allow for recreational marine dealers and manufacturers to exchange identifying information needed to address product warranty issues and product recalls.

NMMA is the leading trade association representing the recreational boating industry in North America. Among its many roles, NMMA is dedicated to facilitating product quality assurance. NMMA's 1,300 member companies produce more than 80 percent of the boats, engines, trailers, accessories and gear used by boaters and anglers throughout the United States and Canada.

California ranks eighth in new boat sales, seventh in new engine sales and, with 745,640 registered boats, is the fourth largest boating state in the United States. Sales of new boats, engines and accessories totaled $718 million in 2018. Overall, recreational boating in California had an estimated direct and indirect annual economic impact of $13 billion in 2018. Clearly, hundreds of thousands of California boaters depend upon a network of manufacturers, dealers and the California state government to effectively and efficiently provide warranty information and repairs and implement product recalls if needed.

We believe the legislature intended to ensure that recreational boat owners would continue to be contacted about important safety recalls and have their boats, engines and associated equipment repaired under warranty. We request, however, that the draft regulations be clarified to give recreational marine manufacturers unambiguous certainty that the CCPA will allow them to collect the information they are required to retain under federal law for important safety, repair and recall notices.

In 2019, the Legislature passed, and the Governor signed, AB 1146 (Berman). Among the amendments this bill made to the CCPA were two standards for consumer data handling for public safety notifications related to recalls and warranties.

- 1798.105(d), relative to a consumer's request to have information deleted as it pertains to warranties and recalls.

Executive Committee
Chairperson
Ben Speciale
Yamaha Marine Group

Vice Chairperson
Steve Heese
Chris-Craft Corporation

Treasurer
Scott Deal
Maverick Boat Company

Secretary
Ned Trigg
Dometic Corporation
Marine Division

BMD Representative
Doug Smoker
Smoker Craft, Inc.

EMD Representative
Ron Huibers
Volvo Penta
of the Americas

MACD Representative
Steve Tilders
Xylem Inc.

Member at Large
Bill Watters
Syntec Industries

President
Frank Hugelmeyer
NMMA

650 Massachusetts Avenue, NW, Suite 520
Washington, D.C. 20001
202.737.9750 Fax 202.737.9762
nmma.org

- 1798.145(g)(1), an explicit exemption from a consumer's ability to opt-out of providing consumer identifying information to manufacturers, who thereafter use it to approve repairs under warranty or to contact owners in the event of a recall.

Chapter 1798.105(d)(1) of the CCPA states that "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 complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, 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."

While Chapter 1798.105(d)(1) provides a broad exemption, the members of NMMA believe the information they need for warranty and recall purposes should have exactly the same protections and latitude as given to the new car industry in the CCPA. The safety of boaters and their passengers can depend upon accurate and expeditious recall actions and warranty approvals.

NMMA suggests that the explicit opt-out provisions for vehicles in 1798.145(g)(1) should be as broadly construed as possible to include recreational vessels. We encourage you to consider a regulatory interpretation that specifically allows a free flow of ownership and product information between marine dealers and manufacturers to provide the database needed for warranty verification and for recalls. This will enhance public safety by giving recreational vessel and marine engine manufacturers as complete a record as possible of product sales and ownership while applying the same provisions for the use of the information that is now in place for vehicles. For the marine industry, identifying information should include, at a minimum, the vessel's hull identification number (HIN), its make, model, model year, and the buyer's name, address and email address. Information on engines should include its serial number. W356-1

Further justification for this regulatory interpretation comes from the requirements of federal law. Manufacturers must have reliable data in order to comply with 46 U.S. Code §4310. 46 U.S. Code §4310 requires recreational boat and engine manufacturers to retain the name and contact information of the buyer of any new vessel, engine or associated product for a minimum of 10 years. Marine dealers are the only source of information about buyers and the products they purchase. Dealers provide these data seamlessly as part of the sales process.

Should a recreational vessel or engine fail to comply with the regulation or contain a defect that creates a substantial risk of personal injury to the public, 46 U.S. Code §4310 states that the manufacturer shall provide notification of the defect or failure of compliance to the original purchaser, and subsequent owners if known. This mandate is rigidly enforced.

In addition to broadly interpreting 1798.145(g)(1), the draft regulations could be amended to create a class of dealers and manufacturers of recreational marine boats and engines, W356-2

automobiles, off-road vehicles and motorcycles, and other products that have similar collection, retention and reporting methods and requirements.

By grouping these business sectors into a class, the regulations could standardize the collection of this information and the conditions under which these data can be transmitted between dealers and manufacturers. Creating a single standard for these retention policies would retain the public's confidence in the recall and warranty repair system.

A possible example would be:

Product information and ownership information may be retained or shared between a new product dealer and the product's manufacturer, if the product or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a repair covered by a warranty or a recall conducted pursuant to Title 49 of the United States Code, provided that the dealer or manufacturer with which that information or ownership information is shared does not sell, share, or use that information for any other purpose.

W356-2
(cont.)

NMMA would welcome an opportunity to work with the California Office of the Attorney General to write and implement such a regulation. For questions or concerns, please contact us using the contact information, below.

Sincerely,



David Dickerson
Vice President, State Government Relations
National Marine Manufacturers Association
650 Massachusetts Ave NW #645
Washington, DC 20001
[redacted]

Message

From: Shanahan, Richard [redacted]
Sent: 3/27/2020 7:27:38 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Mizoguchi, Kenichiro [redacted]
Subject: OAL File No. 2019-1001-05: CCPA Regulations
Attachments: 03272020_CCPA AG Comments.pdf

Ms. Kim,

Please find attached comments from Hitachi Group Companies regarding the 2nd draft of regulations to implement CCPA.

We look forward to continuing the dialogue on this issue to provide the best result for California consumers.

Best regards,

Richard Shanahan
Manager | Government & External Relations
Hitachi, Ltd. | Washington, DC Corporate Office
t. [redacted] | m. [redacted]
[redacted]

Follow Us
www.hitachi.us/gov-relations

HITACHI
Inspire the Next

HITACHI
Inspire the Next

March 27, 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).*

While Hitachi commends the Attorney General ("AG") and the California Department of Justice's commitment to developing the fairest, most equitable regulatory framework for California's new privacy standards, the most recent modifications to the proposed regulations represent a step backwards.

Cookies

Hitachi disagrees with the deletion of *Section 999.302: Guidance Regarding the Interpretation of CCPA Definitions*. As noted in our December 2019 comments:

> When it comes to the use of website cookies, further clarification with regards to CCPA's scope is needed. Given the global nature of many corporate websites, a California resident may access a corporate website that is not designed to target California consumers. Would the corporation's use of cookies—simply to assess web traffic without any sale of that data—bring the corporation under the purview of CCPA? Is it the law's intention to cover this type of site visit even if the corporation is not marketing a product to the consumer?

W357-1

Rather than remove the section, the AG's Office should have provided a clear definition for "reasonable standard." (A "reasonable standard" definition is needed throughout the document). The section's elimination could inadvertently lead companies to gather more data to determine an individual's location or respond to consumer requests. As such, Hitachi urges that *Section 999.*302, including a "reasonable standard" definition, be reinstated in the final regulations.

Annual Gross Revenues / Consumer Ambiguity

We have consistently called on the AG's Office to dispel ambiguity around the annual gross revenues threshold and the term "consumer." Companies need clear guidance—not complexity and confusion. At present, the following questions (among many others) still have not been adequately answered.

- Is a non-California resident, physically in the state, a "consumer"?
- Is a California resident, physically outside the state but still engaging in consumer activity, a "consumer"?
- Is the $25M revenue number based on sales to California consumers, U.S. sales, global sales, or some other method?

W357-2

Failure to deliver definitional clarity could have a chilling effect on Californian innovation. Final regulations must address these issues.

Households

As we observed in our February 2020 comments, the *Treatment of Households (Civil Code section 1798.140, subdivision (o))* provided needed guidance and conditional tests. While a welcome addition, the list of conditions could lead to unsatisfactory results for the consumer.

A business may not possess enough information to verify each individual member of a given household and may have no way of verifying whether each individual is currently a member of that household. This may lead to household information deletion requests being denied.

W357-3

The regulations still do not make clear how personal data rights are assigned for shared devices. Is the modification suggesting that the data is collectively owned? If so, should companies determine the value of data for each individual in the household, or treat the household as a whole unit? How does a business that does not have an on-going relationship with a certain household (and does not know the number of household members) determine the value of newly-collected data?

While the modifications are an improvement over previous versions, the final regulations should clearly define "household."

Risk-Based Verification Process

We continue to recommend the development of a guidance document that favors a risk-based verification process that also considers the sensitivity of the data being processed.

W357-4

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 measures grow more advanced, and it would also give businesses certainty to liability under the title.

Conclusion

Hitachi recognizes the complexity of these efforts and appreciates the AG Office's on-going engagement. Addressing the above points will be critical to making the final rules clear and understandable for businesses and consumers, alike. We look 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.

CCPA_2ND15DAY_00354

Message

From: Kingman, Andrew [redacted]
Sent: 3/27/2020 11:48:22 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Pindrop Security Inc. Comments - Second Set of Modifications to Proposed CCPA Regulations
Attachments: CCPA 3-27-2020.pdf

Good afternoon,
On behalf of Pindrop Security Inc., attached please find comments addressing the Attorney General's Second Set of Modifications to the Proposed CCPA Regulations. We would be happy to answer any questions you may have.

Respectfully submitted,
Andrew A. Kingman

Andrew Kingman
Senior Managing Attorney

T [redacted]
M [redacted]
E [redacted]

DLA PIPER

DLA Piper LLP (US)
33 Arch Street, 26th Floor
Boston, Massachusetts 02110-1447
United States
www.dlapiper.com

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



March 27, 2020

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

Re: Second Set of Modifications to Text of Proposed Regulations

Dear Attorney General Becerra and Staff,

In these highly unusual times, both the public and private sectors bear the burden of helping to protect citizens from threats to their security. At Pindrop, we accept this responsibility with the utmost seriousness. Millions of times per day, fraudsters and hackers attempt to penetrate secure networks and appropriate consumer identities in order to perpetrate identity theft and other types of criminal schemes. As a leading provider of anti-fraud products and services in call centers for financial institutions, insurance, retail, and government organizations, we are on the cutting edge of detecting and preventing this activity, thereby protecting both the privacy and the security of California residents.

As the California Consumer Privacy Act's (CCPA) implementation has phased in, the law's text has revealed crevices that significantly complicate compliance operations, but do not materially increase consumer privacy. In Pindrop's case, we are exclusively a business-to-business (B2B) operation, and do not have direct relationships with consumers. Our business model fits squarely within the CCPA's definition of "service provider."

And yet, as nearly every business does, Pindrop maintains a website that anyone can visit (but that is designed for our customers, which are themselves businesses). We use a free website analytics tool and use a limited number of cookies to advertise our products on other websites. Given the broad definition of "sale" and "personal information" already in the CCPA, we believe the most accurate compliance posture for our company is to be a service provider with respect to our core business, but a business with respect to our public-facing website.

With this by-the-letter interpretation, however, come significant compliance costs in the form of drafting the CCPA privacy policy disclosures, the point of collection notice, the employee, job

applicant, and contractor notices, and the opt-out of sale notice, as well as implementing systems to handle any consumer rights requests. Again, we are putting these in place with the knowledge that very few consumers will likely view these documents or make these requests, but with the goal of fully complying with CCPA's complex statutory requirements.

Pindrop's comments are offered with the goal of minimizing additional burdens and compliance costs for entities in our situation, without harming consumer privacy. We address three points:

- In Section 999.308, we address the proposed additional information to be included in privacy policies, which will significantly lengthen the policies and reduce their comprehensibility for consumers. W358-1
- In Section 999.306, we propose deleting paragraph (e), which sets forth an unrealistic requirement to obtain opt-in consent for information that has already been collected under the CCPA's definition, but not yet sold before the opt-out notice has been posted (but after the opt-out link is active). W358-2
- In Section 999.312, we propose removing the counterintuitive exemption for toll-free numbers only for exclusively online businesses that have a "direct relationship" with consumers. W358-3

Lastly, we reiterate our support for the anti-fraud provision in the Service Provider section, 999.314, which is very important to fraud prevention services such as ours. W358-4

I. Section 999.308 – Privacy Policy Requirements

Your office has undoubtedly already considered the tension in privacy regulation between comprehensiveness and comprehensibility. We believe the proposed additional language in paragraphs (c)(1)(e), (f), and (g)(2) does not appropriately balance these goals, and would significantly lengthen policies. This would actually detract from consumer privacy, as consumers are less likely to read lengthy disclosures.

Already, the CCPA privacy policy disclosures are quite lengthy, even for an entity like Pindrop which, in its narrow role as a business, engages in extremely limited processing of personal information. Paragraph (c)(1)(e) would reinstate the intent of the original draft of the regulations, requiring that in addition to disclosing the categories of information the business collects, discloses for a business purpose, and sells, the business must also disclose "the categories of sources from which the personal information is collected." Read in conjunction with paragraph (c)(1)(f), a business is required to add significant verbiage around the sources of information the business collects, and then is required to identify the business purpose for collecting or selling information, but not for disclosing for a business purpose. Additionally, (c)(1)(f) adds a brand W358-1 (cont.)

new requirement to explain its purposes for *collecting* information, which adds a materially burdensome compliance problem which businesses have not thus far been preparing to implement.

These will not meaningfully improve consumer privacy because they add several layers of complexity for consumers simply seeking out what a company is doing with the information it collects from them. By adding granular detail, the proposed language unnecessarily sacrifices clarity. W358-1 (cont.)

Similarly, the proposed language in paragraph (g), requiring that for each category of personal information the business sells or discloses for a business purpose, the business additionally provide each category of third party to whom the information was disclosed or sold, would also lengthen the policy unnecessarily. Because the right to opt-out is not segmented by types of personal information provided, it is unclear what the aim of this language is. We recommend removing it.

II. Section 999.306 - Opt-in Consent Prior to Opt-Out Notice

Beginning on January 1, 2020, any business that sold personal information was required to operationalize a "Do Not Sell" link on every page on its website. Additionally, every business that sells personal information is required to inform consumers of this right in its privacy policy. Businesses – particularly those like Pindrop, which have minimal processing and sales of personal information and operate primarily as a service provider, have already spent tens of thousands of dollars on drafting the privacy policy requirements and implementing a Do Not Sell link.

The proposed language in 999.306 goes beyond the language in the statute concerning the right to opt-out, and we believe it is unnecessary to invalidate the work that entities have put into crafting workable solutions for this right in compliance with the statute's requirements, simply because the business has not provided a new notice that was not in the statutory language. W358-2

Additionally, because the definition of "sale" is drafted broadly to include cookie activity, it is very difficult to require opt-in consent *after* collection but *before* the "sale," since this transfer of data happens instantaneously. In effect, this would require entities such as Pindrop – whose only "sale" of information" is use of cookies – to shut down all cookie use until receiving opt-in consent, *or* to graft on CCPA language to GDPR cookie banners, but only temporarily.

This is confusing in two ways. First, it is confusing because consumers are just getting used to the opt-out of sale link; moving temporarily and non-uniformly to an opt-in consent model will not provide the needed certainty to encourage consumer participation in the CCPA controls. Second, it is confusing because businesses face the prospect of implementing *three different*

systems in a matter of months, for the same activity: 1) Jan. 1-present, using the "Do Not Sell" link; 2) present-regulation implementation, where opt-in consent will be required; and 3) post-regulation implementation, when businesses will know what is required to be in the Notice of Right to Opt-Out, and can draft and provide it to the public.

W358-2 (cont.)

Again, we believe that this misses the mark in general, but that it also uniquely impacts service providers that maintain a minimal online presence for consumers. For these reasons, we request that this provision be removed.

III. Section 999.312 Toll-Free Number Requirement

We appreciate your office's intent to provide relief to businesses for whom a toll-free number would not be an effective method of contact. Again, however, the drafted language puts entities such as Pindrop at a unique and burdensome disadvantage. By confining the toll-free exclusion to only entities with whom consumers have a "direct relationship" (and operate exclusively online), service providers such as Pindrop, who have some narrow responsibilities as a business, will be required to set up and maintain a toll-free number.

W358-3

This is not a productive use of resources. Service providers should be focused on ensuring that their contracts with customers are updated, that their employees, job applicants, and contractors receive the proper notices, and that their data segregation practices are appropriate. Diverting resources to set up a toll-free number that has a very low likelihood of being used is of no benefit to consumers. From a practical perspective, those consumers who are curious about a service provider will likely visit the service provider's website first, where they will be able to exercise all of their rights using the proper channels.

IV. Section 999.314 - Anti-Fraud Language

Finally, Pindrop wishes to reiterate its support for the anti-fraud language currently in the Service Provider section, which allows service providers to use consumer data for anti-fraud and identity theft purposes. Nearly every business outsources some degree of its security to service providers who specialize in detecting and preventing cybercrime. Allowing these service providers to keep pace with cybercriminals by sharing this information across clients and industries is critical to the health of these ecosystems. Conversely, forcing service providers to silo this information by client ties both hands behind their backs, and puts both consumers and companies at significant and needless risk.

W358-4

March 27, 2019
California Department of Justice
ATTN: Privacy Regulations Coordinator



Pindrop thanks you for your time and consideration. We would be delighted to discuss these issues further at your convenience.

Sincerely,



Clarissa Cerda
General Counsel & Secretary, Pindrop Security Inc.
[redacted]

Message

From: Paul Jurcys [redacted]
Sent: 3/27/2020 4:58:09 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Markus Lampinen [redacted]
Subject: Prifina's comments
Attachments: CCPA Review-March 27-final.pdf

Dear Madam/Sir,

Please find Prifina's comments attached below.

Sincerely,

Paul Jurcys

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

Prifina is a San Francisco-based company building user-centric tools that help individuals gain control of their personal data and where data remains under individuals control and possession.

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, Prifina 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 and release it to the public domain.

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 for how the Office of Attorney General should move forward and what areas to pay attention to. The data set, methodology and related findings, as well as further updates, are available at www.prifina.com/research

1. Study of the Comments on CCPA Regulations

Background

This Study has been prepared based on the resources that emerged during the drafting process of the California Consumer Privacy Act ("CCPA"). The CCPA came into effect on January 1, 2020.

Pursuant to Section 1798.185 of the CCPA, the Attorney General of the State of California was entrusted to adopt the Regulations for the implementation of the CCPA. More particularly, Section 1798.185 mandates the Attorney General to clarify certain definitions and to adopt rules and procedures that would facilitate compliance with various provisions of the CCPA.

The first draft of the Regulations was prepared by the Office of Attorney General and published on October 11, 2019.[1] On the same day, the Department of Justice called for public comments

[1] For more information see https://oag.ca.gov/privacy/ccpa.

CCPA_2ND15DAY_00362

which were to be submitted within 45 days. During the same 45 day period, public consultations were held in Sacramento, Los Angeles, San Francisco, and Fresno.

Sources of this Study

This Study relies on three main sources:

(i) Comments and opinions which have been submitted by various individuals and organizations during the first period of public comments;[2]

(ii) The text of CCPA; and

(iii) Three drafts of the proposed regulations: the Initial Proposed Regulations released on October 11, 2019 (hereinafter, the "Initial Proposed Regulations")[3], the Modifications to Proposed Regulations released on February 10, 2020 (hereinafter the "Second Draft of the Regulations")[4], and the Modifications to Proposed Regulations released on March 11, 2020 (hereinafter, the "Third Draft of the Regulations").[5]

In total, 262 individuals and organizations submitted their comments and suggestions on the initial draft of the Regulations during the first public consultation period (October 11 - December 6, 2019). The depth and wealth of practical insights with regard to the possible implementation of the CCPA and the proposed Regulations turned out to be invaluable. Therefore, Prifina has decided to collect and consolidate the suggestions submitted by various individuals, non-profit organizations, businesses, and industry representatives into one concise document.

The aim of this document is to provide a useful resource for any party that has a vested interest in the regulation of data privacy matters in California or outside California. This Study not only provides a concise synopsis of the main issues that have been raised by the surrounding industry during the process of the adoption of the CCPA and its accompanying Regulations; but also to highlight issues that are more pertinent to different stakeholder groups.

Analysis of Stakeholder Comments

W359-1

This Study is mainly based on 262 comments that have been submitted during the first public consultation period (October 11 - December 6, 2019). Having reviewed comments submitted in writing as well as comments which have been made during public hearings I four cities in California, we have identified and categorized stakeholders into ten groups as follows:

[2] All of which are freely available at the OAG website here: https://oag.ca.gov/privacy/ccpa.

[3] Available at: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf.

[4] Available at: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf?.

[5] Available at: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-second-set-clean-031120.pdf?.

1	**Private individuals**	**8%**
2	**Consumer rights advocates** Non-profit associations, think tanks, university researchers	**9%**
3	**Public/government agencies** Representatives of public utilities, attorney generals, members of representative bodies, etc.	**3%**
4	**Legal industry** Law firms and professional associations of lawyers	**7%**
5	**Finance industry** Individual financial institutions such as banks or credit unions, financial services corporations and trade associations representing finance industry	**10%**
6	**Software industry** Companies and trade associations representing the interests of software companies (e.g., companies building web search, privacy compliance, location and mapping data, software-as-a-service, etc.)	**15%**
7	**Advertising and marketing industry** Trade associations and alliances representing companies operating in advertising, marketing, market research space	**4%**
8	**Publishing industry** Trade associations and alliances representing companies operating in content creation space (e.g., music, media, audio-visual, entertainment content), large-scale and small publishers	**4%**
9	**Other businesses** Companies and trade associations representing businesses (e.g., manufacturing of IoT devices, vehicles, various service providers in hospitality, real estate and other spaces)	**11%**
10	**Trade associations** Trade associations representing various industry sectors	**29%**

W359-1 (cont.)

It should be noted that the number of written responses submitted by certain stakeholder groups does not directly represent the scale or number of organizations, entities or individuals whose interests may be represented. For instance, given the implications which newly adopted CCPA and Regulations have on certain industries, it was important to distinguish publishing and advertising and marketing industries into separate categories of stakeholders. More

specifically, there were 11 comments submitted by the representatives of the publishing industry. Although these 11 comments constitute on 4% of the overall responses received, those comments were submitted by organizations that represent 80-90% of news, audio-visual and digital content the publishing industry (both large and small corporations) which power multi-billion dollar industries in California. It is important to bear in mind this consideration.

Insights and Proposals Based on Stakeholder Comments

The following sections provide some insights and recommendations for the Department of Justice in further drafting the Regulations and taking further steps to implement the CCPA.

Based on the comments submitted by 262 stakeholders and the issues raised, this comment highlights ten major domains which have attracted the most attention from the stakeholders in their comments. We tried to summarize those ten main domains in the "Data Privacy Infographics" (see below). Each of the ten domains contain a number of themes. An In depth investigation of the comments submitted by 262 stakeholders helped identify which themes are more important to different stakeholders.

W359-1 (cont.)

The data collected could be especially useful for multiple purposes.

- First, the data could improve the regulatory framework: namely, the necessary amendments to the CCPA, finalizing the text of the Regulations, and considering future regulatory actions.
- Second, stakeholder comments help better understand the underlying technological foundations that are closely intertwined with the exercise of data privacy rights, the need to search for universal technological standards (most notably, open-source standards for data portability). Given such dependence on technological solutions in collecting and managing data, the legal framework has to be designed using unconventional approaches. Differently from other areas of regulation, the CCPA should offer opportunities for bottom-up solutions (e.g., compliance toolkits, templates for notices, possible recommended technological solutions for businesses to execute consumer requests, reduce compliance costs, and eliminate "privacy fatigue").

The Following Section 3 of this Study reviews ten main domains of data privacy and highlighting some of the major concerns for different stadholder groups. Each of the domains contains a section with key insights and recommendations. Section 4 of this Study offers further insights with regard to the future directions of regulating data privacy.

© 2020 Prifina Inc.

