Message

From: Jessica Simmons [redacted]
Sent: 3/27/2019 12:03:12 PM
To: Privacy Regulations [redacted]
CC: Jessica Simmons [redacted]
Subject: Auto Alliance regulatory text recommendations for CCPA AG Rulemaking
Attachments: CCPA AG Rulemaking proposed rule text - Auto Alliance.pdf

To whom it may concern,

The Auto Alliance was pleased to submit comments to the AG rulemaking a couple of weeks ago. We have worked to fashion some language to put our clarifying recommendations into regulatory text. Please find a document with explanatory cover letter and accompanying draft regulatory text. Should you have any trouble accessing the attachment, please let me know.

Best,

Jessica Simmons

Jessica L. Simmons

Assistant General Counsel

[redacted]

AUTO ALLIANCE
DRIVING INNOVATION

ALLIANCE OF AUTOMOBILE MANUFACTURERS

803 7th Street, NW
Suite 300
Washington, DC 20001

Main Phone: [redacted]
Main Fax: [redacted]

AUTO ALLIANCE
DRIVING INNOVATION®

803 7th Street N.W., Suite 300 | Washington, DC 20001
[redacted]

March 27, 2019

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

RE: Proposed Regulations of the Alliance of Automobile Manufacturers for the California Attorney General's Rulemaking Pursuant to the California Consumer Privacy Act

To Whom It May Concern:

The California Consumer Privacy Act ("CCPA") directs the California Attorney General to promulgate regulations on various specified topics and as necessary to further the purposes of the CCPA. As part of its preliminary activities in the rulemaking process, the Attorney General's Office invited public comments. The Alliance of Automobile Manufacturers ("Alliance") prepared and submitted comments ("Comments") on March 8, 2018. The Alliance is the leading advocacy group for the auto industry, representing 12 member companies that account for approximately 70 percent of all car and light truck sales in the United States.[1]

As follow up to the Alliance's submission, the Alliance believes it may be helpful to provide the California Attorney General's Office actual proposed regulation language associated with the comments we previously submitted. We re-attach our previously submitted Comments for your convenience. The proposed regulations align with those earlier Comments as follows:

- Proposed Rule 1 addresses the concerns raised in Comment 1 and Comment 8 (pages 4-6 and 14-15 of our Comments).
- Proposed Rule 2 addresses the concerns raised in Comment 2 (pages 6-7 of our Comments).
- Proposed Rule 3 addresses the concerns raised in Comment 3 (pages 7-8 of our Comments).
- Proposed Rule 4 addresses the concerns raised in Comment 4 (page 8 of our Comments).
- Proposed Rule 5 addresses the concerns raised in Comment 5 (pages 9-10 of our Comments).

[1] The members of the Alliance include (alphabetically) the BMW Group, Fiat Chrysler Automobiles, Ford Motor Company, General Motors Company, Jaguar Land Rover, Mazda, Mercedes-Benz USA, Mitsubishi Motors, Porsche, Toyota, Volkswagen Group of America, and Volvo Car USA.

AUTO ALLIANCE
DRIVING INNOVATION®

803 7th Street N.W., Suite 300 | Washington, DC 20001
[redacted]

- Proposed Rule 6 addresses the concerns raised in Comment 6 (pages 10-12 of our Comments).
- Proposed Rule 7 addresses the concerns raised in Comment 7 (pages 12-14 of our Comments).
- Proposed Rule 8 addresses the concerns raised in Comment 9 (pages 15-16 of our Comments).
- Proposed Rule 9 addresses the concerns raised in Comment 10 (page 17 of our Comments).
- Proposed Rule 10 addresses the concerns raised in Comment 11 (pages 17-18 of our Comments).
- Proposed Rule 11 addresses the concerns raised in Comment 12 (page 18 of our Comments).

The Alliance recognizes that the CCPA applies across industries and therefore drafted the proposed regulations to apply broadly, not just to the automotive-specific issues raised in our earlier Comments. For example, Proposed Rule 7 clarifies that a consumer's opt-out from sales shall not prevent a business from disclosing personal information where such disclosure is "for purposes related to environmental protection, such as participation in government environmental protection programs." This language is intended to address automakers' disclosures of information when participating in state of California environmental initiatives such as the Clean Fuel Rewards Program; however, the proposed rule was drafted more broadly to cover potential similar programs in other industries. The Alliance appreciates the Attorney General's consideration of these proposed regulations. Please feel free to contact us if you have any questions or would like to discuss any aspect of these proposed regulations.

Best Regards,

Jessica Simmons

Jessica Simmons
Assistant General Counsel

CCPA Attorney General Rulemaking – Proposed Rule Language

Rule 1: Mitigating risks in association with responses to access requests.

CCR §

(a) Nothing in [the Act] shall require a business to provide all specific pieces of personal information a business has collected about a consumer in response to [an access request], where the provision of such personal information:

(1) poses a reasonable risk of having a substantial, adverse impact on the rights and freedoms of other consumers;
(2) may compromise trade secrets and intellectual property rights of the business; or
(3) likely would
    i. provide little meaningful information to the average, reasonable consumer; and
    ii. be unduly burdensome for the business to provide.

(b) In determining whether the provision of personal information in response to an access request may adversely affect the rights and freedoms of other individuals, the Attorney General will take into consideration:

(1) whether the personal information may relate to multiple individuals, including but not limited to where personal information is related to devices operated by multiple users; and
(2) the potential for consumers to suffer harm if personal information relating to them is obtained by other individuals, including for example, where the personal information could reasonably facilitate identity theft or could be misused by someone engaging in stalking behaviors.

(c) In determining whether the provision of personal information in response to an access request would be unduly burdensome to a business, the Attorney General will take into consideration the:

(3) volume and nature of the information;
(4) available technologies; and
(5) cost of providing the information in the format required under [the Act].

(d) In determining whether the provision of personal information in response to an access request would provide little meaningful information to the average, reasonable consumer, the Attorney General will take into consideration the:

(6) level of technical or other knowledge required to understand the information; and
(7) the volume and nature of the information.

(e) If, pursuant to subsection (a), above, a business reasonably believes that it is not required to provide all specific pieces of personal information a business has collected about a consumer in response to [an access request], the business may provide the consumer with:

(1) a subset of the specific pieces of personal information collected;
(2) a compilation of the personal information collected that has been reasonably summarized, as appropriate;
(3) a description of the categories of personal information collected; or

(4) an explanation of why the business cannot respond to the access request.

Rule 2: Clarifying that the sharing of personal information with emergency providers is permitted notwithstanding a consumer's request to opt out of a "sale" of personal information.

CCR §

(a) The right to opt out shall not be construed to prohibit a business from sharing a consumer's personal information with third parties that provide emergency assistance services.

(b) For the purposes of subsection (a), emergency assistance services include, but are not limited to, emergency medical services, roadside assistance providers, and similar entities.

Rule 3: Clarifying that where a device or subscription service may be used by multiple users, only the device owner or registered user of the subscription service has the right to request access to, deletion of, or suspension of the sale of personal information related to the device or subscription service.

CCR §

(a) Where a business holds personal information related to a device or subscription service, only the owner of the device or registered user of the subscription service may exercise rights to request access to personal information associated with the device or subscription service, request deletion of such personal information, or request that the business no longer sell personal information associated with the device or subscription service.

Rule 4: Establishing robust verification standards for access, deletion, and opt-out requests.

CCR §

(a) Before complying with a consumer's access, deletion, or opt-out request, each business may apply verification procedures designed to verify the identity of the person from whom the business received such request. Any such procedures shall be reasonable and appropriate to the nature of the request and the nature of the personal information involved.

(b) Where a business has reasonable grounds to believe that compliance with a consumer request made by someone other than the consumer, or a party authorized by the consumer, to whom the personal information relates may adversely affect the rights and freedoms of other individuals, the business may insist that the requestor provide information that helps the business establish the requestor's identity to a high degree of certainty before complying with a consumer's access, deletion, or opt-out request.

(c) A business that takes reasonable steps appropriate to the nature of the personal information impacted by a consumer's access, deletion, or opt-out request to verify the identity of the person from whom the business receives the request and to verify that the person is authorized to make such a request shall not be liable under [the Act] for complying with the request.

Rule 5: Clarifying the meaning of "solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business."

CCR §

(a) For purposes of [the Act], the use of personal information for internal analysis related to safety, quality, performance, efficiency, or security, where this use is disclosed to consumers in its website privacy policy pursuant to Cal. Civ. Code § 1798.130(a)(5) and at or before the point of collection pursuant to Cal. Civ. Code § 1798.100(b), shall constitute "solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business" such that the personal information would not be subject to a consumer's deletion request.

Rule 6: Clarifying that data will be considered "deidentified" when it cannot reasonably be used to identify a consumer.

CCR §

(a) For purposes of [the Act], information held by a business shall be considered deidentified where given the nature of the information and the safeguards that the business has implemented to prevent reidentication, the business cannot reasonably identify a particular consumer. The safeguards implemented by the business shall include reasonable and appropriate procedures, including contractual safeguards, to prevent reidentification of the information by the business, its service providers, and third parties.