This infographic is published under the Creative Commons 4.0 Sharealike License

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 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

Definitions

Notices & Privacy Policy

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

Handling Requests

Methods for Submitting
Requests to Know and Delete
Responding to Requests
Service Providers
Requests to Opt-out
Requests to Access or Delete Household Information
Privacy by Design
Browser Plug-Ins

Verification and Security

Verification of Individuals
Verification for Non-account Holders
Reasonable Security Measures
Authorized Agents

Sales & Value of Data

Definition of "Sales"
Value and Valuation of Data
Non-Discrimination

Minors & Household Data

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

Training and Record-keeping

Training Employees
Record Keeping
Publication of Compliance Metrics

Service Providers

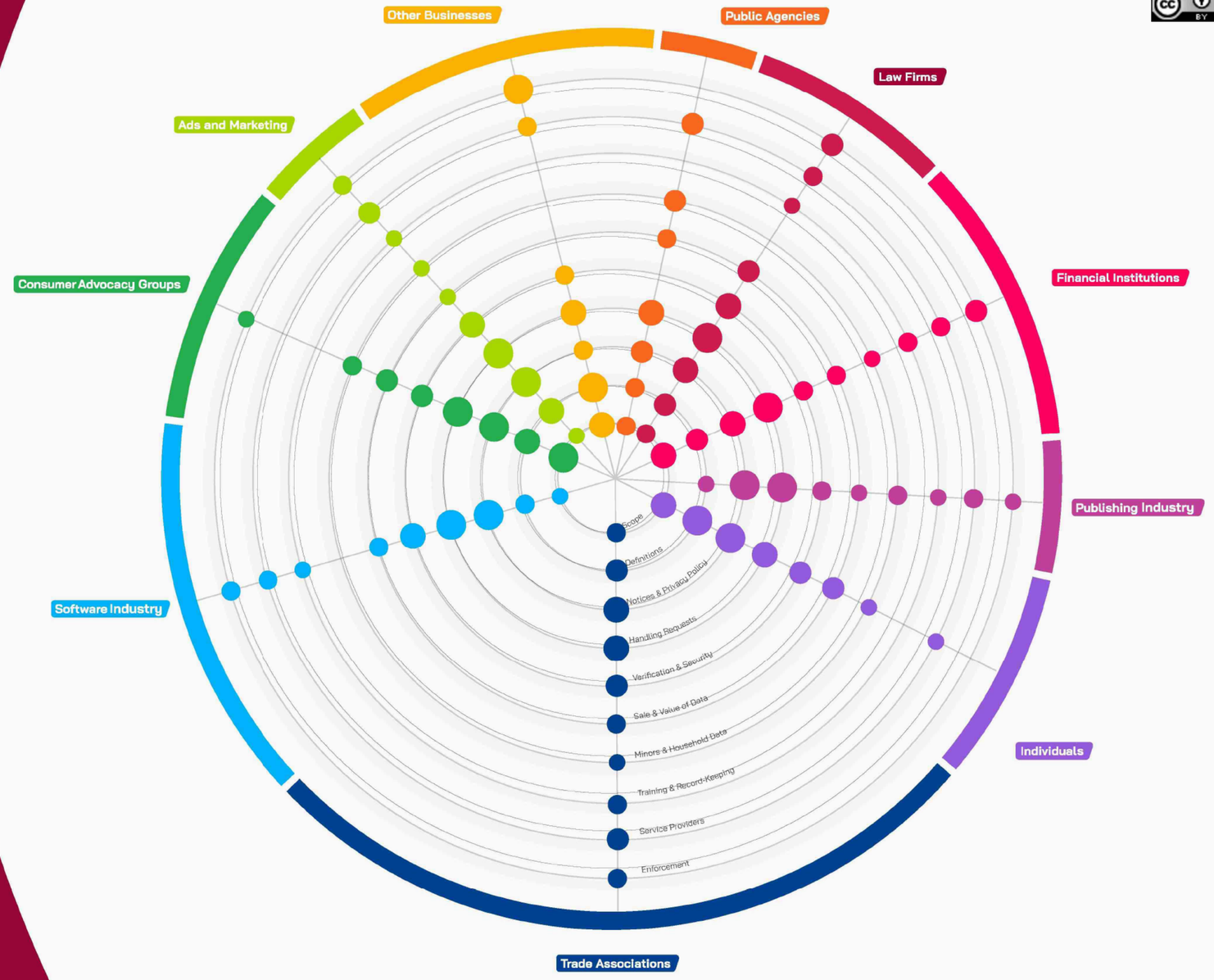
Third Parties
Service Providers
Business Purpose

Enforcement

Compliance Costs
Technical Challenges
Good-Faith Compliance Efforts
Effective Date

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

prifina



2. Main Themes in Data Privacy

The comments and opinions submitted by the public touch upon practically every provision of the CCPA and how the CCPA is reflected in the three drafts of the Regulations. Most of the participants uphold the goal of regulating data privacy issues in a transparent, clear, and comprehensible manner. In addition, many stakeholders notice that regulations should reflect the interests of various parties that are affected by CCPA: individual consumers, businesses, service providers, and third parties.

Having carefully examined the comment papers submitted to the Office of the Attorney General, it is possible to group the issues raised into ten major domains. These ten themes form the foundation for the Data Privacy infographic:

- the scope of the CCPA and Regulations;
- definitions;
- notices and privacy policy;
- handling consumer requests;
- verification of consumers and necessary security measures;
- issues pertaining to the sale of data;
- value and valuation of consumer data;
- problems arising with regard to data practices involving minors and households;
- training employees and record keeping; and
- issues related to the enforcement of the CCPA, compliance and effective date of the Regulations.

W359-1
(cont.)

In the following sections, we will provide some of the main concerns raised by different groups of individuals and organizations. While some of the themes raise questions of general concern (e.g., the scope of the Regulations or concerns of high compliance costs), in some cases certain groups of stakeholders raised industry-specific concerns which may not be necessarily addressed by the Regulations but may require some "out-of-the-box" approaches to implement.

2.1. Scope of Application

The adoption of the CCPA and implementing Regulations ignited extensive discussions with regard to the scope of applicability. In particular, three major dimensions related to the scope of the CCPA Regulations: (a) applicability to various business sectors; (b) territorial reach; and (c) relationship with other state and federal statutes that businesses may have to comply.

With regard to the applicability to businesses, the OAG was requested how the CCPA and Regulations would apply to AdTech sector[6]; whether government agencies (such as DMA) are treated as businesses and could be covered by the CCPA.[7] Some small business representatives and law firms asked to explain in what circumstances data collection and management principles enshrined in the CCPA and Regulations would apply to complex franchising structures.[8] Significant concerns have been raised about delicate situations of personal data collection practices within large corporate structures (conglomerates) and whether the requirements of the CCPA extend to the upstream companies under one holding structure.[9] Several government agencies requested to specify that CCPA does not extend to public utilities that are not selling personal information (even if they are required to do so), such as water supply or public roads.[10] Furthermore, some requests have been made to clarify whether companies offering services to government agencies qualify as service providers and are thus required do comply with the CCPA.[11]

Small and large businesses also raised significant concerns with regard to the scope of CCPA. Most notably, there seems some misunderstanding whether the CCPA is applicable to credit unions which are organized as non-profit mutual benefit corporations.[12] Some stakeholders went so far as to suggest that CCPA should not be applicable to financial institutions.[13] One of the main reasons for such an argument is that financial services organizations already have to comply with a number of other state and federal laws that govern data privacy (e.g., the Gramm-Leach-Bliley Act, "GLBA", California Financial Information Privacy Act, "FIPA", etc.)[14] Some suggestions have been made that this quandary could be resolved by adopting a federal law that should help set uniform privacy standards.[15]

W359-1 (cont.)

Some out-of-state stakeholders are still confused about the meaning of such notions as "Doing Business in California" and the threshold requirements. Quite a number of organizations requested the OAG to provide further clarification and guidance on this matter.[16]

---

[6] Privacy Coalition, p. 4

[7] See e.g., Metropolitan Transportation Commission, p. 200.

[8] Faegre, Baker, Daniels, pt. 4, p. 78.

[9] Hexagon, pt. 1, pp. 56-57.

[10] Transportation Corridor agencies, p. 2.

[11] Metropolitan Transportation Commission, p. 200.

[12] Joseph Garibyam, LA, p. 29.

[13] Card Coalition, pt. 4, p. 170-171.

[14] SF Fire Credit Union, pt. 1, pp. 59-60; International Bancshares Corporation, pt. 1, p. 100; Farmers Insurance Federal Credit Union, pt. 4, p. 79; ETA, pt. 5, p. 174; SIFMA, pt. 7, p. 73; NAFCU, pt 6, p. 157-159; Kinecta Federal Credit Union, p. 9.

[15] NAFCU, pt 6, p. 157-158, for more exact proposals as to what main principles should be in the federal law see id. p. 158.

[16] CUNA, pt. 5, p. 55; International Bancshares Corporation, pt. 1, p. 99; IG US Holdings, pt. 4, p. 70; Hexagon, pt. 1, pp. 56-57; SIFMA, pt. 7, p. 74.

Recommendations

- The OAG should clarify issues pertaining to the applicability of the Regulations in a non-binding compendium. Some hypothetical situations could be provided to better illustrate the scope and reach of the CCPA.

2.2. Notices and Privacy Policy

Notices to consumers about the personal information collected is one of the most discussed issues in the context of drafting the CCPA and Regulations.

Different Perspectives to Notification Requirements

Business and their representatives were wary about the inherent challenges in complying with numerous notification requirements. For instance, with regard to Section 999.305, some businesses have criticized the Regulations for imposing an extremely complex system.[17] It was submitted that Regulations will be impossible to implement in practice (e.g., notices could become extremely long),[18] that the newly imposed regime for notices is "a step backward",[19] or that the notice requirements too onerous and burdensome for small businesses.[20] Furthermore, it was argued that Section 999.305 will lead to abuse, fraud, and consumer fatigue.[21]

W359-1 (cont.)

However, the representatives of consumers express strong support to clear prior notices about the data collection practices and the fact such notices should be provided before or at the point of collection. In particular, consumer interest organizations submit that such rules definitely aid consumers in a better understanding of how their personal data is used.[22] Consumer rights groups and individuals also emphasize that such notices should be "easy to read and understandable to an average consumer," contain "plain, straightforward language," and that notices "avoid technical or legal jargon."

Representatives of data brokers and service providers noted that in many cases it is impossible to provide notices to consumers because they lack direct relationships with consumers.[23] A number of representatives of businesses as well as trade associations noted that the new obligations with regard to notice are unclear with respect to what needs to be disclosed, and

[17] APCIA, Sacramento, p. 25.
[18] Hopkins & Carley, pt. 5, p. 207.
[19] Looker, pt. 3, p. 140.
[20] NFIB et al., p7. 7, p. 27.
[21] Whitepages, LA Comments, p. 50.
[22] Privacy Coalition, p. 11-12
[23] Philip Recht, LA, pp. 64-65.

how, where, and when the notice should appear.[24] In some cases, business representatives noted that it is impossible to provide notices for each possible scenario in which business may be interacting with its consumers.[25] As a particular area of concern where such unforeseeability arises is communication with the consumers via the phone.[26]

> "So many notices and so much nested linking – it's privacy notice inception!"
>
> (Looker, pt. 3, p. 140)

The Requirement of Explicit Consent

One of the most controversial provisions of the Regulations appears to be Section (305(a)(5) of the Regulations, which provides that:

> *(5) A business shall not use a consumer's personal information for a 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.*

W359-1 (cont.)

Many of the industry representatives highlighted the fact that the CCPA does not contain the explicit consent requirement and that CCPA 1798.100(b) only requires notice.[27] It was submitted that by adding such explicit consent requirement the Regulations go beyond what is required by the CCPA,[28] is extralegal,[29] and can be only adopted in a legislative process.[30] Instead, it was proposed that establishing passive consent (i.e., simple notice) with an opportunity to opt-out would suffice.[31]

---

[24] PIFC, pt. 1, p. 182; The News Media Alliance, pt. 2, p. 2.

[25] APCIA, Sac., p. 26.

[26] APCIA, Sac., p. 26; PIFC, pt. 1, p. 181; Performant, pt. 3, p. 34.

[27] CFC, pt. 5, p. 112; Card Coalition, pt. 4, p. 172; ETA, pt. 5, p. 176.

[28] Card Coalition, pt. 4, p. 172; ETA, pt. 5, p. 176.

[29] The News Media Alliance, LA, p. 42.

[30] Gunderson Dettmer et al., pt. 5, p. 91.

[31] IG US Holdings, pt. 4, p. 69; PIFC, pt. 1, p. 182; CUNA, pt. 5, p. 56.

Consumer representatives supported the proposed wording of Section 305(a)(3) and the introduction of the requirement of explicit consent.[32] This is in line with the overall attempt of the CCPA to provide an opportunity for consumers to exercise more granular control of how their data is collected, processed, and used.

The stringent notification requirements imposed by the CCPA and Regulations have served as catalyst for debate about desirable approaches to provide more granular control of personal data to consumers. It goes without saying that most of the stakeholders would benefit if the notices are simple,[33] concise, and can be used in different contexts, uniform in certain domains (e.g. financial services, online social networks, etc.)[34] as well as technological environments (e.g., web, mobile).

One noticeable trend with regard to notices is to strive towards more simplicity and uniformity. For instance, privacy policies could be based on policy standards (e.g., those adopted by APEC, OECD, FIPPs).[35] Financial industry representatives have strongly supported the idea of model notices for financial services or real estate (rental) transactions.[36] The OAG could collaborate with various stakeholders in drafting non-binding model notices (e.g., Notice at or Before Collection, Notice of Right to Opt-Out, Notice of Financial Incentives, Updated Privacy Notice, Requests to Know, and Requests to Delete).[37] Such notices reduce the compliance burden[38] and offer some certainty.[39]

W359-1 (cont.)

Recommendations

- The OAG should pave the way to ascertain that consumers have more opportunities to exercise more granular control over their personal data and how it is used by individuals.
- The OAG should facilitate joint initiatives between different stakeholders in developing default templates of notices and privacy policy clauses.

[32] Privacy Coalition, p. 12

[33] Higgs, Fletcher & Mack LLP, pt. 5, p. 86.

[34] Looker, pt. 3, p. 140.

[35] Looker, pt. 3, p. 140.

[36] SF Fire Credit Union, pt. 1, p. 59; Fresno Credit Union, p. 10.

[37] Travis Credit Union, p. 9.

[38] NAFCU, pt 6, pp. 159-161.

[39] Travis Credit Union, p. 9; CUNA, pt. 5, p. 56; NAFCU, pt 6, p. 161.

3. Look to the Future: User-Centric Data Privacy

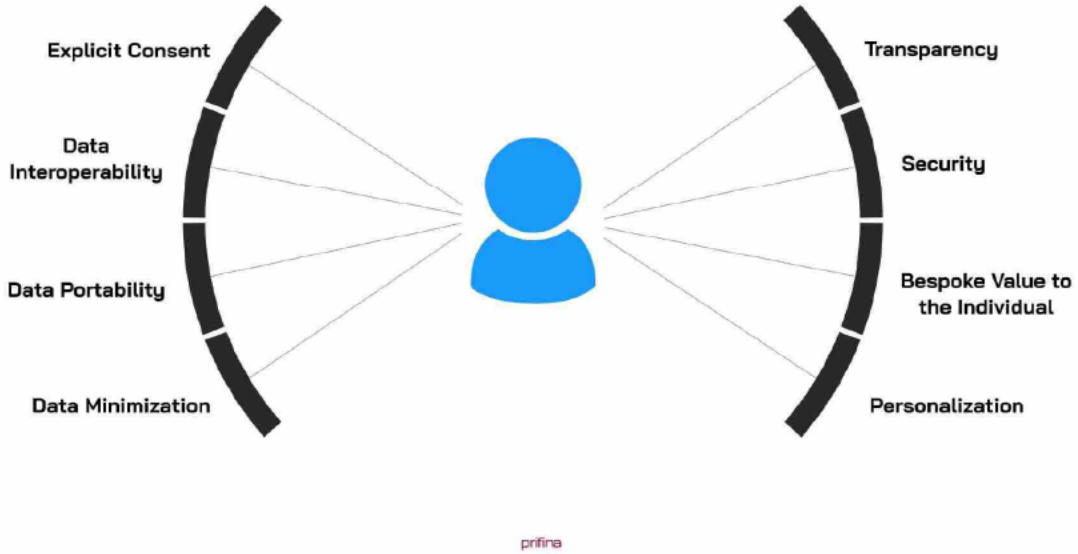
Insights and Proposals Based on Stakeholder Comments

Industry and a large portion of stakeholder comment submissions have raised many issues such as the complexity of compliance, notices to consumers and technical challenges associated with new privacy provisions, which relate to the consumer experience regarding the provision of services and products. The main concern is that the experience of going through notices, and disclosures would result in an onerous, hard to understand and complicated experience that would dampen and damage the consumer experience overall.

Prifina sees how data privacy ecosystem is shifting towards user-centric, user-held data privacy model. Taking this major transformation into account, Prifina has co-authored a proposal for Personal Data Use Licenses[40] which outlines a model where individuals can be presented with a set of standardized icons and language, which would correspond to enforcement of their rights under the CCPA and other regulations as relevant. We believe an open standard model for how right and privileges could easily be communicated can be a solution for the perceived complexity in implementing an optimal consumer experience in line with CCPA guidelines.

W359-1 (cont.)

User-Centric Data Privacy Model:
Key Principles



[40] Jurcys, Donewald, Globocnik & Lampinen, Note, My Data, My Terms: A Proposal for Personal Data Use Licenses, Harv. J.L & Tech. Dig. (2020), https://jolt.law.harvard.edu/digest/my-data-my-terms

This approach has been modeled on the success of the Creative Commons licenses and how those have become standardized and easily recognizable, also to the point of becoming included in the Unicode Standard. We propose the creation of a similar set of easily understandable and electable Personal Data Use Licenses, where the individual can make their own preferences known and exercise their rights to choose over their own personal data.

We believe that such a clear framework can provide value for all parties, namely:

- Making the user experience exercising one's rights and communicating one's preferences easy to understand, intuitive and effective.
- Making it easy for organizations to understand what individuals consent and do not consent to, and being able to provide services according to these choices.

In previous versions of the CCPA draft, there was discussion around a standardized button to make consumer experience optimal and clear. That suggestion does not exist in the current draft, and we submit that a framework for clearly standardized and easy to understand Personal Data Use Licenses could fill the need to bring transparency for the stakeholders involved.

W359-1 (cont.)

Further Prifina has proposed several other standards into the public domain, that relate to the data models and data profiles themselves, which can be utilized by the industry to bring easier public domain models that correspond and include the Personal Data Use Licenses as part of the data. These public domain data profiles can be found at:
https://github.com/libertyequalitydata

While we believe that different stakeholders are working on their own solutions to comply with CCPA, we see parallels from the Creative Commons example and other open-source initiatives, where open standards can be set in collaboration and the industry can converge on easy to understand, clear rules that become widely adopted and understood.

We have a lot of data -
and the technology to use it.
Responsibly.

Message

From: Jacob Snow [redacted]
Sent: 3/27/2020 3:07:03 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Privacy and Consumer Coalition Comments on Second Modified Draft CCPA Regulations
Attachments: 2020.03.27 - Privacy Coalition Comments re 2nd Mod OAG CCPA Regs.pdf

Office of the Attorney General,

Attached are comments from a coalition of privacy and consumer protection organizations regarding the Second Set of Modifications to Proposed Regulations under the California Consumer Privacy Act.

Best,

Jake Snow
Technology and Civil Liberties Attorney
ACLU of Northern California
he/him/his | [redacted] | @snowjake

Comments to the
California Office of the Attorney General

Notice of Second Set of Modifications to Proposed Regulations under The California Consumer Privacy Act

Submitted via Email to PrivacyRegulations@doj.ca.gov

March 27, 2020

On Behalf of the Following Organizations:

ACLU California

Electronic Frontier Foundation

common sense kids action

Privacy Rights Clearinghouse

Media Alliance

CFA

Oakland Privacy

ccfc Campaign for a Commercial-Free Childhood

consumeraction

CDD Center for Digital Democracy

CCPA_2ND15DAY_00375

Table of Contents

Introduction 3

Signing Organizations 3

No Delay of Enforcement is Warranted 5

Section 314(c). Keep the Service Provider Exception Narrow 5

Section 305(d). Mandate Transparency for Data Brokers 8

Section 315(d). Enforce Do Not Sell Through Do Not Track 8

308(c)(1)(g)(3). Clarify Treatment of Minors and Opt-In 9

Conclusion 10

Introduction

The undersigned group of privacy and consumer-advocacy organizations thank the Office of the Attorney General for its continued work on the proposed California Consumer Privacy Act regulations. As the regulations approach their final form, we urge the Attorney General to make the following revisions.

Preserve the CCPA enforcement date. Some industry interests have requested that the enforcement date of the CCPA be extended as a result of the public-health crisis associated with COVID-19. At this time, when so much of daily life is happening through the use of technology, the Attorney General should decline to postpone full enforcement of the CCPA. Now is not the time to weaken protections for consumers, many of whom are more vulnerable than ever. W360-1

Don't allow service providers to build comprehensive consumer profiles. Service providers enjoy a special status under the CCPA as a result of the narrow permission they have under the law to collect and use consumers' personal information. Allowing the construction of detailed consumer profiles using information collected as a service provider is flatly contrary to the purpose of the CCPA. The Attorney General should strictly limit service providers to making use of people's information for providing the specified service, and nothing more. W360-2

Require transparency from data brokers. The CCPA requires that businesses collecting personal information provide notice to consumers at the time of collection. That rule should apply with equal force to data brokers, whose collection and use of people's information pose grave privacy risks. W360-3

Enforce do not sell through do not track. Thousands of Californians have already enabled "do not track" settings in their web browsers. A business that cannot collect a person's information cannot sell that information, and the regulations should recognize that simple fact. The Attorney General should promulgate regulations that require businesses to treat "do not track" headers as requests to opt-out of sale. W360-4

Signing Organizations

The American Civil Liberties Union is a national, non-profit, non-partisan civil liberties organization 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.

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 Center for Digital Democracy's mission is to advance the public interest in the digital age. It is recognized as one of the leading consumer protection and privacy organizations in the United States. Since its founding in 2001 (and prior to that through its predecessor organization, the Center for Media Education), Center for Digital Democracy has been at the forefront of research, public education, and advocacy holding commercial data companies, digital marketers, and media companies accountable.

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.

Consumer Action uses multilingual consumer education materials, community outreach, and issue-focused advocacy to empower low- and moderate-income, limited-English-speaking, and other underrepresented consumers nationwide to financially prosper through education and advocacy.

The Consumer Federation of America is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education.

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.

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.

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.

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.

No Delay of Enforcement is Warranted

We understand some businesses have requested a delay in enforcement of the CCPA as a result of the public-health crisis associated with the response to COVID-19. We do not believe any such delay is justified in this instance. This is precisely the time we need to ensure strong protections for consumers. Technology is being increasingly relied upon for learning, socializing, working-from-home, ordering supplies, and many other activities. Californians are at a greater risk of being exploited under the guise of health, the prospect of employment, or safety. Profiting off of personal information may become more appealing to companies who are facing changes in revenue. The CCPA went into effect on January 1, and companies are already required by law to comply. Now is not the time to weaken protections for consumers, many of whom are more vulnerable than ever.

W360-1 (cont.)

Section 314(c). Keep the Service Provider Exception Narrow

Service providers have a special status under the CCPA. The information shared with them is excluded from the definition of sale, and as a result, consumers have no ability to opt out of the sale of information to service providers. CCPA Section 1798.140(t)(2)(C). Consumers are not entitled to know the categories of service providers who receive their information. CCPA Section 1798.110(a)(4) (limiting disclosure of categories to third parties). And finally, businesses enjoy special limited liability with respect to violations by their service providers. CCPA Section 1798.145(j). Therefore, the permissible use of people's information by service providers should be narrowly circumscribed. The second modified draft regulations

W360-2 (cont.)

would create a large and inappropriate carve-out for service providers to use personal information they obtain from businesses to profile consumers and households. If service providers wish to use consumers' personal information for such a wide range of purposes, they should comply fully with the CCPA.