(b) Information that has been pseudonymized shall be considered deidentified provided the business has developed and implemented reasonable and appropriate procedures to prevent the reidentification of such information by the business or its service providers.

Rule 7: Clarifying the scope of the right to opt-out of sales.

CCR §

(a) Nothing in [the Act] shall prevent a business from disclosing personal information to another business or third party, including after the receipt of a request to opt-out from sales, where such disclosure is:

(1) made to a dealer or franchisee that shares common branding with the business disclosing the information;
(2) for purposes related to public safety, such as product analysis for safety and security, or sharing with emergency assistance providers, including roadside assistance providers; or
(3) for purposes related to environmental protection, such as participation in government environmental protection programs; or
(4) required by state or federal law.

Rule 8: Clarifying that businesses may enforce reasonable terms of financial incentive programs following a consumer's opt out from the program.

CCR §

(a) For purposes of Section 1798.125(a), a consumer's right to revoke opt-in consent to a financial incentive program shall not be construed as the exercise of one of the consumer's rights under [the Act].

(b) A business may enforce the terms of a financial incentive program against a consumer who revokes opt-in consent to such program as long as such terms are not unjust, unreasonable, coercive, or usurious in nature.

Rule 9: Clarifying the interpretation of "collecting" personal information.

CCR §

(a) For purposes of [the Act], personal information that is stored on devices not owned by a business does not constitute personal information that a business has "collected" until the business retrieves such information from the device.

Rule 10: Permitting businesses to deidentify personal information in response to deletion requests.

CCR §

(a) A business shall be deemed to have completed a consumer's request for deletion if the business deidentifies the personal information in accordance with [any sections defining deidentification].

Rule 11: Clarifying the interpretation of "personal information" as it relates to employee information.

CCR §

(a) For purposes of [the Act], information shall not be considered "personal information" if:

(1) it relates to a business's own personnel, including employees and contractors; and
(2) is collected and used within the employment context.

Message

From: M. Forer [redacted]
Sent: 4/22/2019 11:11:51 PM
To: Privacy Regulations [redacted]
Subject: California Consumer Privacy Act (CCPA) Comments

To Whom It May Concern:
If I had known about the the public forum in Los Angeles, I would have attended and made sure to have sat on the front row smack right in the middle in the row due to the importance of the CCPA and its enforcement thereof.

Regarding the preceding paragraph, someone at the AG's Office (especially the office in Los Angeles!) should have notified the technology editors in the major newspapers located in San Francisco, Fresno, Los Angeles, Riverside/Inland Empire, Sacramento, San Diego and Stanford, about the public forums, and their dates about the CCPA. This would have informed them to assign one of their technology writers to cover it, which would have provided "notice" to a larger populated number of citizens in California, since after all, the purpose was a "*public forum*." It is shameful. The AG's office failed to market the public forums correctly.
...

This email concerns the necessity for the AG's Office to make sure that the CCPA complies and elevates the legislative importance of the mandatory opt-out requests by **Safe at Home** program participants of their online personally identifiable information (PII) by data brokers, data aggregators and data mining companies.

The information that has been on on the AG's privacy page for Safe at Home program participants, e.g., "Directory Web Site List with Opt-Out Information," etc., is outrageously out of date, antiquated and teetering on the line of uselessness.

Furthermore, the AG's office, specifically the Consumer Law Section - Privacy Unit in San Francisco, with Supervising Deputy Attorney General Ms. Stacey D. Schesser at the helm, must immediately set up a separate unit for **enforcement** of **Government Code sections 6205-621**7, on behalf of all Safe at Home participants.

The AG's Privacy Unit, along with the executive office of the CA Secretary of State (Ms. Lizette Mata, Assistant Chief Deputy Secretary of State) and the Safe at Home program manager, Ms. Meg Webber (as of 4/1/2018), must jointly, uniformly and consistently take the ethical, legal and moral responsibility to protect Safe at Home participants.

Meg Webber, Manager

California Secretary of State

Safe at Home Program

[redacted]

[redacted]

The CCPA must include PII opt-out request enforcement protections for all Safe at Home participants. If you have any questions, please direct them to the undersigned. Thank you for your focused attention, time and thoughtfulness in seriously addressing the very important security, privacy and safety issues for Safe at Home program participants included herein.

Respectfully,

[redacted]

...

As part of the rulemaking process, Attorney General Becerra invites all interested persons to provide comments on the CCPA rulemaking at any of the following forums, or by submitting written comments to privacyregulations@doj.ca.gov or by mail at California Department of Justice, ATTN: Privacy Regulations Coordinator, 300 S. Spring St., Los Angeles, CA 90013. Please note that any information provided is subject to the Public Records Act. Times and locations subject to change. Please view oag.ca.gov/privacy/ccpa for most updated information.