The first modified draft regulations created an enumerated list of allowed activities that we feared would license service providers to use data in unexpected ways. *See* Privacy and Consumer Advocacy Organization Comments on Draft Regulations, p. 21 (submitted December 6, 2019) ("First Privacy Coalition Comments"). The second set of modifications does address one of our earlier concerns: we appreciate that the new draft narrows the carve-out in section (c)(1) to specify that processing must be "on behalf of the business that provided the personal information." But on the whole, we continue to believe that the regulations give service providers too much leeway to process personal data for their own purposes. Furthermore, the other change to the section is a step back for consumer protection.

Section (c)(3) previously granted service providers the right to use such data for internal purposes, but explicitly forbade use for purposes of "building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source." However, the second set of modifications adds the following italicized clause to section 314(c)(3):

> "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 *to use in providing services to another business,* or correcting or augmenting data acquired from another source;"

W360-2 (cont.)

This is a step backwards. In previous drafts, the regulations clearly stated that a company acting as a service provider may not use data collected in that role in order to build household or consumer profiles. Under the latest revisions, however, service providers may use any data they collect to profile people however the service providers want, as long as the profiles are not used "in providing services to another business." In other words, they can build profiles for themselves.

Some of the world's largest and most prolific tracking companies have already identified themselves as "service providers" for purposes of CCPA. For example, Google has added "service provider terms" as an addendum to its standard contract with publishers who use its ad technology.[1] Similarly, Amazon claims that it does

[1] *See Helping publishers comply with the California Consumer Privacy Act*, Google Adsense Help Center, https://support.google.com/adsense/answer/9560818?hl=en.

not "sell" information under CCPA, despite sharing data through an extensive behavioral advertising network.[2] Under the latest draft regulations, such companies will be able to use personal information they collect as service providers—from which consumers have no CCPA right to opt out—in order to build and augment consumer profiles for any internal use. This new exception would allow significant new intrusions on consumer privacy. It will incentivize large companies to enter into more "service provider" relationships in order to gather data for the purpose of building consumer profiles.

This is especially concerning given the draft regulations unjustified expansion of service providers to include companies that work with government entities. The latest draft regulations seem to imply that service providers may use personal information to build profiles for providing services to a non-business entity. This means, for example, that a "service provider" may collect personal information from relationships with private companies, use it to build profiles of consumers, and offer those profiles as a service to government entities like ICE.

W360-2 (cont.)

We request that 2nd 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.**~~

We stress the importance of removing section 314(c)(3) in particular. This section gives service providers broad license to use personal information for their own purposes, including by building consumer profiles using information collected from different businesses. That expansive permission contradicts the intent of the legislature and should be removed.

The second modified draft regulations further remove important protections for consumers whose information is collected by and held by data brokers. The changes in the second modified regulations should be removed so that consumers have a reasonable opportunity to know when data brokers collect and sell information about them.

---

[2] *See California Consumer Privacy Act Disclosures,* Amazon Help and Customer Service, https://www.amazon.com/gp/help/customer/display.html?nodeId=GC5HB5DVMU5Y8CJ2.

Section 305(d). Mandate Transparency for Data Brokers

Both the modified and second modified draft regulations represent steps backward in providing transparency to consumers who wish to understand and control how their information is being collected, used, and sold. The first draft regulations provided that, before a business that did not collect information directly from consumers could sell their information, efforts needed to be made to notify the consumer of their rights to opt-out, or confirm that the collection of information had, in the first instance, complied with the law. Draft Regs Sec. 305(d). A coalition of privacy and consumer-advocacy groups proposed concrete amendments to improve consumers' ability to exercise their rights. First Privacy Coalition Comments, p. 13–14. The Attorney General should adopt the coalition's proposal from those initial comments.

W360-3 (cont.)

Unfortunately, subsequent modified draft regulations have all but eliminated notice to consumers when their information is collected and sold by data brokers and other entities, many of which consumers have no knowledge of. Each subsequent revision of the draft regulations has further limited consumers' rights with respect to data brokers under the CCPA.

The first modified draft regulations allowed businesses *that do not collect information directly from consumers* to avoid providing notice-at-collection by including a privacy-policy link in their data-broker registration. Mod. Draft Regs. Sec. 305(d). The second draft regulations remove the requirement that the business not collect information directly from consumers, allowing *all* data-broker registrants to avoid notice-at-collection, even if the data broker collects information directly from consumers. 2nd Mod. Draft Regs. Sec. 305(d).

The change in the second draft regulations is a mistake. If a business collects information directly from consumers, it should provide robust notice at collection, whether it is a data broker or not. There is no reason why data brokers—whose business model is particularly pernicious to privacy—who collect information directly from consumers should provide any less notice than other companies who collect information directly from consumers. Therefore, the coalition proposes that the Attorney General adopt the following revision to 2nd Mod. Regs. Section 305(e).

> **A business that is** ~~**A data broker**~~ registered **as a data broker** with the Attorney General pursuant to Civil Code section 1798.99.80 et seq. ~~**the business**~~ does not need to provide a notice at collection to the consumer if **the information is not collected directly from the consumer and the business**~~**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.

Section 315(d). Enforce Do Not Sell Through Do Not Track

W360-4 (cont.)

The regulations require businesses to treat certain privacy controls as opt-out from sale. The second modified draft regulations are an improvement from the previous

round of modifications, but would still hinder consumer choice when compared with the original draft regulations.

We commend the removal of this clause from section 315(d)(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." Many consumers choose the software they use specifically to reflect their privacy choices. If a user selects a browser extension or application in order to protect their privacy, they should not also need to select a separate setting in order to enjoy one of the most important privacy protections granted by CCPA, the right to opt out of sale. This change removes perverse incentives that would have encouraged non-privacy protective defaults by companies.

W360-4 (cont.)

However, we continue to oppose the remainder of the text added by the first modifications at Section 315(d)(1): "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." As the coalition has explained before, 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. Thousands of Californians have already enabled this "do not track" browsing header. 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.

We remain concerned that some businesses may not interpret "do not track" headers as a "clear" signal that the consumer intends to opt out of sale. As detailed in previous comments, a desire to not have one's information tracked encompasses a desire not to have one's information sold. However, the latest regulations do not clearly require businesses to treat the former (a request to opt out of tracking) as indicative of the latter (a request to opt out of sale). They leave open the possibility that a business may ignore a Do Not Track request.

In short, please withdraw 2nd Mod. Reg. Sec. 315(d)(1). And per our earlier sets 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.

308(c)(1)(g)(3). Clarify Treatment of Minors and Opt-In

This section of the proposed regulations details privacy-policy requirements and would require companies to state "whether the business has actual knowledge that it sells the personal information of minors under 16 years of age." As a number of us explained in our comments on February 25 (Comments re Modified Reg. Sec. 308(c)(1)(e)(3)), this provision is unnecessary and should be struck.

W360-5

This language is unnecessary because the 2nd Modified Regulations already require that privacy policies provide the critical information parents or minors need to know in these circumstances. Specifically, privacy policies must provide a description of the process for opting-in to sale of information if companies allow this. That is detailed in Second Modified Regulation Sec. 308(c)(9).

It should be struck for a few reasons. First, the statement is confusing. It is unclear what effect, if any, it may have for a company to state whether it "has actual knowledge that it sells the personal information of minors." Whether a company has actual knowledge that it is selling minors' personal information, which includes willfully disregarding a consumers' age per the statute, is not something a company can disclaim in a privacy policy. Allowing a company to pretend to disclaim it is confusing.

W360-5 (cont.)

Second, requiring additional duplicative disclosures goes against the Second Modified Regulations' aim to require easy to read and understandable privacy policies. Privacy policies are already long.[3] Repeating largely duplicative information, separate from and without critical "how to" information about what consumers can do in response, should be avoided. Removing this requirement may aid in consumer comprehension and understanding and does not take away from the meaningful transparency requirements imposed by the CCPA.

We therefore request that the Attorney General strike 2nd Mod. Reg. 308(c)(1)(g)(3).

Conclusion

The coalition appreciates the Attorney General's work on these proposed rules and urges the Attorney General to take the steps recommended in these comments to ensure that consumers' privacy rights are protected.

[3] Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. Times Privacy Project (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

Message

From: HIZO THAI [redacted]
Sent: 3/22/2020 8:16:04 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Re: CCPA Regulations - Notice of 2nd Set of Modifications

I like to be a regulator with the ccpa to enforces it's law. With a badge. What does a ccpa , Uniform look like. I lived like this everyday. I see metro transit service violating everyday. Business corruption every day. I food service dishonesty everyday. I hear kid getting wrongfully thugout everyday. Senior citizen getting abused everyday. Business selling new car fraudulently. Drug dealer and lottery scam everyday! Laundrymat stealing everyday. I just want to get in work check and balance. Even for this super pandanmic. Sincerely Hai Thai W361-1

On Wed, Mar 11, 2020, 2:45 PM CCPA Mailing List <webmaster@doj.ca.gov> wrote:

March 11, 2020

CCPA Regulations - Notice of 2nd Set of Modifications

NOTICE OF SECOND SET OF MODIFICATIONS TO TEXT OF PROPOSED REGULATIONS

[OAL File No. 2019-1001-05]

Pursuant to the requirements of Government Code section 11346.8, subdivision (c), and section 44 of Title 1 of the California Code of Regulations, the California Department of Justice (Department) is providing notice of a second set of modifications made to the proposed regulations regarding the California Consumer Privacy Act.

The Department first published and noticed the proposed regulations for public comment on October 11, 2019. On February 10, 2020, the Department gave notice of modifications to the proposed regulations, based on comments received during the 45-day comment period. Subsequently, the Department received around 100 comments in response to the modifications. This second set of modifications is in response to those comments and/or to clarify and conform the proposed regulations to existing law.

This Notice, the text of the second set of modifications to the proposed regulations, and comparison of the text as originally proposed with both the first and second set of modifications reflected are available at www.oag.ca.gov/privacy/ccpa. The originally proposed regulations and all documents relating to the first set of modifications to the proposed text are also available at this website.

between Wednesday, March 11, 2020 and Friday, March 27, 2020. All written comments must be submitted to the Department **no later than 5:00 p.m. on March 27, 2020** by email to PrivacyRegulations@doj.ca.gov, or by mail to the address listed below.

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

All timely comments received that are relevant to the second set of modifications will be reviewed and responded to by the Department's staff as part of the compilation of the rulemaking file. Please limit written comments to those items.



You may find more information about the California Consumer Privacy Act (CCPA) on our website at: https://oag.ca.gov/privacy/ccpa

Please visit the remainder of the Attorney General's site at: https://oag.ca.gov/

Unsubscribe from this list

Message

From: [redacted]
Sent: 3/19/2020 7:45:50 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: RE: Chap 20 CCPA 2nd Set Mods TO TEXT OF PROPOSED REGULATIONS [OAL File No. 2019-1001-05]

W362-1

§ 999.301.(o) "Price or service difference"

Hi Lisa,

With regards to "Price or service difference" definition. You need to consider the time to delivery as a definition. Price or service difference cost can swing wildly if the duration or time to delivery is not specified. The term level indicates volume and not time to deliver goods or services.

Current 2nd Set Mod Clean:
(o) "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 collection, retention, 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 Page consumer related to the collection, retention, or sale of personal information, including the denial of goods or services to the consumer.

2nd Mod With My Changes:
(o) "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 collection, retention, 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, or time to delivery of any goods or services offered to any Page consumer related to the collection, retention, or sale of personal information, including the denial of goods or services to the consumer.

Clean incorporating my changes:
(o) "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 collection, retention, 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, quality, and time to delivery of any goods or services offered to any Page consumer related to the collection, retention, or sale of personal information, including the denial of goods or services to the consumer.

JB Eid
Founder and CEO
[redacted]
Safe And Sound Data LLC.

Message

From: Zoe Vilain [redacted]
Sent: 3/27/2020 9:48:12 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Pierre Valade [redacted]
Subject: Re: Comments regarding last proposed CCPA regulations
Attachments: 20200327 - Jumbo Privacy - 2121 Atelier - Comments on proposed CCPA regulations to California GA.pdf

Dear Deputy Attorney General Kim,

Please find attached a letter to your attention containing Jumbo Privacy's comments regarding the last proposed CCPA regulations.

Please disregard our previous email and attachment, as it was a working version.

I am available for any queries,
Sincerely,
Zoé Vilain

--
Zoé Vilain
Chief Privacy Advisor & Europe Representative of Jumbo Privacy
Featured in the New York Times, Bloomberg, The Verge, TechCrunch, FastCo

---

De : Zoe Vilain [redacted]
Date : vendredi 27 mars 2020 à 15:12
À : "PrivacyRegulations@DOJ.CA.GOV" <PrivacyRegulations@DOJ.CA.GOV>
Cc : Pierre Valade [redacted]
Objet : Comments regarding last proposed CCPA regulations

To the attention of Deputy Attorney General Kim

Dear Deputy Attorney General Kim,

Please find attached a letter to your attention containing 2121 Atelier Inc – Jumbo Privacy's comments regarding the last proposed CCPA regulations.

I am available for any queries,
Sincerely,
Zoé Vilain

--
Zoé Vilain
Chief Privacy Advisor & Europe Representative of Jumbo Privacy
Featured in the New York Times, Bloomberg, The Verge, TechCrunch, FastCo

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

March 27th, 2020

By email (privacyregulations@doj.ca.gov)

Subject: Written comments regarding the proposed CCPA regulations

Dear Deputy Attorney General Kim,

We write to you concerning the proposed modifications to the California Consumer Privacy Act ("CCPA") made on March 11, 2020. We are a company that is premised on the philosophy that consumer privacy is paramount, and our tools enable users to establish privacy controls across a host of CCPA-impacted businesses with a few simple steps. Our concern today is rooted in evidence that efforts are being made to roll-back these types of user-based controls.

As mentioned in our previous letter to you dated February 25, 2020, 2121 Atelier Inc. d/b/a Jumbo Privacy[1] has been acting as registered Authorized Agent in California for California residents, thanks to the introduction of such a role in the CCPA on Feb 1, 2020. Jumbo Privacy notably represents California consumers who request to opt-out of the sale of their personal information from consumer-selected businesses falling under the scope of the CCPA. Requests sent to a business by Jumbo Privacy on behalf of a consumer all contain the 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 the date of this letter, 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 the sale of personal information 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.

[1] Available at https://www.jumboprivacy.com/

Doc ID: 01d638d3716322661d6bd134744fe383f51548e9

We are concerned that proposed modifications to the CCPA might highly restrict the efficiency and opportunity for consumers to mandate an Authorized Agent. Therefore, we are addressing once again our suggestions and comments to the proposed rulemakings of the California Attorney General regarding provisions related to the concept of "Authorized Agent".

Specifically, our experience has demonstrated that every business falling under the scope of the CCPA should implement a dedicated communication channel with Authorized Agents, preferably an email address for the 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. We also read proposed amendments to Section 999.326(1) and (3) to place unnecessary hurdles between Authorized Agents and the effective and efficient consumer control of private information.

Consumers that mandate Jumbo Privacy as Authorized Agent to submit their requests 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 an Authorized Agent. We understand the importance of ensuring the validity of received requests to know or requests to delete. However, we would like to emphasize that providing an option for business to require the consumer verification of identity or request made through an agent might highly impair consumer rights by restraining the practicality to mandate an Authorized Agent.

We believe from requests we have made so far on behalf of consumers, that businesses may be tempted to use the presently proposed revisions to bypass an Authorized Agent's authority to act on behalf of said consumers. Therefore, we would suggest these additions to ensure that businesses may verify a consumer's identity only if the business can establish that the Authorized Agent has not provided reasonable proof of such consumer's identity or the existence of a valid mandate. These additions would prevent any unnecessary verification by the business, ensuring respect of the consumer's privacy rights.

Regarding Article § 999.326 - Authorized Agent, please find below our proposed amendments highlighted in yellow below:

« (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:*

W363-1

(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.

Doc ID: 01d638d3716322661d6bd134744fe383f51548e9

(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 reasonable 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.

(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."

W363-1 (cont.)

Regarding Article § 999.325 - Verification for Non-Accountholders, please find below our proposed comments in red:

« 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). »

W363-2

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 identifiers in the consumer's mobile device making the opt-out of sale request. In such cases, the consumer cannot change the advertising identifier. In order to protect the consumer's identity, which was never known to the business to which the request was issued in the first place, the opt-out of sale request only contains the advertising identifier of such consumer, to the exclusion of any other information. Adding a layer of verification of information for opt-out of sale request by permitting business to send notifications to the consumer upon receipt of such opt-out of sale requests would also highly restrict the benefits of mandating an Authorized Agent, where risks of security and error are practically null.

Doc ID: 01d638d3716322661d6bd134744fe383f51548e9

We remain of course at your disposal for any query,

Sincerely,



Zoé Vilain

Chief Privacy Advisor
Jumbo Privacy

Cc: Stacey Schesser, Supervising Deputy Attorney General
Privacy Regulations Coordinator, California Department of Justice

CCPA_2ND15DAY_00392

Doc ID: 01d638d3716322661d6bd134744fe383f51548e9

HELLOSIGN

Audit Trail

TITLE	Zoe Vilain 2121 Atelier Inc - comments on CCPA to California...
FILE NAME	Zoe Vilain 2121 A...California GA.pdf
DOCUMENT ID	01d638d3716322661d6bd134744fe383f51548e9
AUDIT TRAIL DATE FORMAT	MM / DD / YYYY
STATUS	• Completed

Document History

SENT	**03 / 27 / 2020** 16:40:53 UTC	Sent for signature to Zoe Vilain [redacted] from [redacted]
VIEWED	**03 / 27 / 2020** 16:41:10 UTC	Viewed by Zoe Vilain [redacted]) [redacted]
SIGNED	**03 / 27 / 2020** 16:41:28 UTC	Signed by Zoe Vilain [redacted] [redacted]
COMPLETED	**03 / 27 / 2020** 16:41:28 UTC	The document has been completed.

Message

[redacted]

==========

The following are my additional comments on the proposed revisions to the revised CCPA regulations published March 11.

* * *

In the definitions, the proposed revision to strike "disclosure, deletion or sale" in favor of "related to collection, retention or sale" is alarming, suggesting a significant expansion of the scope of the financial incentive provisions beyond the exercise of CCPA rights. This makes the interpretation of the regulations more difficult and I suspect significantly exceeds the statutory intent. W364-1

I believe that change is imprudent, overreaching, and probably at odds with the underlying statute. It should be reversed.

* * *

W364-2

I am disturbed and dismayed that you now propose to strike the sensible and beneficial guidance added in the previous proposed revision (§ 999.302, Guidance Regarding the Interpretation of CCPA Definitions).

This guidance served an important and vital function of reducing the overreach of these regulations. Businesses, including small businesses, may technically "collect" a wide variety of information that is neither retained nor reasonably capable of being associated with a specific individual or household, whether it's the IP addresses in a server log or the fact that a shop owner noticed that some customer in a crowd was wearing strong cologne. To treat those categories of information as "personal information" subject to the law's broad disclosure and deletion requirements is both wholly impractical and completely absurd.

To do so imposes a substantial burden — far more substantial than I think OAG recognizes — for little practical benefit to consumers. It also *encourages* businesses to catalogue and associate information in ways they would not otherwise contemplate, which is contrary to the intent of the CCPA. It also makes far more small businesses subject to the law than appears to have been the legislative intent. (By these rules, anyone who reads a daily newspaper may very well collect "personal information" on more than 50,000 people a year!)

I strongly recommend reinstating the guidance in the manner previously proposed.

* * *

W364-3

As I noted in my previous comments, and as other commenters like PBSA noted, the expectation in Section 999.315(c) that user-enabled privacy controls be treated as opt-out requests remains confusing and impractical. First, it's still not clear if the OAG intends this to be an option for businesses that wish to offer some kind of browser add-on or if it is intended to be an across-the-board requirement. If it IS intended to be an across-the-board requirement, it is a wholly impractical, technically infeasible expectation, unaccompanied by any technical standards or guidance for developers. I

can think of at least two dozen such privacy controls, none of which work the same way, none of which necessarily constitutes an opt-out request in the manner the law indicates, and many of which are designed to be invisible to websites visited. There's no way it's reasonable to expect businesses to navigate them all based on this vague provision.

I strongly recommend striking that section, or substantially revising it.

* * *

W364-4

I am also disheartened to see that the latest revisions still do not address the significant First Amendment grounds that SIIA raised in their comments of February 26. As they noted at that time, the statute and these regulations create substantial barriers to the lawful collection and dissemination of widely available information such as news items, publicly available professional contact information, and other data, treating it as equivalent to private information such as driver's license numbers. As SIIA noted, defining "publicly available information" to include ONLY government information is likely a First Amendment violation and a matter of grave concern to publishers, news services, and other services that depend on such information. I echo their recommendations that Attorney General Becerra add guidance expressly excluding widely available non-governmental information from the scope of the regulations.

However, adding such guidance, while necessary and significant, would not fully address the enormous First Amendment threat that the CCPA presents. The statutory language does suggest a legislative concern for free speech issues, but the degree to which that concern is reflected in the law or these regulations is not nearly sufficient or proportionate to the risk.

The scope of the issue may be best understood with reference to an illustrative example: Let us suppose that a well-known journalist compiles an extremely unflattering but wholly factual (and thus non-libelous) exposé on a well-known public figure, drawn both from publicly available sources and from the journalist's investigation of the public figure's career and conduct, including interviews with the public figure's associates. By definition, such a work and the journalist's notes for it would contain a great deal of personal information about the public figure.

The CCPA statutes suggest that the publication of such a work, which would clearly constitute journalism, would not be deemed a "sale," since "journalism or political speech" are not regarded as commercial activities by the law's definitions. This stipulation, however, leaves many unanswered questions regarding the application of the CCPA's rights of access, deletion, and opt-out, and how they would function in this example if the public figure attempted to exercise those rights to impede or suppress publication of the unflattering work.

For example, while the statutory language suggests that the CCPA would permit the journalist to reject a request to delete the public figure's personal information from the journalist's notes or manuscript on the grounds that doing so would impair the journalist's ability to exercise his or her free speech rights, could the public figure use an access request to compel the journalist to divulge his or her notes and sources? To what extent do the access rights permit such a journalist, or anyone else, to withhold or refuse to disclose certain information that also pertains to other individuals or households? (Even if the journalist could redact the names of sources such as interview subjects, providing access to the interview notes would likely identify at least some of those subjects.) The regulations limit a business's ability to divulge certain specific pieces of sensitive information about an individual, but additional guidance seems called for regarding situations where disclosure of personal information would unavoidably expose the personal information of others — and in particular in cases where doing so might place those others in legal or personal jeopardy!

If we suppose that a work of journalism is not a "sale" of personal information under the CCPA, a public figure could presumably not use an CCPA opt-out request to directly bar a journalist from writing or publishing an unflattering work. However, does that stipulation also apply to the journalist's literary agent pitching the work to publishers? If not, the public figure who became aware of the work prior to publication could use opt-out requests to prevent publishers from ever seeing the manuscript or even to prevent the journalist from obtaining or retaining literary representation.

If the journalist does secure a publishing deal, do the publisher's distribution and marketing of the work — which would necessarily include the public figure's name and certain other identifying details, and is clearly for the publisher's

W364-4 cont.

commercial advantage — constitute a "sale" of the public figure's information? If it does, the public figure could use opt-out requests to block publication of the unflattering work, forcing the publisher to terminate the publishing agreement and potentially subjecting the journalist to civil liability.

If the publisher's distribution and marketing of a journalistic work do NOT constitute a sale of personal information under the CCPA, what about the actual sale of copies of the book, at both the wholesale and retail levels? A bookseller selling a copy of a printed book or ebook to the public IS a sale by most common-sense definitions. If the CCPA regards it as such in this example, the public figure could block any actual sales or distribution of the unflattering work by strategically issuing opt-out requests to each bookseller and major vendor. (Given the ease with which the law and these regulations allow the filing of opt-out requests and businesses' limited ability to reject them, there is little obstacle to doing so.)