Message

From: Jen King [redacted]
Sent: 3/29/2019 11:43:44 AM
To: Privacy Regulations [redacted]
CC: Jana Gooth [redacted]
Subject: CCPA comments
Attachments: king_gooth_CCPA_comments.pdf

Greetings - please accept these extremely late comments on the CCPA, attached.

Sincerely,

Jen King

Jennifer King, Ph.D
Director of Consumer Privacy
Center for Internet and Society
Stanford Law School
[redacted]

Google Scholar profile: [redacted]

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

Re: Comments on Assembly Bill 375, the California Consumer Privacy Act of 2018

March 29, 2019

To Whom It May Concern:

We are pleased to submit comments to the California Attorney General's office regarding AB 375, the California Consumer Privacy Act (CCPA). We submit these comments on behalf of ourselves individually and provide our institutional affiliation for identification purposes only.

The CCPA, as passed, includes provisions that we are concerned will ultimately be ineffective in protecting consumer privacy. We describe our concerns in detail below.

1. <u>This law includes design-based directives that are not supported by existing research.</u>

California is not unique in its efforts to pass laws that include digital design imperatives that are not vetted by design experts, and thus in their implementation may be ineffective, or at worst, contravene the intent of the law. In the absence of a requirement for evidenced based policy-making, California legislators may pass legislation that includes design-based directives that are created *ad hoc* without supporting expert research. In the domain of computer interface design, these ad hoc choices may have unintended effects. For example, research conducted by Dr. Jennifer King and colleagues[1] has demonstrated that CalOPPA's 2003 requirement that all websites conducting business with California residents include a link on the website's homepage with the specific wording "Privacy Policy" has contributed to consumer confusion over the meaning of the phrase itself, with consumers reporting a mistaken belief that the phrase "Privacy Policy" implies an actual level of privacy protection that in fact does not exist.

In Section 1798.135(a)(1), the CCPA specifies that businesses "provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information." How will businesses interpret this 'clear and conspicuous' link requirement? Existing implementations of CalOPPA suggest an answer. CalOPPA gives specific requirements regarding the appearance, content, and placement for links to a company's privacy

[1] See: Hoofnagle, Chris Jay; King, Jennife;, Li, Su; and Turow, Joseph. How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? (April 14, 2010). Available at SSRN: https://ssrn.com/abstract=1589864; Turow, Joseph; King, Jennifer; Hoofnagle, Chris Jay; Bleakley, Amy; and Hennessy, Michae., Americans Reject Tailored Advertising and Three Activities that Enable It (September 29, 2009). Available at SSRN: https://ssrn.com/abstract=1478214

policy. The net result has been that the vast majority of websites place the link in the footer (at the bottom) of their homepages and across their Web sites—arguably not a conspicuous placement, and one that signals the link's relative unimportance in relation to other elements on a Web page. Doubtless we will see the 'Do Not Sell' link relegated to the same placement, where it will join "Privacy Policy," "Your California Privacy Rights," and other mandated links. Given that the current definition of "homepage" in 1798.140(l) includes "any Internet Web page where personal information is collected," businesses will likely need to place a link on every page of a website (and potentially mobile app) due to the fact that both websites and mobile apps often include pervasive advertising trackers that collect personal information from consumers across most or all of a website's or app's pages, irrespective of whether the website or app itself is actively collecting user information.

It is important to note that placing these links at the bottom of a Web page is neither inherently clear nor conspicuous, and is *not based on any research suggesting what the optimal placement would be for consumers to both notice and comprehend these links.* Furthermore, CCPA assumes that the best presentation for this form of notice is a link, as opposed to any other form of interaction, constraining the form of notice and potentially making it future-incompatible, particularly as voice-based interfaces become more common. CCPA, like CalOPPA, contains inherent assumptions about how to communicate notice to consumers about privacy without any reference to the decade-plus research efforts in this area to determine how best to do so. As such, it may contain the seeds of its own ineffectiveness by reifying a paradigm of notice that research has demonstrated repeatedly that consumers ignore or misinterpret.

2. <u>Educating consumers about their new deletion rights will require considerable effort, which appears both unaddressed and unfunded in CCPA.</u>

In order for this law to be effective, the public must know that it exists and how to act on it, specifically what rights they have, and how to exercise them. California must provide public outreach and educational materials informing consumers of the CCPA. However, the existing legislation is silent on the matter of consumer education, and appears to not contain any mechanisms for funding such education. We must not assume that consumers will naturally understand what these new rights are or how to use them. Furthermore, should our predictions in Section 1 be accurate and the 'Do Not Sell' link is relegated to website footers, *most consumers will not know this right exists.* Public knowledge of the 'Do Not Sell' or 'Deletion' rights will become dependent upon media coverage and outreach by civil society organizations, filling in the gaps left by a lack of public outreach by the State of California.