This scenario, while hypothetical, is not at all far-fetched, and it is easy to envision other, comparable situations with similarly grave implications for free speech and public participation. There are multiple ways politicians and other public figures could use their CCPA rights to block, suppress, or censor information they deem unflattering or simply don't want publicly aired (even where doing so would be in the public interest, such as in the case of a politician running for office). Since a CCPA access, deletion, or opt-out request is not a lawsuit, California's anti-SLAPP suit laws would likely provide little protection for journalists, writers, photographers, or publishers, or for the distributors and sellers who release the end product to the public. Worse, because the CCPA does not require an individual or household to live in California to be considered a California resident, any wealthy individual who owns property in this state could easily exploit these rights for purposes of censorship or harassment.

The Attorney General's failure to offer any substantive guidance or clarification on these alarming First Amendment concerns is disturbing. Does Attorney General Becerra wish California to become a national hub for efforts to suppress journalism, political speech, and public participation, in the way Virginia's lack of anti-SLAPP laws has recently invited a wave of frivolous defamation suits filed in that state? I fear that without significant corrective action on the part of OAG and the Legislature, such an outcome is almost inevitable.

Worse, the continued absence of coherent guidance may itself have a chilling effect on publishers, distributors, and retailers, causing them to preemptively avoid potentially controversial works of journalism (or even relatively uncontroversial biographies) on the grounds that the subjects of those works could completely block publication or sales by simply having an authorized agent fill out a few webforms.

These are serious constitutional issues of breathtaking scope and seriousness, and they demand clear response from the Attorney General that so far has not been forthcoming.

* * *

W364-5

Likewise, I am concerned that none of the matters I raised in my comments of Feb. 11 and Feb. 12 have been substantively addressed in the proposed revisions, particularly with regards to the strong potential for abuse of the request systems by pranksters or malicious actors.

Another commenter raised the possibility of altering the verification requirements to encourage, if not actually require, two-factor verification. I think this would be prudent to reduce the danger of frivolous and/or fraudulent requests.

The lack of verification for opt-out requests remains an obvious avenue for abusive or fraudulent requests, which these revisions still do not address.

* * *

W364-6

I noted in reviewing the published comments from the previous revision that some commenters feel the service provider exemption is too broad. I strongly disagree; I think both the statute and the regulations define the exemption

so narrowly as to treat a wide range of routine, perfectly legitimate good-faith business activity as "selling" personal information, to an extent without precedent in prior law.

I can only assume that neither those commenters, the Legislature, nor the Attorney General have any idea how much modern online activity relies on third-party infrastructure. A quick check reveals that OAG's own website uses at least three third-party service providers: Google (which serves some of your website's content via gstatic.com, google.com, and jquery.com, as well as providing the ubiquitous reCAPTCHA service used by many California government agencies), BootstrapCDN, and JSDelivr. Each of those services shares personal information (as defined by the CCPA) with those providers; indeed, the services could not function otherwise. Similarly, I'm sure many OAG employees, including the Attorney General himself, use Android or iPhone smartphones. Each of those devices constantly transmits personal information not only of the employee, but of other individuals with whom the employee interacts or communicates, to Google and/or Apple as well as other service providers.

The narrow definition of service provider means that a wide range of businesses that have websites, send or receive email, store data in cloud services, display Google Maps or embedded YouTube videos, or use smartphones are technically "selling" their clients' and customers personal information, even absent of any "sale" as the average consumer or established case law understand that term, unless the business has a very narrowly stipulated contractual agreement with all the applicable service providers. While Google (to name one common example) does offer service provider agreements or data processor agreements for certain of its commercial services, such as Google Ads and Google Analytics, I know of no such provisions for other widely used services such as Google Fonts, Google Hosted Libraries (which includes jquery.com), reCAPTCHA, or YouTube (which not only collects personal information, but also uses it for expressly commercial purposes such as display advertising, all of which are entirely outside the control of any website or online service that posts an embedded YouTube video).

Small or even medium-sized businesses have no leverage to demand such agreements from corporations like Google, nor have Google, Apple, Amazon Web Services, or the rest indicated any particular intention to offer them. Consequently, unless a business has some way to prevent consumers who have opted-out from viewing, for example, any YouTube videos posted on the business's website — from any device or browser, on any visit (which is technologically improbable) — many businesses will be technically unable to comply with the law's requirements.

The absurdity of this issue may become apparent when considered in regards to shipping agencies, a point raised by another previous commenter. A business that sends a letter or package to a customer must necessarily provide the customer's address to some shipping or delivery agency, whether the USPS or a common carrier like UPS or FedEx. An individual business does not have the ability to compel the Post Office or a common carrier to agree to a data processing or confidentiality agreement, or to respond to an access or deletion request from the business's clients and customers. While California-based couriers and common carriers may eventually incorporate such terms into their standard terms of service as a result of the CCPA, a California business has no way to demand that national or international services like USPS make such an agreement for each letter or invoice that goes out by postal mail.

By the standards of the law and these regulations, therefore, even responding to an opt-out request could be technically prohibited, since responding by any means would entail transmitting the recipient's personal information to some service for which the business almost certainly does not have and almost certainly cannot obtain a CCPA-compliant service agreement! (In that case, how a business could continue to maintain a business relationship with a customer who has opted-out — which the regulations' overbroad nondiscrimination rules expressly require — is a question for philosophy students: If you cannot legally communicate with the customer, cannot submit their payment information to a credit card processor or deposit their check in your account, and cannot deliver any goods or services to them, are they really a customer?)

If the business services exemption is intended to enable businesses to conduct their operations and provide their services within the online and business environment as it actually exists, the exemption is ridiculously, impractically narrow and needs to be significantly broadened.

W364-6
cont.

The exemption parameters need to be evaluated with input from stakeholders actually conversant with the technical and logistical issues involved. I propose that the Attorney General begin by having a serious conversation with the Office's own IT staff, asking the question, "If we were a business subject to the CCPA, could we comply with our own rules as stipulated?" I submit that the current answer to that question is very likely "no," which underscores the deep-seated limitations of both the law and these regulations.

Rules that are technologically and logistically infeasible will result in widespread noncompliance, much of it inadvertent, which will in turn make enforcement inherently arbitrary. They also provide an enormous, unfair advantage to large corporations and big businesses that either own their own infrastructure or can demand special dispensation from their vendors and service providers. Encouraging vertical integration and monopolization does not seem congruent with the legislative intent.

==========

[Comments end]

Message

From: Ferber, Scott [redacted]
Sent: 3/26/2020 2:11:35 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Farber, David [redacted]; Chittenden, Kelley [redacted]
Subject: Second Set of Modified Proposed California Consumer Privacy Act Regulations
Attachments: ACP-ltr-3-26-20.pdf; 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 second set of 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. ACP also joins the reasoned request from the coalition of trade associations, companies, and other organizations on March 17, 2020 that the Attorney General temporarily forebear from enforcing the CCPA until January 2, 2021, given the current health crisis and to allow businesses sufficient time to build processes that are in line with the yet-to-be finalized regulations. The attached supplements and incorporates our submissions from March 8, 2019, December 6, 2019, and February 25, 2020, which also are included for ease of reference. W365-1

Thank you for considering our comments.

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

King & Spalding Confidentiality Notice:

This message is being sent by or on behalf of a lawyer. It is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is proprietary, privileged or confidential or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately by e-mail and delete all copies of the message. Click here to view our Privacy Notice.

association of claims professionals



March 26, 2020

BY EMAIL

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: **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 second set of modifications to the proposed California Consumer Privacy Act (CCPA) regulations. We write to recommend adjustments 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, as underscored in our previous submissions, 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. To avoid those consequences, we therefore renew our request that the CCPA be amended to exempt 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. In addition, as a member of the broader business community, we join the reasoned request from the coalition of trade associations, companies, and other organizations on March 17, 2020 that you temporarily forebear from enforcing the CCPA until January 2, 2021, given the current health crisis and to allow businesses sufficient time to build processes that are in line with the yet-to-be finalized regulations. W365-1 cont.

This letter supplements and incorporates our submissions from March 8, 2019, December 6, 2019, and February 25, 2020 (which are attached for ease of reference).

ACP's Interest in Revising the CCPA Regulations

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.

Proposed Revisions to the CCPA Regulations

Given these important roles and responsibilities, and to ensure the most expedient claims management and administration, while avoiding consumer confusion and consternation, there must 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. §§ 999.301(h), [x] 999.301(i), [xi] 999.305(d), [xii] 999.313(c)(3), [xiii] 999.314(c)(1). [xiv] W365-2

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:

> 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.

Temporary Forbearance from CCPA Enforcement

We also join the March 17, 2020 request from trade associations, companies, and other organizations that you temporarily forebear from enforcing the CCPA until January 2, 2021. Recent, truly singular events stemming from the COVID-19 pandemic have encumbered businesses in their earnest efforts to operationalize the draft rules prior to July 1, 2020. As of today, 38 states, including California, have initiated orders or directives requiring the public to "shelter in place" or "stay at home."[xv] California has ordered "all individuals living in the State of California to stay home or at their place of residence except as needed to maintain continuity of operations of [16] federal critical infrastructure areas."[xvi] Violations are a criminal offense.[xvii] As emphasized in the March 17 request, "[d]eveloping innovative business procedures to comply with brand-new legal requirements is a formidable undertaking on its own, but it is an especially tall order when there are no dedicated, on-site staff available to build and test necessary new systems and processes… Now is not the time to threaten business leaders with premature CCPA enforcement lawsuits, particularly when the legal regime is not yet in its final form." A temporary enforcement deferral is appropriate and warranted and "would relieve many pressures and stressors placed on organizations due to COVID-19 and would better enable business leaders to make responsible decisions that prioritize the needs and health of their workforce over other matters." Though the CCPA directs the Office of the Attorney General not to bring an enforcement action before July 1, 2020,[xviii] the statute does not restrict the Office from providing an appropriate period of additional time for businesses to implement the final regulations before enforcement begins. As a result, we join the request that you temporarily forbear on enforcement of the CCPA until January 2, 2021.

W365-1 cont.

****

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,

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] "'Employment benefits' means retirement, health, and other benefit programs, services, or products to which consumers and their dependents or their beneficiaries receive access through the consumer's employer."

[xi] "'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."

[xii] "A business that does not collect personal information directly from a consumer does not need to provide a notice at collection to the consumer if it does not sell the consumer's personal information."

[xiii] "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."

[xiv] "A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except: (1) To process or maintain personal information on behalf of the business that provided the personal information, or that directed the service provider to collect the personal information, and in compliance with the written contract for services required by the CCPA; (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 to use in providing services to another business, or correcting 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 subdivision (a)(1) through (4)."

[xv] Executive Order N-33-20.

[xvi] Id.

[xvii] Cal. Gov. Code § 8665.

[xviii] Cal. Civ. Code §§1798.105(c).



association of
claims professionals

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:

W365-3

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.

W365-3 cont.

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:

> 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."



December 6, 2019

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 proposed California Consumer Privacy Act (CCPA) regulations and writes to suggest ways of improving the text of the proposed regulations to provide consistency and clarity to CCPA 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 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. We therefore submit this letter outlining suggested refinements to the proposed regulations. This supplements and incorporates our preliminary rulemaking submission from March 8, 2019 (attached for ease of reference).

W365-3 cont.

ACP's Interest in the Regulations

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.

Resolve Potential Consumer Confusion over Conflict of Law.

As shared in our March 8, 2019 submission, there are a number of existing California laws that appear to create competing obligations for our industry and others, including the California Insurance Code, Labor Code, and health laws. With that said, Section 1798.196 of the CCPA

provides that "[t]his title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution." The Act further provides that "[t]he obligations imposed on businesses by this title shall not restrict a business' ability to … comply with federal, state, or local laws… or exercise or defend legal claims." Section 1798.145(a)(1), (4). The Act then specifically calls out a limited number of statutory scenarios in which the CCPA would not apply, including under the Confidentiality of Medical Information Act, Health Insurance Portability and Accountability Act, Fair Credit Reporting Act, and Gramm-Leach-Bliley Act, as well as clinical trials.

W365-3 cont.

The imprecise language in the proposed regulations could be misconstrued to undercut this foundational principle. Respectfully, revisions are warranted. By way of example, the proposed regulations reference the conflict of law issue in guidance on responding to verified consumer requests to know, providing:

> 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....

Section 999.313(c)(5) (emphasis added). However, similar language is missing from that section's guidance on responding to verified consumer request to delete.

> In cases where a business denies a consumer's request to delete the business shall do all of the following:
> a. Inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including any statutory and regulatory exception therefor;
> 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.

Section 999.313(d)(6).

To avoid confusion, we respectfully request that this Section reinforce that such requests can be denied "**because of a conflict with federal or state law, or an exception to the CCPA.**" Section 999.313(d)(6)(a) should be amended to read:

> In cases where a business denies a consumer's request to delete the business shall do all of the following
> a. Inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including ~~any~~

~~statutory and regulatory exception therefor~~ if there is a conflict with federal or state law, or an exception to the CCPA.

W365-3 cont.

Greater Clarity on the Interplay of "Businesses" and "Service Providers"

The proposed regulations could also be misread to impede members' ability to duly carry out their lawful responsibilities. ACP companies respond every day to individuals and businesses who suffer a loss such as a 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, there are adjustments that should be made to the proposed regulations' guidance on Service Providers. In particular, Section 999.314 should be revised to bring more clarity to who qualifies as a service provider and what their duties are under the Act.

- Subsection (a) states a person or entity that provides services to a person or organization that is a service provider to also be a service provider under the law. More concrete detail is needed to define those relationships. For example, does a service provider pass on deletion requests to its own service providers, or does the business, as the CCPA text seem to indicate, have the responsibility to direct each and every service provider in the provision chain?

- Subsection (c) states that a service provider "shall not use personal information received 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." There is, however, a carve out for service providers' combining personal information received from one or more entities "to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity." To reduce confusion about the ability to share information between claimants and carriers, and remove unnecessary barriers to appropriate information sharing, the subsection should be revised to also allow the following sharing: "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, complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or otherwise perform

a contract between the business and the consumer, as well as where the combination is reasonably anticipated within the context of the service provider's business purpose."

W365-3 cont.

- Subsection (d) requires service providers that receive a request to know or delete from a consumer to "explain the basis for the denial" if the service provider does not comply with the request and to inform the consumer that the consumer should submit the request directly to the business. This provision would seem to impermissibly expand the Act's reach to require service providers to comply with obligations otherwise resting with "business." In addition, compliance with such a new standard would be unduly burdensome and create confusion about where the line should be drawn between service providers and businesses on request management. It should therefore be removed.

****

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,

Susan R. Murdock
Executive Director
Association of Claims Professionals
1700 Pennsylvania Avenue, Suite 200
Washington, DC 20006
Phone: [redacted]
www.claimsprofession.org

association of claims professionals

March 8, 2019

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

RE: **Preliminary Rulemaking Activities related to The California Consumer Privacy Act**

W365-3 cont.

Ladies and Gentlemen:

The Association of Claims Professionals (ACP) is pleased to respond to the request for comment on the Preliminary Rulemaking Activities related to The California Consumer Privacy Act (CCPA). While ACP members are strong proponents of individual privacy rights, we have significant concerns that the unintended application of the CCPA to claims professionals will cause widespread confusion and discord among California consumers and result in conflicting regulatory standards for our members. As such, for the reasons below, we ask the California Department of Justice to clarify the intent of the legislature that the CCPA does not apply to the activities of independent claims professionals.

ACP's Interest in Preliminary Rule Making Activities

ACP (formerly known as the American Association of Independent Claims Professionals or AAICP) was formed in 2002 as the only national association representing the interests of the nation's independent claims professionals. ACP members employ thousands of claims specialists and other professionals across the country and handle millions of property and casualty, workers' compensation, disability, and other liability claims annually. Membership is comprised of independent claims adjusters and third-party administrator organizations, many of whom handle claims administration responsibilities for California insureds and their carriers. ACP member companies employ thousands of adjusters in the State of California and manage billions of dollars of claims for California insurers and policyholders.

Comments on the CCPA

I. The Department Should Clarify that the Claims Adjusting Industry is Exempt from the CCPA.

1. The California Insurance Code, Labor Code, and health laws extensively regulate the claims adjusting industry in the area of transparency and privacy and already provide greater protection specific to insured consumers.

The CCPA was intended to fill in gaps in California privacy law, which is why the California legislature believes existing law should be construed to harmonize with the CCPA *if possible* but preempts the CCPA in the event of a conflict.[1] Moreover, California has specifically and comprehensively addressed transparency and privacy in the claims adjusting industry in a manner that provides greater protection to the consumer than what will be afforded under the CCPA when it is implemented. Given this extensive existing regulation, the Department should clarify that the CCPA does not apply to the claims adjusting industry to avoid conflicting regulation, an uncertain preemption analysis, and to protect consumers.

W365-3 cont.

Perhaps most notably, the California Insurance Information and Privacy Protection Act (IIPPA) regulates the claims management industry as "Insurance Support Organizations" in the context of certain insurance transactions for substantially the same purpose as the CCPA.[2] Indeed, not only are the purposes of the IIPPA substantially similar to the CCPA, but the protections contained within the IIPPA mirrors if not exceed much of the CCPA. For example, insurance institutions or agents must provide a "notice of information practices" upon delivery of a policy or collection of personal information that includes all of the information the CCPA would require *plus* the investigative techniques used to collect such information. Not only that, but California insureds already have rights pursuant to the IIPPA to access, amend, correct, and delete certain information in a manner that actually makes sense in the insurance context.[3]

Other aspects of the California Insurance Code, Labor Code, and health laws have also required transparency and privacy protection for years. Administrators must provide written notice explaining its relationship with the insurer and policyholder "agents of insurers" and face criminal penalties for unauthorized disclosure of confidential information. The Labor Code severely limits what medical information may be disclosed when processing worker's compensation claims.[4] Relatedly, where the CCPA allows requests for the disclosure of relationships with third parties related to a consumer's personal information, the Insurance Code already requires administrators to provide written notice advising insured individuals of the identity of details regarding the relationship between the administrator, policyholder,

---

[1] *See* Cal. Civ. Code §1798.175.

[2] *See* Cal. Ins. Code § 791 ("[T]o establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions by insurance institutions, agents or insurance-support organizations; to maintain a balance between the need for information by those conducting the business of insurance and the public's need for fairness in insurance information practices, including the need to minimize intrusiveness; to establish a regulatory mechanism to enable natural persons to ascertain what information is being or has been collected about them in connection with insurance transactions and to have access to such information for the purpose of verifying or disputing its accuracy; to limit the disclosure of information collected in connection with insurance transactions; and to enable insurance applicants and policyholders to obtain the reasons for any adverse underwriting decision."); Cal. Ins. Code § 791.02 (defining "insurance support organization).

[3] *See* Cal. Ins. Code § 791.08. Similar to the CCPA, access requests must be honored within 30 days, although unlike section 1798.100(d), the IIPPA allows a reasonable fee for the expenses incurred, which is not a difference in the level of privacy protection but rather a reasonable business practice. *See* Cal. Ins. Code §791.10.

[4] *See* Cal. Ins. Code §§ 1759.9, 1877.4; Cal. Lab. Code § 3762.

and insurer.[5] In the context of workers compensation insurance, "agents of insurers" are obligated to keep information confidential and face criminal penalties for unauthorized disclosure of such information.[6]

W365-3 cont.

As referenced above, in addition to the Insurance Code the California Labor Code also limits disclosure of medical information insurers and third party administrators retained by self-insured employers to administer workers' compensation claims receive to: (1) medical information limited to the diagnosis of the mental or physical condition for which workers' compensation is claimed and the treatment provided for this condition; and (2) medical information regarding the injury for which workers' compensation is claimed that is necessary for the employer to have in order for the employer to modify the employee's work duties.[7] Again, these protections are greater than those which will be afforded by the CCPA, arguing in favor of a blanket exemption from the CCPA for independent claims adjusters.

Beyond both the Insurance and Labor Codes, a third law -- the Confidential Medical Information Act (CMIA) -- also restricts the use and disclosure of any medical information claims professionals receive. For example, "[n]o person or entity engaged in the business of furnishing administrative services to programs that provide payment for health care services shall knowingly use, disclose, or permit its employees or agents to use or disclose medical information possessed in connection with performing administrative functions for a program, except as reasonably necessary in connection with the administration or maintenance of the program, or as required by law, or with an authorization."[8] Further, when claims professionals ("that provide[] billing, claims management, medical data processing, or other administrative services for providers of health care or health care service plans or for insurers, employers, hospital service plans, employee benefit plans, governmental authorities, contractors, or other persons or entities responsible for paying for health care services rendered to the patient receive medical information from health care providers and health care service plans") receive medical information from health care providers or health care service plans, they cannot further disclose the information in a way that would violate the CMIA.[9]

California has already enacted a significant body of law to increase transparency for and protect the privacy of insured California consumers. If the CCPA was interpreted to apply to the claims adjusting industry the result would be a complicated patchwork quilt of regulation that lessens, rather than increases, consumer privacy. Further, application of the CCPA to the claims management industry would result in uneven application of the law given that each company would need to apply a complicated preemption analysis to nearly every right in the CCPA and decide if existing law or the CCPA is more stringent in the particular scenario.

---

[5] *See* Cal. Ins. Code § 1759.9.
[6] *See* Cal. Ins. Code § 1877.4.
[7] *See* Cal. Lab. Code § 3762.
[8] Cal. Civ. Code § 56.26(a).
[9] *See* Cal. Civ. Code § 56.10(c)(3).

association of claims professionals

2. Where the CCPA may be said to apply, the law already contains explicit exceptions for key aspects of the claims adjusting industry, creating confusion for consumers.

W365-3 cont.

The application of the CCPA to the claims adjusting industry will result in widespread consumer confusion without providing additional privacy or transparency protections. Where the law could arguably be read to apply, the CCPA exempts nearly all of the personal information the claims management industry receives in order to process claims: medical information governed by the CMIA, protected health information (PHI) collected as a business associate under HIPAA, information collected as part of a clinical trial, information in consumer credit reports, and in some cases, financial information disclosed pursuant to federal and California law. It is unclear and debatable whether any remaining information that does not fit neatly into the above exempt categories would be subject to CCPA obligations.

Further, claims management activities will constantly trigger CCPA exceptions, particularly when it comes to deletion requests directly from consumers or indirectly from businesses subject to the CCPA. The application of exceptions, which are needed to comply with existing law, will create confusion and likely frustration for consumers trying to exercise CCPA rights.[10] For example, administrators will be exempt from deleting information related to transactions they are required to maintain confidentially in books and records and make available to insurers for at least five years pursuant to existing legal obligations.[11] In other words, insureds that lodge deletion requests in accordance with the CCPA rather than the proper procedure for the insurance context provided by the IIPPA will fall within an exception and therefore be rendered meaningless. This is why in addition to drafting the legal obligation exception to deletion requests, the CCPA repeats that the law is not intended to restrict the ability to comply with other laws.

As noted above, wherever the CCPA may be stretched to cover any remaining claims management activities that are not already facially exempt based on the category of information, the law will nevertheless constantly provide exception. Not only does this create a genuine question for members of the claims adjusting industry as to whether the CCPA is relevant to them, but it will undoubtedly create confusion and likely frustration for consumers and CCPA-regulated businesses that may not understand why the industry is exempt from complying with so many of their requests. To avoid both outcomes, the Department should issue a clear statement exempting the independent claims adjusting industry from the scope of the CCPA.

---

[10] The most common exceptions will include (1) to complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer; (2) to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business; (3) to comply with a legal obligation; or (4) to otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information. *See* Cal. Civ. Code §1798.105(d).

[11] *See* Cal. Ins. Code § 1759.3.

association of claims professionals

3. The California legislature did not intend the CCPA to further regulate the pro-consumer claims adjusting industry; the Department should make that explicitly clear.

W365-3 cont.

The preamble to the CCPA emphasizes the intent of the California legislature to create privacy protections in response to business practices proliferated by the age of big data, while acknowledging existing law has already provided such protection in various other contexts. California had the same concerns regarding transparency and privacy protection in the claims management and broader insurance industry and intentionally addressed these concerns effectively throughout the state's legal code. Claims adjusters are specifically covered by existing law. The adjusting industry works on behalf of individuals and businesses in times of need, such as the recent California wildfires, delivering an estimated $45 billion each year in claims payments. It would be deeply unfortunate if the CCPA were to unintentionally sweep up claims adjusters and double-regulate the industry, likely lessening today's existing protections. These unnecessary gray areas would disrupt functioning privacy compliance programs in the claims industry and even worse, burden claims recovery efforts from proceeding as quickly and smoothly as possible. It is clear that the California legislature intended the CCPA to exempt claims adjusters -- the Department's regulations should remove any ambiguity and clearly reflect that intent.

****

ACP appreciates the opportunity to provide comments on the Preliminary Rulemaking Activities related to the CCPA. If you have any questions concerning our comments, or if we can be of further assistance, please contact Susan Murdock at [redacted]. We thank you for consideration of these comments and welcome any further questions you may have.

Sincerely,

Susa R Murdock

Susan R. Murdock
Executive Director
Association of Claims Professionals
1700 Pennsylvania Avenue, Suite 200
Washington, DC 20006
Phone: [redacted]
www.claimsprofession.org

Message

From: Sara DePaul [redacted]
Sent: 3/27/2020 2:12:15 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Carl Schonander [redacted] Christopher Mohr [redacted]; Sharon Burk [redacted]
Subject: SIIA Comments on the Second Set of Modifications to the Proposed Text of the CCPA Regulations
Attachments: SIIA Comments on CCPA Regs 27 MAR.pdf

On behalf of the Software & Information Industry Association (SIIA), I submit the attached comments on the second set of modifications to the proposed text of the CCPA Regulations. Thank you for your consideration of our written submission.

Best regards,



Sara DePaul
Senior Director, Technology Policy
SIIA - The Software & Information Industry Association
1090 Vermont Ave NW, Sixth Floor, Washington, DC 20005
[redacted] Office / [redacted] Mobile / @saracdepaul Twitter
siia.net/policy

SIIA Accelerating Innovation in Technology, Data & Media

1090 Vermont Ave NW Sixth Floor
Washington DC 20005-4905
www.siia.net

March 27, 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 Second Set of Modifications to the Proposed Text of the CCPA Regulations

The Software & Information Industry Association (SIIA) [1] appreciates the opportunity to submit additional comments on the proposed regulations implementing the California Consumer Privacy Act (CCPA). We wish to begin by thanking the Office of the Attorney General for its leadership in drafting the proposed regulations, both with respect to its swift work and for offering stakeholders multiple opportunities to submit comments.

These comments, like our prior submissions, begin with our ongoing concern regarding the First Amendment defects created by the CCPA and the opportunity for the Attorney General to remedy these constitutional flaws through the rulemaking process. In addition, we ask the Attorney General to add a new provision protecting trade secrets and intellectual property rights, as contemplated by the CCPA. We also point your attention to several compliance issues raised by provisions in the proposed regulations, including requesting a modification to Section 999.305(e) to ensure that socially valuable business models, like those that gather information for the extension of business credit, are not destroyed by a compliance requirement that is impossible to meet.[2] We thank you for your consideration of our comments.

---

[1] As noted in our prior comments, SIIA is the principal trade association for the software and digital content industries. We have over 800 members spready across eight specialized divisions. SIIA members include software publishers, financial trading and investment services, specialized and B2B publishers, and education technology service providers. For more information on SIIA, our members, and our concerns regarding the proposed regulations, we refer you to our prior comments filed on **December 6, 2019** and **February 25, 2020.**

[2] Although we do not reiterate them here, we also incorporate our February 25 comments (*see*, fn. 1) that the Attorney General should revise Section 999.312(a) to not require businesses that operate online to maintain toll-free telephone numbers for requests to know.

W366-14

The Attorney General Should Use the Authority Granted by the CCPA to Add Provisions to the CCPA that Cure First Amendment Defects and Protect Trade Secrets and Intellectual Property Rights

W366-1

We reiterate our concern that the CCPA unconstitutionally interferes with commercial speech in a way that renders it vulnerable to a First Amendment challenge. As we have repeatedly noted in this and other fora,[3] the CCPA unconstitutionally restricts the communication of public domain information that is widely available from non-governmental sources. This includes data on or relating to public-facing websites, credential and licensing details (such as taxi medallions), biographical data, and other information drawn from registries, directories, news reports, and public social media channels. Consumers have a minimal, if any, expectation of privacy in this kind of information.

The First Amendment mandates that the government tightly draw the regulation of speech. Simply put, the CCPA fails in this regard. It subjects public domain information, in a vague and overbroad fashion, to near blanket rights of deletion in the service of an undifferentiated interest in privacy. That kind of statute neither advances a compelling government interest nor engages in the tailoring the First Amendment demands. It is plainly unconstitutional.

It is puzzling to us why the drafter of the pending ballot initiative has acknowledged this fact, but the Attorney General has not. The California Privacy Rights and Enforcement Act of 2020 (CPREA) defines personal information to ***exclude*** three categories of publicly available information: (1) public records; (2) "information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from ***widely distributed media***, or by the consumer;" and (3) "information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to specific audience." *See* Section 1798.140(v)(2) of the CPREA.[4] These are exactly the elements that we urged the legislature to adopt to address the First Amendment concerns raised by the CCPA as enacted.

---

[3] The CCPA's treatment of publicly available information has been a concern of SIIA's throughout 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 and February 25, 2020 written comments (*see* fn. 1, *supra*), which cite to a memorandum from our outside counsel, our December 26, 2018 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).

[4] The term "widely distributed media" is not new to California privacy law. The California Financial Privacy Act, for instances defines *nonpublic* personal information to exclude widely distributed media. *See* Section 4052(a).

The Attorney General has a unique opportunity to cure these constitutional defects through the authority given to him by the CCPA. Section 1798.185(a)(3) expressly gives authority to the Attorney General through the rulemaking process to establish "any exceptions necessary to comply with state or federal law . . ." The Attorney General can and should use this authority to cure the CCPA of its First Amendment flaws. The regulations could, for instance, adopt the ballot initiative language pointed to above. More simply, the regulations could include a definition for "publicly available information" that expands the CCPA's Section 1798.140(o)(2) exclusion to "widely distributed media." Either option will cure the defects that render the CCPA and its implementing regulation vulnerable to a First Amendment challenge. W366-1 cont.

Adopting this approach makes eminent policy sense. There is no organized opposition to the ballot initiative, and it wastes resources to have businesses change their practices twice. It also greatly reduces the state's exposure to what would be successful litigation challenging the CCPA on First Amendment grounds. We urge the Attorney General to use his authority to rectify the CCPA's First Amendment failings.

Additionally, we urge the Attorney General to use his authority under Section 1798.185(a)(3) to include a provision to ensure compliance with laws relating to trade secrets and intellectual property rights. Section 1798.185(a)(3) when read in full gives the Attorney General the authority to promulgate a regulation that establishes "any exceptions necessary to comply with state or federal laws, *including, but not limited to, those relating to trade secrets and intellectual property right*s. . . ." Yet, to date, the proposed regulations have not addressed laws relating to trade secrets or intellectual property rights, and how they may intertwine with the CCPA's provisions at all. **To correct this and comply with the CCPA's instructions, we urge the Attorney General to issue a regulation that establishes an exception to protect against violations of laws relating to the disclosure of trade secrets and intellectual property rights with respect to the CCPA's requirements in Sections 1798.110 to .135. To do this, we suggest adding a new provision as Section 999.319 that reads:** W366-2

> **§ 999.319 Intellectual Property and Trade Secrets.** 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 the business's intellectual property rights or result in the disclosure of trade secrets.

Section 999.305(d), As Proposed, will Decimate the Availability of Business Credit and Should Be Deleted

W366-3

The most recent modifications to the proposed regulations add a new and problematic provision at Section 999.305(d). This provision clarifies that a business that indirectly collects personal information about consumers does not have to provide notices at the time of collection *provided it does not sell the consumer's personal information*. This added provision is partially responsive to a concern we raised in our February 25 submission that focused on the need for the regulations to clarify that third parties that do not meet the definition of a data broker but collect personal information indirectly should not be required to provide notices at the time of collection. As proposed, however, .305(d) does not achieve the result we sought. Because .305(d) would only exempt such businesses from the notice requirement if they do not sell personal information, it will effectively create impossible compliance obstacles that will disrupt and even decimate valuable business models.

Take, for instance, businesses that indirectly collect personal information for purposes of compiling reports relating to the extension of business, rather than personal credit. While the CCPA excludes activities relating to the extension of *consumer* credit, it is silent on activities relating to *business* credit, which necessarily involves the collection and sale (as broadly defined by the CCPA) of the personal information of individuals who control the underlying businesses.[5] As currently proposed, Section 999.305(d) will require providers of business credit information to issue prior notices contemporaneous with collection, and filter out any personal information for which this cannot be done. This is not just Herculean. It is impossible.

For instance, the data collected often will not yield sufficient contact details for a compliance notice at or before collection. Even where it does, this requirement can be interpreted to require businesses to contact consumers directly, possibly even by telephone, in order to give the notice. In the context of business credit, this means contacting millions of consumers, a feat which simply cannot be achieved. As a result, the regulations force these businesses, including SIIA members, to choose between the cessation of this business model (which ultimately means they stop furnishing information for business credit determinations) or risk enormous fines that can put them out of business. This is neither a privacy win for consumers nor a benefit to our economy and SMEs.

---

[5] Business credit refers to the extension of financing to business entities. This is in contrast to consumer (i.e. personal) credit, which is regulated by the Fair Credit Reporting Act and bears on the creditworthiness of an individual. Although business credit involves the extension of credit to a business entity rather than an individual, the information relied upon for credit determinations may include personal information relating to the owners, officers, directors, or other individuals who control the business, particularly with respect to small businesses.

To avoid this outcome for business credit, and other socially valuable business models, Section .305(d) should be amended as follows:

W366-3 cont.

> A business that does not collect personal information directly from a consumer does not need to provide a notice at collection to the consumer if its online privacy policy includes instructions on how a consumer can submit a request to opt-out ~~does not sell the consumer's personal information~~.

Then, Section 999.305(e) should either be stricken or modified to make it mandatory for data brokers that register with the Attorney General to include the link to its online privacy policy that includes instructions on opt-out.

Section 999.313(c)(3) Needs Revised to Avoid Unfairly Burdening Business

W366-4

The CCPA's "right to know" requires a business to disclose personal information the business has collected about a consumer in response to a valid request from a consumer. The CCPA requires the Attorney General to promulgate regulations implementing these access request rights that "tak[e] into account," *inter alia*, "security concerns, and the burden on the business." Section 1798.185(a)(7). As proposed, Section 999.313(c)(3) recognizes that not *all* personal information a business collects about a consumer should be made available upon a valid access request. While we appreciate and agree with that outcome, the four-part test set out by the proposed provision sets the wrong standard for determining when information should not be disclosed. As currently proposed, Section 999.313(c)(3) is overly restrictive, fails to sufficiently address privacy and security concerns, and creates undue burdens for businesses. In short, the outcome of this provision as proposed is the antithesis of the privacy-protective goals of the CCPA and must be revised.

First, the provision is too restrictive by setting forth a four-part test that, in practice, cannot be met and thus will result in inappropriate disclosures of personal information. For example, the test conditions the withholding for a disclosure on a business not maintaining the personal information in a searchable or reasonably accessible format. This fails, however, to recognize normal business practices. For example, if a business maintains a consumer's personal information solely for legal or compliance purposes, then it necessarily has to maintain the information in a searchable or reasonably accessible format. If it did not, it could not search or access the information for its legal or compliance obligations. The provision as proposed, therefore, fails to meaningfully limit the scope of what must be provided in response to access requests because it fails to take into account routine and normal business practices and calibrate the standard accordingly. To overcome, this each of the four prongs on their own should provide a sufficient basis for not providing personal information covered by that prong.

Second, the provision as proposed fails to address the privacy and security concerns the CCPA was enacted to address. The outcome of this provision is to force businesses to create systems that enable them to search user-level data, which reduces individual privacy and creates security concerns by forcing businesses to associate more data with individuals than they otherwise would. For instance, many businesses log data and store it in a data warehouse, but not in a centralized profile. When this is done, it is difficult to impossible to retrieve data about a single user without either scanning potentially billions of lines of warehouse data or making copies of the data and centralizing. The first option is unfairly and overly burdensome. The second raises privacy risks because it results in the centralization of disparate data and for it to be indexed by user identifiers.

W366-4 cont.

With respect to security, the proposed provision fails to protect from the external disclosure of personal information that could pose a security risk to either a business's systems and/or networks (and by extension to the personal information of all consumers held by the business) by allowing bad actors to exploit systems or networks. Notably, the Initial Proposed Regulations appropriately recognized this, but the current proposal entirely abandons that initial and high standard. As initially proposed, this provision would have prohibited businesses from providing consumers with specific pieces of personal information if doing so would present "substantial, articulable, and unreasonable" security risks to the personal information, the consumer's account with the business, or the security of the business's systems or networks. To advance data security, this prohibition must be added back into the proposed provision. It will protect consumers and businesses alike.

Third, Section 999.313(c)(3) as proposed creates undue burdens for businesses, especially for SMEs. For example, many businesses possess personal information that is not readily searchable (and capable of being produced) on a user-level basis. Many businesses, for instance, maintain property or sales records in paper form that contain personal information of prospective customers. Retrieving personal information belonging to specific individuals in these records would be overly burdensome. This burden is exacerbated for those businesses, like SMEs, that lack the technical ability to identify which records may contain the personal information about the user. To meet the four-part test, however, a business would not be able to rely on the lack of searchability or accessibility alone as a basis for not disclosing the information. But these circumstances, when a business cannot readily search or access the data at issue, should be a basis on its own for not requiring a search for personal information. Not recognizing this unfairly and unnecessarily burdens businesses, particularly SMEs, which many of our members include.

We urge the Attorney General to revise Section 999.313(c)(3) before finalizing the regulations to avoid these problematic outcomes. We recommend the following revisions:

> A business shall not provide a consumer with specific pieces of personal information if the disclose would: (1) create a substantial, articulable, and unreasonable risk to the privacy or security of that personal information, the

consumer's account with the business, or the security of the business's systems, networks, or consumers; (2) interfere with law enforcement, judicial proceedings, investigations, or efforts to guard against, detect, or investigate malicious or unlawful activity or enforce contracts; (3) disclose the covered entity's trade secrets or proprietary information; (4) require the covered entity to re-identify or otherwise link information that is not maintained in a manner that would be considered personal information; or (5) violate federal, state, or local laws, including rights and freedoms under the United States Constitution. 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 ~~are met~~, provided the business describes to the consumer the categories of information it collects:

W366-4 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; or
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.~~

The Attorney General Should Add a New Provision Specifying that the Businesses Do Not Need Respond to Requests to Know with Duplicative Disclosures

W366-5

The Attorney General should insert a new provision at Section 999.313(c)(12) to specify that businesses do not need to provide substantially similar or duplicative information to consumers in response to requests to know. The CCPA recognizes there are limits to information that must be provided in response to requests to know. For instance, it permits a business to refuse to act on "manifestly unfounded or excessive requests." The proposed regulations should expand on this with respect to substantially similar or duplicative data, the provision of which can be disproportionately burdensome on businesses and not useful for consumers.

For example, a business might receive a request to know from a consumer and have the following specific pieces of information: (1) data indicating a consumer watched a video; (2) data indicating that a consumer watched at least 25% of a video; (3) data indicating that a consumer watched at least 75% of a video; and (4) data indicating that a consumer watched at least 90% of a video. Without a provision that specifies a business need not provide substantially similar or duplicative data, a business would be forced to provide all

of this data in response to a request to know rather than a single data point that would provide the requesting consumer with a meaningful understanding of the information the business has collected.

W366-5 cont.

To avoid these outcomes, the Attorney General should add a provision at Section 999.313(c)(12) that provides:

> In responding to a verified request to know categories of personal information, a business shall not be required to produce substantially similar or duplicative pieces of personal information.

The Attorney General Should Re-Insert the Guidance in Section 999.302 and Expand for Guidance on the Term "Collect"

W366-6

The notice of modifications to the regulations released on February 10, 2020 included a new provision at Section 999.302 that provide guidance regarding the interpretation of CCPA definitions. Unfortunately, the second and most recent modifications propose deleting this section. The proposed guidance, which focused on the definition for "personal information", was helpful and appropriate. It is critical for businesses that the Attorney General provide as much guidance as possible to help businesses overcome many of the compliance uncertainties raised by the CCPA. **We urge the Attorney General to reinstate 999.302 and expand on it to provide guidance on the term "collection."**

The guidance on the term "collection" should clarify that it does not refer to personal information that is generated internally, provided that such personal information is not transferred or disclosed to any third parties. This guidance aligns with the CCPA, which appropriately limits access rights to "collected" data and in defining collected, specifically and appropriately excluded a broader definition for "collect" as proposed by the ballot initiative that was the CCPA's genesis. Specifically, the CCPA does not define "collect" to include "making inferences based upon" personal information, as was proposed by the ballot initiative. This legislative choice was sensible, and the Attorney General's guidance should clarify that.

Section 999.314(c)(1) Should Be Modified to Allow Service Providers to Process Personal Information for All Businesses Permitted Under the Statute

W366-7

We are concerned that the modifications to Section 999.314(c)(1) do not align with the text of the CCPA. As you know, the CCPA defines "service provider" as a for-profit entity "that processes information on behalf of a business and to which the business discloses a consumer's personal information for a *business purpose*, pursuant to a written contract." Thus, by the text of the CCPA, a service provider's right to use personal information received from a business depends on what constitutes a "business purpose," under the CCPA. The CCPA, in turn, defines "business purpose" to mean "the use of personal information for the business's *or a service provider's operational purposes*, or *other notified purposes*." As other commenters have explained, this text plainly affords service providers with the flexibility necessary to process personal information not only for the business's purposes, but also for the service provider's own purposes provided that those purposes are necessary to perform the services specified in the contract. Yet, the regulations as currently proposed contemplate deleting the text that upholds this basic CCPA premise; namely to delete that service providers can retain, use, or disclose personal information obtained in the course of providing services" if it is to "perform the services specific in the written contract with the business that provided the personal information."

This proposed deletion is wrong, and fails to align with the text of the CCPA. **To correct this, the Attorney General should reinstate the language in 999.314(c)(1). Then, to clarify that the regulations are meant to be consistent with the CCPA, the Attorney General should modify subsection (c). The modified 999.314(c)(1) would be:**

> A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except <u>to the extent permitted by the CCPA, including</u> (1) <u>To perform the services specified in the written contract with the business that provided the personal information</u> . . .

The Proposed Regulations Continued Reliance on Global Privacy Controls for an Opt-Out Undermines Consumer Choice, and the Second Modifications Continue This Problem – Section 999.315(d)

W366-8

In our December 2019 submission, we urged the Attorney General to strike then-proposed section 999.315(c), which obligated businesses to treat global privacy controls as a valid opt-out request from the consumer even though it comes from a browser or device. We identified the many ways this curtails, rather than advances consumer choice and disrupts business. For instance, it weakens consumer choice by creating a legal assumption that browser-based privacy controls are the equivalent to an opt-out. It also ignores that that it

will result in overinclusive opt-outs, capturing consumers who did not exercise control but use a shared IP address or browser.

W366-8 cont.

As the modifications have developed, these problems have not gone away. Instead, your office continues to propose modifications that don't and cannot fix the problem, which is that this proposed requirement vitiates the individual choice that the CCPA was enacted to provide. The CCPA's focus is on allowing individual consumers to direct specific businesses not to sell their data. It does not contemplate or even suggest a single browser control that applies to all businesses for all consumers who may be identified by that browser.

More troubling, the most recent modification to this provision explicitly contravenes the CCPA's grant of an individual right to opt-out by removing the prior proposed requirement that such privacy controls cannot be designed with any pre-selected settings. Not only does this contravene the intentions of the CCPA, but it gives extraordinary and unwarranted power to browser publishers by allowing them to unilaterally turn on an opt-out and to even do it selectively for particular companies. **To resolve these concerns, the Attorney General should strike Section 999.315(d) in its entirety.**

The Regulations Should Not Require Misleading Disclosures About the Value of Data and Should Align the Definition of Financial Incentive with the CCPA – Sections 999.307(b)(5), 999.337, and 999.301(j)

W366-9

We reiterate the concerns raised in our February comments with respect to Sections 999.307(b)(5) and 999.337, which force businesses that offer financial incentives to provide estimates of the value of the consumer's data. It is a common misconception that a single or combined aspect of an individual's personal information has a unique value point that is capable of disclosure. In reality, the value of an individual consumer's data is impossible to calculate. As a general matter, data does not have an independent value. Its value, to the extent it can be discerned is subjective and in flux, often based on how it is aggregated. Even experts are flummoxed when estimating the value of data, often arriving at wildly different estimates for the same service. The regulations, as proposed, mandate unverifiable guesswork and ultimately will lead to meaningless and misleading value disclosures unrelated to the ultimate value of any offered financial incentives.

As we previously noted, the impetus for attempts to require this type of disclosure often come from the fundamentally flawed assumption that the value of data is tied to its advertising value because of its use by free ad-supported tools. With respect to ad-supported and free online services, individuals do not provide their data for their experience. Instead, their experience is possible because of the data. The core of these services is personalized content, which is made possible by the data. These businesses make money by selling ads and the metrics that determine the value of the ad placement, such as

the number of clicks or impressions. The data may influence the delivery of the ads, and thus give the consumer their personalize content, but the assumption that drives the value of the ad sales is wrong.

W366-9 cont.

To correct these flawed assumptions, and the mistake of forcing businesses to make misleading disclosures, we urge the Attorney General to strike Section 999.337 and to modify Section 999.307(b)(5) to read:

> An explanation of why the financial incentive or price or service different is permitted under the CCPA~~, including: a good faith estimate of the value of the consumer's data that form 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~~.

Relatedly, we also note that the updated proposed definition of "financial incentive" is broader than what the CCPA's provisions contemplated, which addresses *compensation* for *the sale or deletion* of personal information. The second proposed regulations contemplate significantly broadening the definition of "financial incentive" to capture much more than this. **To properly align the definition with the statute it implements, we recommend revising the definition as follows**:

W366-10

> Financial incentive means a program, benefit, or other offering, including payments to consumers, ~~related to~~ as compensation for the collection, ~~retention~~, deletion, or sale of personal information.

The Addition of the New Requirements for Privacy Policy Disclosures Strikes the Wrong Balance – Section 999.308(c)(1)(e)

W366-11

The recent modifications introduce two new disclosure requirements for privacy policies at Section 999.308(c)(1)(e) and (f). The second and less problematic addition is a requirement for privacy policies to identify the business or commercial purpose for collecting or selling information in a manner that provides consumers with a meaningful understanding for why the information is collected. Although we question the need for this late addition, we recognize that it presents few compliance concerns because the identification of the business purpose itself is a meaningful explanation for why the data is collected. The first addition in subsection (c)(e), however, strikes the wrong balance. It requires businesses to identify the categories of sources form which personal information is collected, which is sensible. It goes on to require that the "categories be described in a manner that provides consumers a meaningful understanding *of the information being collected*" rather than a meaningfully understanding of the identity of the source. This

could be read to imply that businesses need to describe the data collected from the sources. **To correct this, we urge the following revisions to Section 999.308(c)(1)(e):**

W366-11 cont.

> Identify the categories of sources from which the personal information is collected. The categories shall be described in a manner that provides consumers a meaningful understanding of the sources from which the information is ~~being~~ collected.

The Affirmative Authorization Requirements Strike the Wrong Balance and Should Be Revised – Sections 999.301(a) and .316(a)

W366-12

As we requested in our December and February submissions, the Attorney General should revise Sections 999.301(a) and 999.316(a) to remove the two-step verification process for consumers 13 years and older to opt-in to the sale of their personal information. A two-step verification, or double opt-in, fails to meaningfully advance while unduly interfering with consumer choice. It is not the job of the State to send signals to consumers that their affirmative choice is wrong by requiring them to confirm an already intentional opt-in.

W366-13

If this modification is not made, then at a minimum Section 999.316(a) must be revised to clarify that it is not intended to create a triple opt-in. As currently drafted .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 that means "the *affirmative authorization* that the business may sell personal information about the consumer…" *See* Section 999.301(t). In turn, affirmative authorization is defined to require a two-step process for obtaining consent and then confirming consent. *See* Section 999.301(a). Thus, the "request to opt-in" requirements contemplated by 999.316(a) require the two-step authorization as required by the definition for affirmative authorization ***plus*** a separate confirmation of the consumer's choice to opt-in. In practice, this can be interpreted as requiring a triple opt-in, which is absolutely unnecessary and will unduly interfere with consumer choice.

Conclusion

We again thank the Attorney General's Office for this opportunity to provide comments and suggested edits, and for your thoughtful leadership on the proposed regulations. We standby, ready to answer any questions or concerns that you may have.

Respectfully submitted,



Sara C. DePaul, Senior Director, Technology Policy
Software & Information Industry Association
1090 Vermont Avenue NW, 6th Floor
Washington D.C. 20005
www.siia.net

Message

From: Halpert, Jim [redacted]
Sent: 3/28/2020 8:10:47 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Kingman, Andrew [redacted]; Hurley, Megan [redacted]
Subject: State Privacy & Security Coalition -- Final Comments re AG_s Office CCPA Draft Rules version 3.0
Attachments: State Coalition -- Final Comments re AG_s Office CCPA Draft Rules version 3.0 March 27 2020.DOCX

Importance: High

Dear Sir or Madam,

Attached please find the comments of the State Privacy & Security Coalition, a coalition of 30 companies and 8 trade associations, regarding the March 11th version of General Becerra's proposed CCPA Regulations.

We hope that these are helpful as your office works to finalize the regulations and would be very happy to answer any questions you may have.

And most importantly, we hope that you and your families all are safe and comfortable through the COVID-19 stay home period.

With my best – Jim Halpert

Jim Halpert
co-Chair, Global Data Protection, Privacy & Security Practice
co-Chair, Global Cybersecurity Practice

T [redacted]
F +1 202 799 5441
M [redacted]

DLA Piper LLP (US)
500 Eighth Street, NW
Washington, DC 20004

DLA PIPER

dlapiper.com

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

State Privacy and Security Coalition, Inc.

March 27, 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 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 consumer privacy groups on amendments to clarify confusing language in the CCPA, to reduce the risk of fraudulent consumer requests that would create risks to the security of consumer data, and to focus CCPA requirements on consumer data, consistent with the title of the law.

We very much appreciate that the second set of proposed modifications to the draft Regulations issued on March 11, 2020, address a number of outstanding confusing aspects of the CCPA and recognize that service providers should be able to use personal information that they receive for cybersecurity and fraud prevention and internal purposes that do not involve sale or profiling for the service provider's own purposes (although we suggest a few additional changes to align with the statute). W367-1

At the same time, we urge the Attorney General's Office to amend the final rules to fix several apparent errors in the latest iteration of the draft Rules and to make them more workable before they are finalized.

II. The Definition of "Financial Incentive" Needs to Be Corrected

The reference to incentives "related to" information "collection" in the definition goes beyond the plain language of the statute and would needlessly complicate the already long CCPA mandatory privacy notices by requiring notice about all incentives for information collection. The newest revisions to § 999.301(j) define a "financial incentive" as a benefit related to the *"collection, retention, or sale of personal information."* This is a change from the February proposal which defined a financial incentive to W367-2

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

be a benefit related to the *"disclosure, deletion, or sale"* of personal information. These changes, as well as the continued reference to a benefit "related to" the collection, retention, or sale of data (as opposed to "compensation" which is the term included in § 1798.125(b) of the CCPA) is ambiguous.

W367-2 cont.

These revisions would be confusing to consumers and businesses alike, because consumers have no rights under the CCPA with regard to "discrimination" regarding information collection, and the CCPA does not regulate collection or place any restriction on incentives for collection. What is more, the term "related to" would create significant uncertainty for businesses and could be broadly interpreted to require lengthy disclosures regarding affinity and loyalty programs consumers enjoy.

This may be a simple drafting error, but it would have the effect of greatly complicating notices of financial incentives in ways that would confuse consumers with overly long notices. It is therefore not only contrary to law, but also unwise policy.

III. The Guidance of the Status of IP Addresses in Former § 999.302 Should Be Restored

W367-3

On balance, we believe that the guidance in former § 999.302 shedding light on when IP addresses constitute "personal information" provided helpful direction and that it should be restored.

In 2019, the definition of "personal information" was amended to exclude information that the business is not *reasonably* capable of associating or linking to a particular consumer or household.[2] In addition, the statute specifies that nothing in the CCPA requires that a business "reidentify *or otherwise link* information that is not maintained" in a manner that identifies or is reasonably capable of identifying a particular consumer or household.[3]

The CCPA's unusual definitions are often counter-intuitive and very difficult for lay users to understand. This clarification of how the definition of "personal information" applies to IP addresses would advance compliance and should be restored, adding a further caveat at the end: "If the IP addresses are aggregated or de-identified, they would also not be personal information." Alternatively, we request, to avoid further confusion, that the Final Statement of Reasons explain that this section was removed because it is unnecessary.

---

[2] AB 874 (adding the following italicized language: "'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: [enumerated examples, including IP address]").

[3] Cal. Civ. Code § 1798.145(l) (emphasis added).

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

IV. The Prohibition Against Charging Fees for Verification Should Be Removed as to Agent Requests or Verification of Authorization Should Be Made Easier

W367-4

The rules acknowledge that there are significant fraud and pretexting risks associated with data deletion and access requests. However, the modifications made to § 999.323(d) in the latest draft do not alleviate concerns we previously raised related to proper authentication of the Consumer-Authorized Agent relationship. The CCPA is at best ambiguous as to whether agents should be able to exercise these rights.

In fact, the requirements in § 999.323(d) that prohibit businesses from charging consumers for proper identity verification increase the potential for fraudsters to have a "free" shot at attempting fraud, and may well facilitate attempts to claim reimbursement for notarization fees associated with submitting powers of attorneys and inflating the demand for reimbursement.

This language would have the negative effect of discouraging the use of notaries, a commonly accepted method for legally authenticating the identity of an individual. The Uniform Statutory Form Power of Attorney (Cal. Probate Code § 4401) even references the attachment of a required notary certification.

When read in tandem with § 999.326(b), which explicitly references the Probate Code's requirements as a means for businesses to streamline the verification of Authorized Agents, the text in § 999.323(b) conflicts with § 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."

W367-5

Businesses required by the CCPA 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.

W367-4 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.

In any event, it is critical that businesses be able to confirm agent authorization directly with the California resident on whose behalf the agent purports to have authority to ask. Otherwise, the CCPA will become easy fodder for a wave of fraudulent requests. Moreover, the final rule should specifically allow businesses to verify the identity of the person holding the power of attorney. Without this commonsense clarification, the power of attorney provision could create a significant security loophole and invite fraudulent activity.

W367-5 cont.

V. The exception that businesses do not need to locate and retrieve personal information for legal or compliance purposes under certain conditions should be expanded

W367-6

§ 999.313(c)(3)(b) currently states that in responding to a request to know, a business is not required to search for personal information if *all* of the following 4 conditions are met: (a) "The

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

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." W367-6 cont.

We agree with the thrust of this exception. As we have previously explained, requiring deletion of or access to personal information that is not sold and is very difficult to retrieve (that is, information that is not maintained in a searchable or reasonably accessible format) is counter-productive to the privacy goal of the CCPA, as it requires that personal data be *more retrievable*. In fact, this requirement would go beyond the European Union's General Data Protection Regulation (GDPR), which generally imposes "proportionality" limits on user rights.

However, limiting this exception to information held only for legal or compliance purposes does not address this problem sufficiently. Businesses should not be required to engage in, and consumers will not benefit from, extraordinary eDiscovery searches to try to locate every bit of the broad range of personal information that are never used in the ordinary course of business and that might be located somewhere in their systems -- including in unstructured formats -- in order to comply with CCPA rights. This would create a perverse and anti-privacy incentive to make all this data that the business does not use and cannot easily retrieve much more readily retrievable and thereby more usable by the business.

Instead, we request that condition (b) above —which requires the information to be maintained "solely for legal or compliance purposes"— be stricken from the final rule. This would clarify that businesses need not engage in extraordinary eDiscovery searches to try to locate every bit of the broad range of personal information, where that information is not sold or used in the ordinary course of business, and the business so notifies the consumer. This change would also be consistent with § 1798.145(j)(3) of the CPRA Initiative.

VI. The Change to § 315(d)(1) Denying Businesses Responding to a Do Not Sell Signal the Ability to Present Users with an Option to Accept Sale Should Be Reversed in the Final Rules

W367-7

As we have stated in prior comments, we do not believe that this proceeding comes at the appropriate time to consider a Do Not Sell signal, because of the technical and operational complexity of the issue.

Version 3.0 deletes from § 999.315(d)(1) the sentence: "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". The clarity provided by the deleted language is important compliance guidance because otherwise it is impossible for organizations to tell whether a consumer intended to opt out of sale or whether they are simply receiving a default signal. This clarity would preserve the intent of the CCPA to provide an opt out from sale of data. Requiring an affirmative act by the consumer is at the very core of the CCPA framework. Accordingly, to avoid confusion, the first part of the deleted sentence must be restored to make it clear that an affirmative act is required by the consumer to express intent

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

to stop the sale of data. The second clause, referring to pre-selected settings, is inconsistent with both the first part of the sentence and the CCPA's emphasis on consumer choice. Consequently, the phrase "and shall not be designed with any pre-selected settings" should be deleted. This change would have the further advantage of avoiding the competitive risk of browser and other technology providers opting users out of competing services. W367-7 cont.

The ability of businesses who are complying with the Do Not Sell signal to present a page in order to encourage California residents with reasons to accept sale, including an offer in exchange for accepting sale, should be restored. This is likely required by the 1st Amendment. It also gives consumers the ability to "bargain with" websites, and is consistent with the CPRA Initiative.

VII. The Requirement that Businesses Inform the consumer with sufficient particularity that they have collected types of information that are Barred From Disclosure under § 999.313(c)(4) Should Be Removed and the Definition of "Biometric Data" Should be Clarified. W367-8

We strongly support the language now moved to § 999.313(c) prohibiting disclosing sensitive personal information that would trigger a breach notice obligation if obtained by an unauthorized person. However, this provision has been amended to require stating "with sufficient particularity" what types of information the businesses have collected. There are important security reasons not to notify fraudsters and hackers "with sufficient particularity" of specific types of sensitive data elements held that businesses are barred from disclosing. This often includes means of authentication, for example, that are targeted by these bad actors.

What is more, the CCPA does not require notice "with sufficient particularity." Instead, the statute states that businesses shall respond to a request to know categories of information with "reference to the enumerated category or categories . . . that most closely describes the personal information disclosed." If the information is too sensitive to disclose specifically, then the default should be the category disclosure required in the statute, not a newly created disclosure standard that risks informing fraudsters and hackers precisely what sensitive personal information a business holds.

Finally, as a technical drafting matter, we note that the CCPA contains a confusing and much broader definition of "biometric" data than the definition in Civil Code § 1798.81.5(d)(1)(A). The CCPA definition of biometric data reaches health or exercise data containing identifying information. § 1798.140(b). The final regulations should clarify that this prohibition applies only to biometric personal information as defined in Civil Code § 1798.81.5(d)(1)(A).

VIII. 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" W367-9

We reiterate our request to reinstate the important exception that was included in the original 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, the

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

consumer's account with the business, or the security of the business's systems or networks. The original exception was tightly drafted and addressed the very real risk of "pretexting" requests for personal information.

W367-9 cont.

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, cyber criminals and even foreign intelligence services may attempt to abuse the CCPA access right to obtain personal information about California residents to carry out illicit activities, commit fraud, engage in identity theft, access unauthorized accounts, or engaged in other harmful practices. If the Final Rules limit businesses' ability to protect against these threats only through verification procedures, businesses will not be able to prevent harm to consumers because bad actors may well be able to obtain the requisite number of verifying data elements through phishing or other tactics in order to falsify an authorization request.

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

IX. The Service Provider Conditions Should Be Modified Slightly to Account for Other Exceptions in the CCPA

W367-1 cont.

While we strongly support the service provider language, we note that the list of exceptions should be modified somewhat to make clear that service providers may perform other "business or operational purposes".

§ 999.314(c)(3) is more restrictive than the CCPA statutory language with regard to internal uses. The CCPA defines "service provider" as a for-profit entity "that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose, pursuant to a written contract."[1] Accordingly, a service provider's rights to use personal information received from a business depend on what constitutes a "business purpose" under the statute. The CCPA in turn defines a "business purpose" as "the use of personal information for the business's *or a service provider's operational purposes*, or *other notified purposes.*"[2] This statutory language on its face affords service providers flexibility to process personal information not only for the *business's* purposes, but also for the *service provider's* own purposes, at least as long as those purposes are necessary to perform the services specified in the contract.

[1] Cal. Civ. Code § 1798.140(v).

[2] Id. at § 1798.140(d) (emphasis added).

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

X. **The Requirement in § 999.305(a)(5) to Obtain Opt-in Consent for Specific Data Uses Is Inconsistent with the Statute.** W367-10

We appreciate that the explicit consent requirement in this section has been cabined somewhat through a "materially different" standard. However, we remain concerned that 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 statute provides. § 1798.100(b) clearly states that use of collected personal information for additional purposes should be subject to further notice requirements only.

The drafters of the CCPA required the further step of obtaining explicit consent from a consumer only for the sale of a minor consumer's personal information[3], participation in an entity's financial incentive program[4], or retention of a consumer's personal information for the purposes of peer-reviewed scientific, historical, or statistical research in the public interest[5].

Requiring explicit consent beyond these well-defined and clearly cabined use cases in the statute goes beyond the scope of the CCPA.

XI. The Final Rules Must Contain a Trade Secret and Intellectual Property Exceptions Provision W367-11

Before finalizing the rules, the Attorney General's Office should add a section addressing the scope of the trade secret and intellectual property exception, as required by § 1798.185(a)(3).

In some situations, CCPA access and data deletion rights can significantly impair intellectual property rights. For example, requiring deletion of evidence of trade secret theft or IP infringement interferes with discouraging infringement. Similarly, the right to know or access to specific pieces of personal data can, in some cases, require disclosure of trade secrets regarding data sources or combinations of personal data.

Accordingly, this proceeding should solicit comment on and set out rules to resolve these issues in order to fulfill this statutory requirement.

Respectfully submitted,

Jim Halpert, Counsel
State Privacy & Security Coalition

---

[3] Civ. Code §1798.120(d).

[4] Civ. Code §1798.125(b)(3).

[5] Civ. Code §1798.105(d)(6).

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

Message

From: Stauss, David [redacted]
Sent: 3/17/2020 1:56:31 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Status of CCPA Regulations and Enforcement Date

To Whom it May Concern,

W368-1

Due to COVID-19, do you anticipate delaying either the publication of the final CCPA regulations or the enforcement start date?

Thank you in advance for any information that you are able to provide.

David M. Stauss
Partner

HUSCH BLACKWELL LLP
1801 Wewatta St.,
Suite 1000
Denver, CO 80202
Direct: [redacted]
Fax: 303.749.7272
[redacted]
huschblackwell.com
View Bio | View VCard

Message

From: Showleh R El-Hage [redacted]
Sent: 3/19/2020 8:48:44 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Showleh El-Hage [redacted]
Subject: Surveillance with and Owl cam for Profit - Invasion of Privacy
Attachments: Surveillance with an Owl Cam for Undisclosed Use 1.doc

W369-1

Ms. Lisa Kim,

I am submitting a letter in which I am experiencing Electronic Stalking and yet there are no regulations clearly defined against mental and emotional distress as a cause of it. As a woman I have contacted all the government agencies necessary and yet it is hard to prove other than a log detailing time, duration of the camera on, what where the surroundings at the time and who was present.

Attached is a letter explaining invasion of privacy in a residential area and mainly targeted at a woman as I am more accessible to notice the surveillance aimed at our front door, front garden, front door, front driveway and mailbox from a fixed curb adopted for the last nine years.

sre

s roxanne el-hage

[redacted]

Surveillance with an Owl Cam for Undisclosed Use

W369-1
cont.

"Surveillance is the covert observation of people, places and vehicles which law enforcement agencies and private detectives use to investigate allegations of illegal behavior. These techniques range from physical observation to the electronic monitoring of conversations."

*"**Surveillance cameras** are video **cameras** used for the purpose of observing an area. They are often connected to a recording device or IP network, and may be watched by a **security** guard or law enforcement officer."*

My view

Large profits to be made through real estate sales, combined with commercial use of a property and/or properties in a residential area for warehousing construction materials, construction debris and also for purposes of construction pop-up work shops to expedite quickly accompanied by a new dash cam technology from Silicon Valley can be very impactful to residents and our society.

I am a resident of Menlo Park that is experiencing surveillance in a corner property, more specifically I am experiencing "close surveillance" and my observation and rational for this act is the correlation between the processes involved cosmetically, structurally and bureaucratically prep a house to complete a sale. The formation of groups and/or teams consisting of members with different expertise are formed including investors, real estate agents, lenders and contractors to facilitate the sale and to make the sale experience streamlines and quick.

Real Estate Market in the Bay Area

Zane Real Estate office analysis explains the 2019 Forecast written by Steve Price. Zane realty is a boutique real estate office that understands the supply and demand housing market of the peninsula: Palo Alto, Menlo Park, Redwood City, and Santa Clare and San Mateo Counties.

.

My Concern

Digital Civil Rights

a. - Eavesdropping,
b. - WIFI eavesdropping and borrowed WIFI with consent of a different resident for commercial use and gain.
c. - Privacy harm in a residential area.
d. - Stalking thorough technology.

W369-1
cont.

History of the surveillance

At the beginning of March of 2018, I observed that a commercial vehicle Ford Super Duty truck, that for our discussion purposes, we will call it **vehicle B,** had installed an Owl cam in its dashboard adjacent to my house. The street is approximately at a 2 to 5 degree angle. Although a wheel lock already is in place while parked, on this commercial vehicle, which is a second commercial vehicle of a contractor and owner of the car that is a room renter from another contractor's and landlord's house up the street in the Menlo Park, Unincorporated Area. This location is zoned a single family dwelling neighborhood.

The Owl cam is a new product and camera from a start-up company out of Page Mill Road, Palo Alto and the founder is Andy Hodge (Please refer to the You tube launching interview where the WIFI options after a year of purchase are explained). The company introduced its dash cam back in February of 2018. The camera can be purchased only through Amazon with an expensive price tag and most recently it is available for purchase through Best Buy and Ebay. In this scenario the tenant owns **car A** and **car B** and seems to monitor more times than none for his landlord. The times that I have observed the car camera screen on, coincide with activities for profit through scheduled of construction deliveries, scheduled arrival of co-workers, scheduled moving, scheduled transfer of construction and scheduled disposal of construction debris.

Strategic Curb Parking

The vehicle owner of **car B**, only parks in a strategic position located at the second house from the intersection of Alameda de Las Pulgas and Manzanita Avenue for the past eight and a half years and it hosts the Owl cam since March of 2018. When the camera is on it has a full view to the intersection, and beyond depending on the settings selected. This is something the manufacturer should disclose. According to customer service you can voice activate from a far through your cell phone.

Function of the Dash cam Camera

W369-1
cont.

Dash cams are meant for theft and accident protection while driving or stationary.

This model and technology allows surveillance while stationary.
This dash cam is randomly turned on when the vehicle is stationary and parked; it is on "watch mode". Since the dash cam owner and vehicle owner only parks adjacent to my house, it is few feet away from my recycling bins. The owner can activate it, store pictures, and video record while parked at any time since it has night vision. The car owner turns the dash cam on while walking towards vehicle. And it is on approximately six minutes after the vehicle is parked and a locked wheel bar is placed. The range and scope of the lens is modified and the angle of the camera is also often modified. The time length that the camera remains on while parking on arrival has increased.

Objective

Create policy on privacy protection of dash cam recording and viewing in residential areas, areas close to schools and areas close to public bus stops where students take the bus to school.

Surveillance for purpose of quick profit does not take into consideration, building permits needed for proper urban planning and raises privacy and security issues.

Quote: ***"Under what circumstances do privacy issues escalate into conflicts? "***

.

Contacted amd Reached for help, awareness
And future Policy Making

The following offices:

San Mateo Sheriff's Office
San Mateo Sheriff's Chief of Patrol
San Mateo Code Enforcement
Electronic Frontier Foundation
Board of Supervisor for my district: District 4
All Board of Supervisors for San Mateo County
Town Hall Meeting for San Mateo County
Town Hall Meeting in Palo Alto as the manufacturer is in Palo Alto
Electronic Frontier Foundation in SF

Kamala Harris's Office in Oakland
Nancy Pelosi's Office in San Francisco
London Breed's Office in San Francisco
Jackie Speier's Office in San Francisco
Anna Eshoo's Office in Palo Alto
Dianne Feinstein's Office in San Francisco
Anthony Portantino's Office in Sacramento
Ranking Digital Civil Rights
Danielle Citron's Office
Privacy Regulations Attorney General's Office

W369-1
cont.

The Patrol Sergeant of San Mateo Sheriff's Office came unannounced to see the set up from my house, the position of car B, and the location where the owner lives. He sent deputies to ask the truck owner and driver to see if he could park anywhere else such as at the driveway where he rents a room, the four car space in front of the house, or other curbs to the left, to the right or across and he refused.

Questions

1. - Who is monitoring what is being recorded beyond the thirty second allowances which is what California mandates?

2. – Surveillance gathers information that the owner of the dash cam and those that may share this information gain knowledge and advantage.

3. - The person watched and/or filmed through this device cannot combat this activity and is at a disadvantage.

4. – In this case the monitoring for commercial use from a house with parking strategy for disguise and formed a web consisting of two contractors living at the same residence, a real estate agent, and other outside specialty construction workers for quick turn around, to lower costs and increase profits.

5. - Currently, the dash cam owner uses **car A** as the primary vehicle, which is another smaller commercial vehicle parked always in front of where he lives. That car **doesn't have a camera** and is never parked at the curb where **car B** has used for eight and half years and the past year and a half it is still parked same place but now with and active Owl dash cam.

6. - The **blinking green lights,** that you see from the front of the camera that faces the front of the vehicle**,** the reflection penetrates into our residence both

upstairs and downstairs. The technicality is that it is not considered invasion of privacy, since it is not a beam we were told. However, my concern is that it has night vision.

W369-1 cont.

7. - "Deep fake" can be done on what is filmed and recorded.

8. - Is the manufacturer disclosing all features in its website? Does the launching interview of the founder Andy Hodge in his You Tube launching interview mention all WIFI capturing possibilities?

9.- After two years of increased monitoring it is beginning to feel like stalking as defamation of character is occurring with California utility workers in our street, presence at my work, harm to my property, and the question is who can help? Who can help a women and a homeowner?

WIFI Network

I had written a paper called Surveillance for Profit and spoke at the Town Hall Meeting in Palo Alto in early April.

As of April 17th, I noticed on settings of our Apple TV a new network named **NSA Surveillance Van 1**, is this for intimidation? I have been reaching out to government agencies and other organizations for awareness with my letter called: **Surveillance with an Owl cam for Profit**.

Walking up and down the street with my i-phone the WIFI reception is captured and the NSA Surveillance Van 1 network name appeared at a specific location and disappeared going up the street or going west. Does this network or the owner of this so called network feed the Owl Cam monitoring and recording for profit?

After the tenant of the location of the network "NSA Surveillance Van 1" moved the network called NSA Surveillance Van 1 disappeared. This deduction is through process of elimination. I am not technical, but I am learning though trial and error.

As of November, the dash cam is on when the truck owner comes to the truck from his residing location, up the street, and when he parks, the span of time it is on is approximately six minutes or beyond and it correlates with the **time to load into the car or unload building materials, electric tools and/or debris** to and from his rental.

In years past bagged construction debris was twice dumped in my blue recycling bin in years past, had I not noticed my address and named would have been tagged by the residential garbage removal company

W369-1 cont.

For a better visual understanding, please view google maps and start with 2110 Manzanita Avenue, Menlo Park, which shows the renter's white truck which is **car A in front of the house,** then continue with 2108 and finally view the white commercial **car B** that contains the dash cam at 2107 Manzanita curb. As you can see it is strategic for viewing Alameda de Las Pulgas and 2101 residence.

Through this snapshot and current experience I have learned that creating debate may lead to a better understanding in cyber policy making to enforce privacy protection and to improve digital rights from technological devices and its software.

I hope for better policy making protecting our digital civil rights. I thank you in advance for your cooperation in this matter.

Sincerely,

S. Roxanne El-Hage

Message

From: Carkhuff, Braden [redacted]
Sent: 3/27/2020 4:40:53 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Sutter Health Comments on the Second Set of Proposed Modified CCPA Regulations
Attachments: Sutter Health Comments to Modified Proposed CCPA Regulations.pdf

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

Thank you,

Braden Carkhuff

Braden Carkhuff
Privacy and Information Security Officer, Special Projects and System Enterprise
CCPA | Communications | Design & Innovation
Marketing | My Health Online | Philanthropy
Office of the General Counsel
Cell: [redacted]
Email: [redacted]



Quick Tip: Patient care and information doesn't belong on Social Media; be mindful of what you post.

Sutter Health

March 27, 2020

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

Re: Comments on the California Consumer Privacy Act's Second Set of Modified Proposed Regulations

Dear Attorney General Becerra:

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

Article 1. General Provisions

W370-1

§999.302. Guidance Regarding the Interpretation of CCPA Definitions

Issue with the Current Regulation:

The deletion of this section removes valuable insight and guidance in regard to the Attorney General's intent to regulate web analytics or other web-based services where only IP address is shared.

[Proposed] Regulatory Solution:

The Attorney General should provide additional guidance materials, for example, in the final Statement of Reasons, for determining what web-based information transactions constitute transfers and sales under the CCPA. By providing greater insight, the Attorney General will alleviate confusion in web technology services and will allow businesses to accomplish the intent of the CCPA.

Article 3. Business Practices for Handling Consumer Requests

W370-2

§999.313(d)(7). Responding to Requests to Delete

Issue with Current Regulation:

The proposed modified regulations now require a business to proactively reach out to an individual whose request to delete has been denied for any reason to opt out of the sale of their data if they have not already submitted a request to opt out. This requirement will be frustrating to a requestor as the business would be communicating that the business denying either a portion of the request or the entire request and will "sell" the data until the consumer opts out.

In the instance where a request is partially denied, the CCPA exception is required to be disclosed, unless prohibited by law. Businesses may not sell the data that is subject to the exception to deletion, but by pairing the notification to opt out of the sale with the notification that not all of the consumer's information is being deleted, it is reasonable that the consumer would understand that to mean the businesses sells the excepted data, when, in fact, the business does not.

W370-2 cont.

When the request is denied completely due to the business being unable to verify the consumer, the average consumer will not understand the difference between the verification requirements for deletion and opt-out and likely not understand why one request may be acquiesced and the other cannot.

Finally, providing a link to or contents of the notice, rather than the actual method of submitting a request to opt-out does not accomplish the goal of this section. If a business must ask a consumer if they would like to opt-out, then the business should be required to direct the consumer to the appropriate channel for an opt-out, rather than providing the notice of the right to opt-out.

[Proposed] Regulatory Solution:

This section should be modified as to not require a business "ask" the consumer whose request is denied if they would also like to opt-out. Instead, only the opt-out of sale of information or link should be provided in the response to the requestor of a deletion request that cannot be verified. Additionally, the information communicated to the consumer should direct the consumer to the method or channel of opt-out, rather than providing the notice of opt-out of the sale of personal information.

§999.317(g) Training; Record-Keeping

W370-3

Issue with Current Regulation:

The current regulation states that a business that knows or reasonably should know that it, 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. However, it is unclear if that number is unique consumers or the number may be derived from duplicate consumers. Additionally, if a business utilizes or directs a service provider to collect the personal information of the consumers, and does not receive the personal information of those consumers, must the business account for the consumers collected by the service provider?

[Proposed] Regulatory Solution:

The reporting requirement should be based on 10,000,000 unique consumers. Additionally, the information collected by a service provider at the request of a business should not be included in the threshold for reporting if the business does not receive the personal information of the consumers from the service provider.

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

Sutter Health

Respectfully,



Jacki Monson
Chief Privacy and Information Security Officer
Sutter Health

Message

From: Courtney Jensen [redacted]
Sent: 3/27/2020 3:50:34 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: TechNet Comment Letter Regarding Proposed CCPA Regulations
Attachments: TechNet CCPA Regulation Letter 3.27.20.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

March 26, 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. As the enforcement date quickly approaches, the CCPA continues to contain unclear requirements that raise significant operational and compliance problems that do not advance privacy or data security. We respectfully request a delay in the effective date of these regulations. Given the breadth and scope of the regulations, it would be difficult to achieve compliance by July 1st under the best of circumstances. Given the current COVID-19 crisis that is severely impacting working conditions for the near future, nearly all personnel are working remotely, including the technical teams that are critical to designing, testing and implementing the necessary online flows and behind the scene mechanisms, which in turn will create a suboptimal experience for consumers attempting to exercise their rights under CCPA. These same teams are also working on their companies' response to COVID-19, supporting essential businesses and keeping essential service running for their customers. Such conditions have negative impacts on productivity, the consumer experience and a direct impact on the ability to comply with these broad regulations, the final form of which is still unknown. We urge enforcement to be delayed until January 2, 2021. W371-1

As we have noted previously, compliance has already been costly for businesses throughout California, estimated at $55 billion according to a report prepared for your office, and every small change to the requirements of AB 375, via Attorney General W371-2

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. W371-2 cont.

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

§ 999.301. Definitions

- TechNet recommends the following revisions to the definition of financial incentive, *"(j) Financial incentive means a program, benefit, or other offering, including payments to consumers, ~~related to~~ as compensation for the use ~~collection~~, ~~retention~~, deletion, or sale of personal information."* W371-3

§ 999.302. Guidance Regarding the Interpretation of CCPA Definitions

- The Attorney General should re-insert this subsection and, pursuant to that section, issue guidance regarding the term "collect." W371-4
  - Specifically, the guidance should clarify that "collect" does not refer to personal information that is generated internally about a consumer, provided such personal information is not transferred or disclosed to any third parties.
  - It is appropriate to exclude information generated internally from disclosure in response to access requests because providing such information would impose significant burdens on businesses without corresponding benefits to consumers, who are likely to be confused by receiving such information. For example, businesses often generate internal information for reporting and other mundane business reasons. This internal information is not provided by a consumer or acquired from third parties, nor is it shared externally. It is used only for internal business reasons.
  - The CCPA appropriately limits access rights to "collected" data and, in defining "collected," specifically excluded language from the CCPA ballot initiative that defined "collect" more broadly, to include "buying, renting, gathering, obtaining, storing, using, monitoring, accessing, **or making inferences** based upon, any personal information pertaining to a consumer by any means." If the CCPA required businesses to return *all* generated data, including inferences, in response to consumer access requests, in many instances, businesses would have to build new systems for searching for them and collecting them in a centralized way. This is because generated data is commonly not maintained in a human-readable way.

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

- 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 W371-5

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. W371-5 cont.

§ 999.307. Notice of Financial Incentive

- The draft regulations articulate standards by which businesses can calculate the "value" of consumer data. However, 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. Specifically with respect to free, ads-based, 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 ad-based services to provide the core of the service itself, which is personalized content. W371-6
  - For the reasons above, we strongly recommend removing any requirements for providing an estimate of the value of consumer data.
  - We also recommend revising the updated definition of "financial incentive," which appears broader than the statute.
  - Accordingly, the draft language in (b)(5) 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 and compliance with this requirement would be near impossible. We urge that this requirement be struck from the draft regulations. W371-7

Article 3. Business Practices for Handling Consumer Requests

- One of the foundational consumer rights under the CCPA is the consumer right to access personal information about that consumer. Importantly, the statute recognizes practical qualifications to that right to ensure businesses can comply with consumers' requests and that privacy and security can be maintained. As described below, we encourage the Attorney General to better align the proposed regulations with the statute.

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

- § 999.313 (c)(3) is overly restrictive, creates undue burdens for businesses, and increases privacy and security concerns. W371-8
  - 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 Attorney General's Office to promulgate regulations for access requests that "*tak[e] into account*," *inter alia*, "*security concerns, and the burden on the business.*" See § 1798.185(a)(7).
  - (c)(3) properly recognizes that not *all* personal information a business has collected about a consumer needs to be made available. We appreciate and

agree with the recognition that an absolute access requirement is not desirable or consistent with privacy best practices.

- (c)(3) is also overly restrictive and does not sufficiently recognize privacy concerns or undue burdens. As currently drafted, (c)(3) contemplates a four-part test that is of limited utility, because little is likely to meet all four prongs. For example, if a business maintains the personal information solely for legal or compliance purposes, then it necessarily has to maintain it in a searchable or reasonably accessible format. If it did not, it could not search or access the information for its legal or compliance obligations. Or, if a business maintains personal information "solely" for legal or compliance purposes, then it cannot sell the personal information because it maintains the information for discreet legal or compliance purposes. In these ways, (c)(3) does not meaningfully limit the scope of what must be provided in response to access requests. Each of the prongs, on their own, should provide a sufficient basis for not providing personal information covered by that prong.
- (c)(3) also does not sufficiently address privacy and security concerns. Having to create systems that enable searching user-level data is not only burdensome but would actually reduce people's privacy and create security concerns by associating more data with people than otherwise would be. For example, log data stored in a data warehouse may not be stored in a centralized profile, making it difficult to retrieve data about a single user without (a) scanning potentially billions of lines of warehoused data, or (b) making copies of the data and centralizing it, thus raising privacy risks by requiring businesses to centralize disparate data and index it by user identifiers. Additionally, there may be specific pieces of personal information that businesses collect and maintain that, if disclosed externally, could pose security risks to either the business's systems or networks or consumer personal information by allowing bad actors to exploit systems or networks. The 2019 draft regulations appropriately recognized these scenarios and would prohibit businesses from providing consumers with specific pieces of personal information if doing so would present "*substantial, articulable, and unreasonable*" security risks to the personal information, the consumer's account with the business, or the security of the business's systems or networks. This prohibition should be added back to the final regulations to protect both consumers and businesses alike. Additionally, the draft regulations should recognize other important qualifications for when a business should not have to provide consumers with specific pieces of information.
- Finally, (c)(3) creates undue burdens for businesses. Many businesses possess personal information that is not typically readily searchable (and able to be produced) on a user-level basis. For example, businesses may maintain property or sales records that contain personal information of prospective customers, sometimes in paper form. Retrieving personal information belonging to specific individuals in these records would be overly burdensome if the business lacks the technical ability to identify which records contain personal information from the user. Because that data is not readily searchable or in a reasonably accessible format, under

W371-8 cont.

that factor alone, businesses should not be required to search for personal information within that data.

- To address all the concerns shared above, we recommend the following revision to (c)(3),
  - *"A business shall not provide a consumer with specific pieces of personal information if the disclosure would: (1) create a substantial, articulable, and unreasonable risk to the privacy or security of that personal information, the consumer's account with the business, or the security of the business's systems, networks, or consumers; (2) interfere with law enforcement, judicial proceedings, investigations, or efforts to guard against, detect, or investigate malicious or unlawful activity or enforce contracts; (3) disclose the covered entity's trade secrets or proprietary information; (4) require the covered entity to re-identify or otherwise link information that is not maintained in a manner that would be considered personal information; or (5) violate federal, state, or local laws, including rights and freedoms under the United States Constitution."*
  - "*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 information it collects: 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; or c. The business does not sell the personal information and does not use it for any commercial purpose."*

W371-8 cont.

- TechNet recommends that the Attorney General specify that businesses need not provide substantially similar or duplicative pieces of personal information to consumers in response to their requests to know.
  - The CCPA already permits a business to refuse to act on "*manifestly unfounded or excessive requests*," recognizing that there are limits to information that must be provided to consumers in response to requests to know. Similarly, there are other instances in which it would be useful to limit the information required to be provided to consumers. For example, providing consumers with substantially similar or duplicative pieces of personal information would be disproportionately burdensome on businesses and not useful for consumers. An illustrative example is useful here. A business might keep the following specific pieces of information about a consumer: (1) data indicating a consumer watched a video; (2) data indicating that a consumer watched at least 25% of a video; (3) data indicating that a consumer watched at least 75% of a video; and (4) data indicating that a consumer watched at least 90% of a video. In response to a consumer's request to know what personal information a business has collected about her, the business should need only to produce a single data point to provide a consumer with a meaningful understanding of the information it has collected.
  - Accordingly, TechNet recommends the following new text:

W371-9

- *"§ 999.313 (c)(12) In responding to a verified request to know categories of personal information, a business shall not be required to produce substantially similar or duplicative specific pieces of personal information."*

W371-9 cont.

- § 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 proposed rule improperly 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 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.

W371-10

§ 999.314. Service Providers

- The CCPA regulations should allow service providers to process personal information for all business purposes permitted under the statute. In response to the initial draft regulations, several commenters raised concerns that the regulations' restrictions on service providers' use of personal information did not align with the text of the CCPA statute.[1] As many commenters recognized,[2] this not only makes the regulations susceptible to judicial challenge, but also creates regulatory uncertainty that frustrates businesses' ability to engage service providers to efficiently and effectively perform tasks critical to offering products and services to California consumers. The second set of CCPA regulations appear to create anew the problems presented by the initial draft service provider regulation. We urge the Attorney General to further clarify (through the text of the regulations and the Final Statement of Reasons) that the regulations allow service providers to process personal information for any "business purpose," as that term is defined in the statute. Specifically, the regulations should make it clear that a service provider may use personal information for any "operational purposes" enumerated in Section 1798.140(d) of the statute permitted under the written agreement between the business and the service provider without introducing non-statutory restrictions on service providers.
- The CCPA defines "*service provider*" as a for-profit entity "*that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose, pursuant to a written contract.*"[3] Accordingly, a service provider's rights to use personal information

W371-11

[1] *See, e.g.*, Written Comments Received During 45-Day Comment Period, Comments of NAI at 24-25; Comments of California Cable and Telecommunications Association at 8-11; Comments of Consumer Data Industry Association at 13; Comments of CCIA at 7; Comments of CTIA at 14-16; Comments of Engine Advocacy at 5-6; Comments of California Chamber of Commerce at 11-12.

[2] See, e.g., Written Comments Received During 15-Day Comment Period, pdf [last updated on March 9, 2020], Comments of the Department of Justice at 5; Comments of the Entertainment Software Association at 4; Comments of the State Privacy and Security Coalition at 4; Comments of NAI at 14.

[3] Cal. Civ. Code § 1798.140(v).

W371-11 cont.

received from a business depends on what constitutes a "business purpose" under the statute. The statute defines "*business purpose*" as "the use of personal information for the business's *or a service provider's operational purposes*, or *other notified purposes.*"[4] As multiple commenters have explained, this statutory text plainly affords service providers flexibility to process personal information not only for the *business's* purposes, but also for the *service provider's* own purposes so long as those purposes are necessary to perform the services specified in the contract.[5]

- The statute provides several examples of permitted operational purposes, such as "*[p]erforming services on behalf of the business or service provider, including . . . processing orders and transactions . . . providing advertising or marketing services . . . providing analytic services, or providing similar services on behalf of the business or service provider.*"[6] Operational purposes also include, for instance, "*auditing related to a current interaction with a consumer, including but not limited to verifying the positioning and quality of advertising impressions,*"[7] and "*undertaking internal research for technological development and demonstration.*"[8]
- The plain language of the "*business purpose*" definition sensibly limits uses of personal information to those which are "*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.*"[9] The written agreement between the business and service provider, along with the privacy notices that consumers receive under the statute, specify the purposes for which personal information is collected and processed and also inform what uses are compatible with the context in which personal information is collected. Personal information disclosed to a service provider must be "*pursuant to a written contract,*" which must prohibit the service provider from processing the information "*for any purpose other than for the specific purpose of performing the services specified in the contract for the business . . . including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.*"[10]
- Permitting service providers to use personal information for their own operational purposes is not only required by a plain reading of the statutory text, but also is sound policy: in order to perform the contracted-for services on behalf of the business, service providers often *must* process personal information received from multiple businesses internally.

---

[4] Id. at § 1798.140(d) (emphasis added).

[5] *See, e.g.*, Written Comments Received During 45-Day Comment Period, Comments of Entertainment Software Association at 4; Comments of Google at 1; Comments of TechNet at 12; Written Comments Received During 15-Day Comment Period, pdf [last updated on March 9, 2020], Comments of Entertainment Software Association at 4.

[6] Cal. Civ. Code § 1798.140(d)(5).

[7] *Id.* at § 1798.140(d)(1).

[8] *Id.* at § 1798.140(d)(6).

[9] *Id.* at § 1798.140(d).

[10] *Id.* at § 1798.140(v).

- For example, a business may hire a consulting service to help it determine the best location for its next retail store. To facilitate this analysis, the business likely will need to provide the service provider with personal information (such as names and transaction history) about its existing customers, consistent with its privacy policy. The service provider likely will need to combine this information internally with similar information it has collected from other customers to analyze where these existing customers, and other potential new customers with similar interests or preferences, might shop. Without disclosing any personal information received from other customers to the business, the service provider would use this combined data to inform the recommendations it provides to the business on where to build a new store. If the consultant is not permitted to combine personal information received from its different customers and use that information to perform its services consistent with its written agreements with those different businesses, the consultant's recommendations to the retail store would be based on incomplete and less relevant information that ultimately could produce a worse outcome for consumers and lead to poor investment decisions.[11]
- Importantly, this interpretation also ensures that the privacy of consumers' personal information remains protected at all times for at least two reasons. First, consumers must have received notice that their personal information may be shared with the service provider for business purposes. Second, the CCPA requires that the written agreements between the service provider and its business customers prohibit the service provider "*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*," which safeguards the data from unauthorized processing and ensures that all uses are compatible with the context in which the personal information was collected.[12]
- Moreover, this interpretation aligns with the Attorney General's second modified draft regulations and the plain text of the enabling statute. The Attorney General's Office cannot enact rules that are inconsistent with the statutory text, including by narrowing a statute.[13] And the California legislature also specified that the Attorney General's regulations must further the CCPA's purposes.[14] Accordingly, we ask that the Attorney General further clarify that the regulations allow service

W371-11 cont.

---

[11] Relatedly, the store might decide not to engage a service provider at all for these services if it meant having to treat the disclosure as a "sale" of data, which would require the store to expend significant resources to update its privacy notice, build and maintain an opt-out mechanism, and provide additional information when responding to consumers' "right to know" requests. This alternative is particularly problematic because reasonable consumers are unlikely to consider such disclosures, where the recipient of the data is providing services to the business and is subject to contractual restrictions on how the personal information is processed, to be a sale of personal information.

[12] *See* Cal. Civ. Code §1798.140(v) (requiring service providers to receive personal information "for a business purpose" and to process personal information for "the specific purpose of performing the services specified in the contract for the business").

[13] *In re Edwards*, 26 Cal. App. 5th 1181, 1189, 237 Cal. Rptr. 3d 673, 679 (Ct. App. 2018) (quoting Gov. Code, § 11342.2). Agencies do not have the discretion to promulgate regulations that are inconsistent with the relevant statute. *See Ontario Community Foundations, Inc. v. State Bd. of Equalization* (1984) 35 Cal.3d 811, 816–817, 201 Cal.Rptr. 165, 678 P.2d 378, ("[T]here is no agency discretion to promulgate a regulation which is inconsistent with the governing statute.") (Emphasis, citations and internal quotation marks deleted.)

[14] Cal. Civ. Code §§ 1798.185(a)(1); (b)(2).

providers to process personal information received from a business for any "business purpose," as that term is defined in the statute.

- Accordingly, we recommend the following revisions for § 999.314(c):
  - The Attorney General should reinstate the deleted language in (c)(1) to clearly permit a service provider to use personal information for any permitted business purpose pursuant to the written agreement between the business and the service provider.[15]
  - To clarify that the Attorney General's regulations are meant to be consistent, and not in conflict, with the statute, we request that the Attorney General further modify the draft regulations by adding the underlined language to § 999.314 (c**)**:
  - *"A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except to the extent permitted by the CCPA, including: . . ."*

W371-11 cont.

- Finally, the inclusion of "*correcting or augmenting data*" in § 999.314(c) will create confusion and inconsistent implementation of the CCPA. "Augmenting" is not defined under California law and does not have a common meaning in industry standards and practices and thereby will likely lead to confusion and inconsistent application. In the latest draft of the regulations "cleaning" of data has now been replaced with "correcting". However, this addition is not helpful in order to create clarity around rights and obligations of service providers under the CCPA. The correction of data is a helpful activity that should be in the interest of consumers and it should be clarified that such activity is appropriate to be carried out by any party, which processes consumer data.

§ 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. Browser-level controls would not indicate whether the setting is user-activated or set by an intermediary company. This again takes away consumer control. We support 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

W371-12

[15] Section 999.314(c)(3) permits service providers to process personal information for internal purposes but includes the limitation "provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business." For the reasons discussed above, this example must be in alignment with the permissions service providers enjoy under the statute. Therefore, we understand the limitation to apply *only if* the written agreement between the business and the service provider does not permit the service provider to process personal information to build or modify profiles for other businesses.

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. W371-12 cont.

- 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.
- A browser plug-in or global device setting also risks creating a situation where a user affirmatively exercises choices on a publisher's website, but then has his or her choices unintentionally overridden by default by the default browser setting. This would be confusing to users and could potentially create consumer frustration in cases where the user does not want to opt-out from the sale of data and cannot figure out how to enable his or her actual choices. An example of this is the situation where in order to access content, consumers do not wish to use an ad blocker, but then often have trouble switching the ad blocker off if it is browser enabled.
- A global on-by-default setting is contrary to the legislature's intent to create a strong opt-out, and instead creates an opt-in law where only a few companies may be the gatekeepers to the entire internet economy.
- Additionally, § 999.315 (d)(1) removed the consumer's choice to opt-out by removing the requirement that the privacy control shall not be designed with any pre-selected settings. This is in explicit contravention of the statute's grant to consumer "*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.*" See 1798.120(a). W371-13
- We strongly recommend any provision related to user-enabled privacy controls be removed from the draft regulations. In the event this requirement is not removed, we have included a suggested revision, including reinserting the requirement that privacy control shall not be designed with any pre-selected settings, below and 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.
- If not removed completely we recommend the following revisions, "*§ 999.315 (d) ~~(c)~~ 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* W371-12 cont.

mechanism, that communicate or signal the consumer's interest in potentially opting-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~~ as a as an expression of interest in opting out and shall provide the consumer with an opportunity to opt out under Civil Code section 1798.120. For example, the business may show the consumer a pop-up window that, when clicked, redirects the consumer to the business's Notice of right to opt out, or provide the consumer with other similar methods designed to facilitate the consumer's right to opt out.

W371-12 cont.

- *(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.*

W371-13 cont.

- *(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 may ~~shall~~ provide the consumer with the opportunity to manage those settings when consumers direct themselves to the business's site. ~~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.~~ For example, the business may show consumers a pop-up window that, when clicked, redirects the consumer's to a page where consumers may manage their privacy settings, or provide the consumer with other similar methods designed to facilitate the management of the consumer's privacy settings."*

W371-12 cont.

§ 999.319. Intellectual Property and Trade Secrets

- We recommend that the Attorney General issue a new regulation protecting businesses' intellectual property rights with respect to compliance with Sections 1798.110 to 1798.135.
  - The CCPA requires the Attorney General to promulgate a regulation including "Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights…" 1798.185(a)(3). Despite the mandatory nature of this requirement, to date, the Attorney General has not issued any draft regulations related to trade secrets and intellectual property rights. We request that, to comply with its obligations under the CCPA, the AG issue a regulation establishing an exception to the requirements of the CCPA to protect against violations of intellectual property rights and the disclosure of trade secrets. In so doing, we believe the Attorney General should take into consideration the proprietary nature of certain data, particularly internally generated or derived data, and the impact that may have on a business.
  - Accordingly we suggest this new section and language,

W371-14

- *"§ 999.319 Intellectual Property and Trade Secrets. 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 the business's intellectual property rights or result in the disclosure of trade secrets."*

W371-14 cont.

§ 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.

W371-7 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. We also urge a delay in the July 1 enforcement date to January 2, 2021 given that the regulations are complex, far-reaching, and still unsettled, and that the current health crisis TechNet's member companies and their employees and customers throughout the state and world are currently facing will make compliance by the July 1 date even more difficult. 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. A delay in enforcement allows companies time to make sure they are implementing the law and regulations correctly and in the best interest of their customers.

W371-1 cont.

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

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

Message

From: Crenshaw, Jordan [redacted]
Sent: 3/27/2020 12:50:34 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: U.S. Chamber of Commerce Comments on Second Set of Modifications to CCPA Regulations
Attachments: 200327_Comments_CCPA_AGBecerra.pdf

To Whom It May Concern:

Please find the U.S. Chamber of Commerce's public comments regarding CCPA regulations.

Thank you.

Best,

Jordan Crenshaw
Executive Director & Policy Counsel
Chamber Technology Engagement Center
U.S. Chamber of Commerce
Direct: [redacted], Cell: [redacted]



U.S. Chamber of Commerce
Technology Engagement Center

JORDAN CRENSHAW
Executive Director and Policy Counsel

1615 H STREET, NW
WASHINGTON, DC 20062-2000
[redacted]

March 27, 2020

VIA ELECTRONIC FILING

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

RE: Second Set of Modifications to Text of Proposed Regulations (OAL File No. 2019-1001-05)

Dear Attorney General Becerra and Ms. Kim:

The U.S. Chamber of Commerce ("Chamber") respectfully submits these comments in response to the second set of modifications to the proposed regulations ("Proposed Regulations") to implement the California Consumer Privacy Act ("Act" or "CCPA"). The Chamber continues to pursue a national privacy standard that protects all Americans equally and is working to ensure that privacy laws give consumers and business certainty. It is for this reason that the business community applauds revisions to the proposed regulations that effectively protect consumers without added confusion.

I. POSITIVE CHANGES TO THE PROPOSED REGULATIONS IN THE INITIAL MODIFICATIONS

The first set of modifications made many significant improvements such as eliminating the two-step deletion mandate at Section 999.312(d). The modification provided needed flexibility for business working to delete personal information. W372-1

Another positive change the Chamber applauds revisions in the first set of modification Proposed Regulations at Section 999.313(d)(1). Eliminating the originally proposed requirement that a business treat an unverified request to delete as a request to opt out of sale was a first step in the right direction. W372-2

II. FINANCIAL INCENTIVE PROGRAMS

CCPA prevents covered businesses from engaging in "discriminatory" practices such denying goods or services, charging different prices, or giving a different level of quality, against W372-3

consumers that exercise their privacy rights under the Act.[1] An overly broad interpretation of the Anti-Discrimination rights in CCPA threatens the ability of retailers, airlines, restaurants, and entertainment companies to offer loyalty and reward programs that greatly benefit consumers. According to one study, the overwhelming majority of consumers agree that loyalty programs save them money.[2] The Chamber strongly urges the Attorney General to interpret CCPA in a manner that ensures that the consumers continue to enjoy loyalty and rewards programs without disruption to businesses or their customers. W372-3 cont.

Although the Act prohibits discrimination against consumer who exercise privacy rights, CCPA permits covered businesses to offer financial incentives for data collection, sales, and deletion if the difference in price or quality of goods and services "is directly related to the value provided to the business by the consumer's data."[3] The covered entity must also provide notice to consumers and receive prior opt-in consent to enroll consumers in the incentive program.[4]

The first revisions in February included several guidelines to follow for businesses that offer a financial incentive for a customer based upon the value of that customer's personal information. For example, businesses should provide a notice of financial incentive to customers in a way that is "easy to read" and uses "a format that draws the consumer's attention to the notice." The newest revisions at Section 999.301(j) define a "financial incentive" to be a benefit related to the *"collection, retention, or sale of personal information."*[5] This is a change from the February proposal which defined a financial incentive to be a benefit related to the *"disclosure, deletion, or sale"* of personal information. These changes, as well as the continued reference to a benefit "related to" the collection, retention, or sale of data (as opposed to "compensation" which is the term included in the text of the CCPA), creates uncertainty for businesses and could be broadly interpreted once enforcement begins. Such uncertainty threatens the affinity and loyalty programs consumers enjoy.

III. PERSONAL INFORMATION.

The clarification language in 999.302 as to what constitutes personal information should be restored. It provides businesses with important clarifications as to what is considered personal information. W372-4

IV. SECURITY

We urge the reinstatement of the critical exception that was included in the original version of § 999.313(c)(3) which provided that: W372-5

---

[1] CAL. CIV CODE § 1798.125(a).
[2] Emily Collins, "How Consumers Really Feel About Loyalty Programs," FORRESTER (May 8, 2017) *available at* http://www.oracle.com/us/solutions/consumers-loyalty-programs-3738548.pdf.
[3] *Id.* at §1798.125(b)(1) as modified by the legislature.
[4] *Id* at § 1798.125(b)(2)-(3).
[5] Modified Privacy Regulations Comparison at 2 (March 11, 2020) *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-second-set-mod-031120.pdf?.

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.

W372-5 cont.

This 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, cyber criminals and even foreign intelligence services may attempt to abuse the CCPA access right to obtain personal information about California residents to carry out illicit activities to commit fraud, engage in identity theft, access unauthorized accounts, or other harmful practices. By allowing businesses to protect against these threats only through verification procedures, businesses will not be able to prevent harm to consumers since bad actors may well be able to obtain the requisite number of verifying data elements through phishing or other tactics in order to falsify an authorization request.

For these reasons, we encourage the AG to restore this vital exception in order to avoid undermining the privacy of Californians' personal information in ways that can be very damaging and to prevent placing businesses in a position where they have to choose between compliance and security.

V. GLOBAL PRIVACY CONTROLS.

W372-6

The Chamber once again requests the removal of the provisions on global device settings contained in sections 999.315(a) and (d), as these present challenges for both competition and implementation. In 999.315(d)(1) the sentence was removed relating to pre-selected settings. Note that as originally written it was confusing because it was not clear that allowing sale should be the default (i.e., the "pre-selected" setting), but at a minimum, the first clause must be restored ("The privacy control shall require that the consumer affirmatively select their choice to opt-out"). Without this, there exists a risk that consumers will inadvertently be opted-out of sale without having had an opportunity to actually make that selection. Consumer control is a fundamental tenet of the California Consumer Privacy Act. A number of services feature pre-selected settings that would seem to have the effect of opting consumers out of sale automatically. By establishing that these services can constitute a valid request to opt out, the regulations would deprive consumers of the information and tools necessary to make this choice and to exercise this control independently. Nor would mere use of such a service constitute authorization for another person to opt a consumer out of sale, if the elements of notice and choice are missing.

W372-7

Products containing pre-selected settings have also been developed in a context and for a purpose that differ from the CCPA and its concept of sale. As such, they do not "clearly communicate or signal that a consumer intends to opt out of the sale of personal information," as

section 999.315(d)(1) of the proposed Regulations provides. For these reasons, the Chamber continues to oppose the requirement that a global device setting constitute a valid consumer request to opt out of the sale of personal information. If this requirement must remain, the Chamber requests the re-insertion of the sentence that has been deleted from section 999.315(d)(1). W372-7 cont.

VI. The Requirement in § 999.305(a)(5) to Obtain Opt-in Consent for Specific Data Uses Is Inconsistent with the Statute W372-8

We appreciate that the explicit consent requirement in this section has been cabined somewhat through a "materially different" standard. However, we remain concerns that 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.

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[6], participation in an entity's financial incentive program[7], and retention of a consumer's personal information for the purposes of peer-reviewed scientific, historical, or statistical research in the public interest[8]. Requiring explicit consent beyond these well-defined and clearly cabined use cases in the statute goes beyond the scope of the CCPA.

VII. Reporting Requirements W372-9

The reporting requirement in Section 999.317(g) should be deleted or at the least be greatly simplified and eliminate the requirement to have the metrics posted in the privacy policy. This reporting requirement does not exist in the CCPA and has no support in the law. In addition, the requirement is very burdensome -- a business that buys, sells, or receives/shares for a commercial purpose, the personal information of 10 million+ consumers in a year shall compile metrics on data rights requests and disclose them in its privacy policy.

VIII. The Attorney General Should Delay Enforcement to Enable Effective Compliance W372-10

As previously asserted in the Chamber's initial comments on the Proposed Regulations, any major rules should give the regulated community adequate time to institute compliance

[6] Civ. Code §1798.120(d).
[7] Civ. Code §1798.125(b)(3).
[8] Civ. Code §1798.105(d)(6).

programs. The State's Regulatory Impact Analysis ("RIA") estimates that the Regulations will cover up to 570,066 California companies, the vast majority of which are small businesses and will cost up to **$55 billion** in compliance costs for California companies alone.[9] The State's RIA assumes that the Regulation will require companies with fewer than 20 employees to incur up to $50,000 in compliance costs.[10] In order to give consumers more certainty about proper implementation of CCPA, giving companies the ability to know what the final Regulations are and have adequate compliance time will be paramount. Unfortunately, according to a July 2019 nationwide survey that poll mostly small businesses, only 11.8 percent of companies knew if CCPA applied to them.[11] Many small businesses are just becoming aware of CCPA and will need adequate time to develop solutions to protect consumers' CCPA rights. W372-10 cont.

Many small businesses must rely on technological solutions to be developed and become available many months before the new law's effective date in order to implement the CCPA's new requirements. With regulations anticipated to be finalized no more than a couple months before the statutory enforcement date, the narrow window of compliance time makes the successful adoption of these solutions industrywide unlikely. As witnessed in Europe's implementation of the General Data Protection Regulation ("GDPR), a robust market for solutions to new privacy regulations takes time to develop and can only get started once the implementing regulations are in final form. The Chamber asserts that the time Europe gave companies to comply with GDPR-two years—represented an adequate and reasonable timeframe. Unfortunately, given the current status of the Proposed Regulations, businesses now have no more than three months between final promulgation of rules and the July 1, 2020 enforcement date.

In addition to the reasons stated in previous comments and above, the COVID-19 pandemic is also causing heavy financial strain for companies—particularly small businesses. The coronavirus outbreak further compounds the problems that small business will face having to change business models within a short timeframe before July 1. For the time being, businesses should focus their resources on coronavirus efforts and operations affected by government responses to the pandemic. Although the Chamber has advocated for delaying enforcement until 2022, in light of recent circumstances, we ask the Attorney to give companies an extra six months at a minimum. W372-11

Californians deserve to have their privacy protected in ways that are both strong and responsibly implemented. A delayed enforcement date protects consumers from rushed and potentially incomplete compliance programs, and maximizes the ability of businesses to provide consumers with their privacy rights. Consumers benefit when they can trust that companies have

[9] *See* Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, State of California Department of Justice and Office of the Attorney General at 11 (August 2019) *available at* http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.
[10] *Id.*
[11] *See* ESET CCPA Survey Results (July 19-22, 2019) *available at* https://cdn1.esetstatic.com/ESET/US/download/ESET_CCPA_Survey_Results.pdf.

built well-planned compliance and accountability programs to protect their statutory privacy rights. W372-11 cont.

Sincerely,

Jordan Crenshaw

Jordan Crenshaw
Executive Director & Policy Counsel
Chamber Technology Engagement Center

Message

From: Robert Clarke [redacted]
Sent: 3/28/2020 6:43:07 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Will the CCPA Enforcement date be extended because of COVID-19?

Will the 7/1/20 endorsement date be extended because of the current Safe At Home order? W373-1

Rob Clarke
CFO
National Notary Association

Sent from my iPhone

Message

From: Lev Sugarman [redacted]
Sent: 3/27/2020 11:35:27 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Workday, Inc. Comments: Second Proposed Modifications to CCPA Regulations
Attachments: Workday Second CCPA Regs Comments.pdf

Comments attached.

Best,

Lev Sugarman | Associate Policy Analyst, Corporate Affairs | [redacted] | [redacted]

[redacted]

Thank you for considering the environment.

March 27, 2020

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

RE: Second Modifications to Proposed California Consumer Privacy Act Regulations

Dear Attorney General Becerra,

Workday appreciates the opportunity to comment on the California Attorney General's second set of modifications to the 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. Over 60% of the Fortune 50 and over 45% of the Fortune 500 have selected Workday.

We ask that § 999.314(c)(3) be revised to clarify that the restriction on correcting or augmenting data acquired from another source is specific to augmentation or correction for the purpose of building or modifying household or consumer profiles. W374-1

As drafted, the provision could be read as prohibiting a service provider from using data it obtains in providing services to correct or augment data acquired *from another source in general*. Technologies like machine learning rely on combining data from disparate sources to train and improve algorithms—an activity which, for Workday, would be "internal use by the service provider to build or improve the quality of its services." If "correcting or augmenting" is read to include the combining of data that is foundational to machine learning, the provision could be read as a restriction on service provider internal training and improvement of machine learning systems writ large—*regardless* of whether that particular activity has a nexus to building or modifying consumer or household profiles. Workday asks that § 999.314(c)(3) be modified such that it does not limit the ability of service providers to train or improve machine learning algorithms when that activity is unrelated to consumer or household profiling.

To resolve this issue, we recommend explicitly tying the restriction on correcting or augmenting data from another source to the prohibited profiling activity at the heart of the provision. In particular, **we recommend deleting the following language in ~~strikethrough~~ and adding the language in underline:**

> "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 to use in providing services to

another business, ~~or~~ including correcting or augmenting data from another source for use in such household or consumer profiles."

W374-1 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.

Message

From: Norman Sadeh [redacted]
Sent: 3/27/2020 5:25:20 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Written Comments Regarding Proposed Changes - CCPA Privacy Regulation
Attachments: Norman Sadeh - Comments to AG CCPA March 2020.pdf

Please find attached some comments regarding proposed changes to the CCPA regulations.

Thank you for your consideration.

Norman Sadeh
--

Prof. Norman M. Sadeh – www.normsadeh.org

ISR - School of Computer Science

Carnegie Mellon University

5000 Forbes Avenue -- Pittsburgh, PA 15213

Lab Manager: Ms. Linda Moreci – [redacted] - Tel: [redacted]

Carnegie Mellon

Comments from:
Prof. Norman M. Sadeh
School of Computer Science
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA – 15213-3891
Tel: [redacted]
Email: [redacted]
www.normsadeh.org

March 27, 2020

Submitted 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

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)
Notice of 2nd Set of Modifications

About the Author:

Norman Sadeh is a Professor of Computer Science at Carnegie Mellon Univeraity (CMU). He co-founded and co-directed School of Computer Science's PhD program in Societal Computing at CMU for about ten years (http://sc.cs.cmu.edu/). He is also co-founder and co-director of CMU's Master's Program in Privacy Engineering (http://privacy.cs.cmu.edu/). He has been on the faculty at CMU since 1991, and also received his PhD in Computer Science from CMU. In addition to his affiliation with the School of Computer Science at CMU, Prof. Sadeh is also a core faculty member of CMU's CyLab Security and Privacy Institute and holds a courtesy appointment in CMU's Heinz College of Management and Public Policy.

Dr. Sadeh is an IAPP Certified Information Privacy Technologist (CIPT) and has authored over 300 publications. He serves as Principal Investigator on two of the largest national research projects in privacy: The Usable Privacy Policy Project (https://usableprivacy.org) and the Personalized Privacy Project (https://privacyassistant.org) . You can find out more about him at https://www.normsadeh.org/short-narrative/

Carnegie Mellon University
Master of Science in Information Technology
privacy ENGINEERING

W375-1

This brief comment is to urge modification of the proposed rulemaking around the Consumer Privacy Protection Act (CCPA) and the adoption of a requirement that opt-out/do-not-sell buttons be accompanied with a standardized API that allows 3rd party software such as a browser or some other 3rd party software agent to submit an opt-out/do-not-sell request on behalf of a data subject. Such functionality is critical, as our research has shown over and over again that requesting data subjects to manually submit such requests to potentially every website and/or every technology with which they interact is simply unrealistic: the number of actions that would be required from a user is simply too great. In addition, these types of buttons, whether intentionally or not, are often difficult for users to find and actually use.

Instead, an API would make it possible for users to configure privacy settings once (or a limited number of times), whether in their browser or in some other 3rd party software. The browser or other 3rd party software would then submit opt-out/do-not-sell requests on behalf of the user based on the settings specified by the user in his/her browser/third party software. Such settings could be based on attributes such as type of website, category of app, type of data being collected, etc. For instance browser settings could be configured to allow users to specify specific categories of websites they want to prevent from selling their data, or specific types of data about them they do not want to be sold. Similarly, privacy assistant software running on a user's smartphone could be configured to submit such requests to different categories of apps or possibly for specific types of data collected by different categories of apps. The user's browser or his/her privacy assistant app would then submit opt-out/do-not-sell requests on behalf of the data subject to the websites/apps specified by the settings selected by the data subject. With such functionality, the number of actions required by a data subject would be drastically lower, making it practical for people to actually take advantage of the opt-out/do-not-sell options made available to them by CCPA.

Relevant Publications Supporting this Proposed Modification:

- Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, Florian Schaub, **"“It's a scavenger hunt”: Usability of Websites' Opt-Out and Data Deletion Choices"**, CHI '20, Apr 2020 [pdf]
- Vinayshekhar Bannihatti Kumar, Roger Iyengar, Namita Nisal, Yuanyuan Feng, Hana Habib, Peter Story, Sushain Cherivirala, Margaret Hagan, Lorrie Faith Cranor, Shomir Wilson, Florian Schaub, Norman Sadeh, **"Finding a Choice in a Haystack: Automatic Extraction of Opt-Out Statements from Privacy Policy Text"**, WWW '20, Apr 2020 [pdf]
- B. Liu, M.S. Andersen, F. Schaub, H. Almuhimedi, S. Zhang, N. Sadeh, A. Acquisti, and Y. Agarwal. "Follow My Recommendations: A Personalized Assistant for Mobile App Permissions", Symposium on Usable Privacy and Security (SOUPS'16), June 2016, [pdf]
- A. Das, M. Degeling, D.Smullen, and N. Sadeh, "Personalized Privacy Assistants for the Internet of Things," 2018 IEEE Pervasive Computing: Special Issue – Securing IoT, Apr. 2018, [pdf]

Carnegie Mellon University
Master of Science in Information Technology
privacy ENGINEERING

Message

From: James Harrison [redacted]
Sent: 3/30/2020 12:10:18 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: RE: Californians for Consumer Privacy Comments Re Revised Proposed Regulations
Attachments: 00406260.pdf

Attached please find a reformatted pdf of the letter we submitted on Friday. The content has not changed. Thank you.

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

From: James Harrison
Sent: Friday, March 27, 2020 4:59 PM
To: PrivacyRegulations@doj.ca.gov
Subject: Californians for Consumer Privacy Comments Re Revised Proposed Regulations

Attached please find 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

March 27, 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:

Thank you for the opportunity to offer comments regarding the Attorney General's revised proposed regulations (modified on March 11, 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.

Rather than reiterating all of our previous comments with respect to regulations that have not been altered, we focus below on our most pressing concerns. Please note, however, that the comments in our February 25, 2020, letter regarding the following sections remain relevant with respect to the current version of the proposed regulations:

- Section 999.301(u)
- Section 999.305(d)
- Section 999.306(a)(2)
- Section 999.306(b)(1)
- Section 999.306(c)
- Section 999.306(f): we note that the section covering the Opt-Out Button or Logo has been deleted, and we would encourage the Attorney General to include a regulation requiring a clear, conspicuous DNS button and process, so that consumers have consistency and businesses have clear direction
- Section 999.307
- Section 999.308
- Section 999.313(b)
- Section 999.313(d)(2)(b)
- Section 999.319(d)(2)(c)
- Section 999.313(d)(8), which referenced the previous Section 999.313(d)(7)
- Section 999.315(a)
- Section 999.315(e)
- Section 999.315(h)
- Section 999.316(b)
- Section 999.325(f)
- Section 999.326(a)(3)
- Section 999.336(d)(3)

W376-1

Below, please find our comments and suggestions regarding improvements to key proposed regulations:

Notice at Collection: Online (999.305(c))

W376-2

We remain concerned that that Section 999.305(c) introduces uncertainty regarding a business's obligation to include a "Do Not Sell My Personal Information" link on its homepage, including any page where it collects consumers' personal information, as required by Civil Code sections 1798.135(a) and 1798.140(l). By authorizing a business to include the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link in the business's privacy policy, as specified in Section 999.305(c), which incorporates Section 999.305(b)(3), the proposed regulations appear to suggest that a business could satisfy its obligation to post the "Do Not Sell My Personal Information" link on any webpage on which it collects information merely by including that link in its privacy policy. We recognize that the statutory mandates in Sections 1798.135 and 1798.140 govern the obligations of the businesses with respect to the "Do Not Sell My Personal Information" link, but we are concerned that without a clarification, businesses may understand that the Attorney General, who is charged with enforcing the law, has construed it to require something less, namely including the link in its privacy policy.

Responding to Requests to Know (999.313)

W376-3

Section 999.313(c)(4): In our December and February comments, we urged 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 those businesses had collected about the consumer. Indeed, there is nothing in the California Consumer Privacy Act that states that a business would NOT have to turn over that information to a consumer.

This regulation would remove a vast category of information from any consumer's reach—**and with the addition of biometric data**, this regulation would vastly increase the scope of this exception. Although the revision to Section 999.313(c)(4) allowing for consumers to learn what pieces of information the business has collected about them is an improvement, it does not change the fact that the Attorney General does not have the statutory right to deny consumers the right to know deeply personal information that businesses have collected about them.

Civil Code Section 1798.185(a)(7) reads as follows:

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

Nowhere does the statute authorize the Attorney General to limit the amount of information consumers are entitled to receive in response to a request. Indeed, the spirit of the provision is to facilitate a consumer's access to all information with appropriate security precautions.

W376-3 cont.

We urge you to modify the proposed regulation to allow businesses to require more stringent steps to verify consumer identity when consumers request highly sensitive information. The notion that a consumer could show up in person, with identification, at a business; and that that business could then refuse to hand over the information they had collected about that consumer, is contrary to the spirit of the law. This is akin to allowing doctors not to permit their patients access to their own medical file, and Californians will be outraged if this becomes the law of the land.

If this language is kept in the regulations, it will be a massive hole in the heart of CCPA, and we think the Attorney General would be overstepping his legal authority.

Service Providers (999.314)

W376-4

Section 999.314(a): Although you have improved this regulation in some respects, it remains fundamentally problematic, and in our opinion, would represent a *massive* weakening of CCPA's reach.

We appreciate your decision to use 'business' rather than 'person,' which provides greater clarity.

However, the inclusion of government entities within the scope of this regulation is highly troubling. While the CCPA was not intended to directly regulate government entities, 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, notwithstanding the right of access to government records under the Public Records Act and the Freedom of Information Act. Indeed, companies like Palantir are not subject to FOIA or the PRA, but they are subject to the CCPA and they should be required to inform consumers about information they have collected about them on behalf of the government.

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), Section 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.

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. W376-4 cont.

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.

> *[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.

W376-4 cont.

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.

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 999.315(f)

W376-5

As stated in our February letter, we continue to object strenuously to the notion that businesses need three full weeks to opt a consumer out of the sale of their information, following a consumer's request to do so. Businesses can capture a consumer's information and sell it in microseconds—but now they need three weeks to reverse the process?

This regulation would be a massive win for businesses, in that fresh consumer information is the most valuable consumer information. We urge you to shorten this time frame. W376-5 cont.

Thank you for your consideration of our comments. We look forward to working towards the completion and issuance of the proposed regulations and enforcement of the CCPA by the Department of Justice beginning on July 1, 2020.

Yours sincerely,

/s/ Alastair Mactaggart, Chair

Californians for Consumer Privacy