The inclusion of Section 1798.185(a)(3)(C) ("*For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.*") attempts to address the issue of public knowledge by calling for the development (by whom?) of a consistent logo or button to increase consumer awareness of the 'Do Not Sell' right. But absent an accompanying public relations or education campaign, the mere existence of this button or logo does not guarantee that the public will be well-informed of this new right. Further, this button or logo will compete against an already crowded field

of privacy and security seals, as well as other visual elements competing for one's attention. Assuming a button or logo is an effective means of informing the public of this new right, what would be the most effective way of displaying it in relation to the link requirement? If most companies do display the 'Do Not Sell' link at the footer of their page, should this button/logo be placed near it? Or somewhere else? How should it display on mobile Web pages? Or within mobile apps? Or, what would be the most effective way of communicating this information to consumers, period? Unfortunately, while experts such as ourselves can make research-based suggestions to attempt to optimize this requirement, ideally we would have the ability to review these proposals before the law's passage, or even better, be provided with the time and resources to design and test possible solutions to make formal recommendations to the State.

3. CCPA, as written, focuses on first party relationships, but is silent on how consumers will identify the companies that acquire and sell/share their data.

While consumers may understand who the first party businesses are who collect their data, what is particularly unclear to the majority of the public is who else is collecting information about them. This is a category of actors that include advertising technology (Adtech) businesses, data brokers, and others who collect, buy, sell, and trade in consumer data, typically without consumers' tacit knowledge or express consent. Consumers generally do not have direct relationships with these businesses. As written, CCPA makes assumptions around notice that presupposes consumers will know exactly which companies they wish to target to exercise their 'Do Not Sell' and 'Deletion' rights. How will consumers determine which companies hold their identifiable or household data outside of the first party business relationships they have initiated directly?

One solution could be for first party businesses to publicly identify the companies (and include contact information) to whom they sell or share data (and thus potentially obviate Section 1798.83., a.k.a. The Shine the Light law[2]), as well as the companies for whom they facilitate direct data collection from consumers (*e.g.*, Adtech companies). The original text of the ballot initiative included a similar provision, and it is regrettable that the current legislation does not. Another solution could be found in the European Union's General Data Protection Regulation (GDPR): businesses have to actively inform a consumer within a reasonable time period that they are processing their data and from which source the data originates.[3]

This requirement should extend to any business that collects data facilitated by a first party relationship. Compliance with this requirement would ensure that the websites and mobile apps that utilize advertising technology services must identify all of the parties collecting their customers' data.

---

[2] See: Hoofnagle, Chris Jay and King, Jennifer. Consumer Information Sharing: Where the Sun Still Don't Shine (December 17, 2007). Available at SSRN: https://ssrn.com/abstract=1137990.

[3] See GDPR art. 14(1), (2)(f) and recital 61, http://data.europa.eu/eli/reg/2016/679/oj

4. CCPA, as written, does not appear to provide consumers with meaningful deletion rights with respect to Adtech-type businesses.

The deletion right provided by the CCPA makes the most sense when considering consumers' direct relationships with information-collecting businesses (*e.g.*, Facebook, Google, etc.). In these cases, a consumer can make an affirmative decision to end a relationship with a specific company or website and thus request the deletion of her data. Looking forward, the company or website presumably would not continue to collect data about the individual, unless the individual consumer re-initiated a relationship.

However, when considering businesses such as Adtech companies that collect consumer information through another company's website or app, this deletion right appears misleading. Given that consumers today typically do not affirmatively consent to, or are even aware of, these 'secondary' relationships, what will be the practical effect of initiating a deletion request with one of these businesses? Our concern is that these companies can restart the collection process as soon as a consumer visits a website or uses an app that deploys their services. Assuming an individual could even keep track of the myriad of secondary companies that silently collect her personal information, if an individual consumer wishes to prevent further collection of her information by these secondary businesses, she would have to know which websites and apps engage with the primary companies she engages with. Furthermore, for the deletion requests to be meaningful, she would potentially have to track herself to whom and how often she had made deletion requests and then judge how often she would need to repeat the requests. A scenario such as this calls into question the efficacy and meaningfulness of the deletion right itself.

It would seem most sensible to switch our engagement with information collection in California to opt-in, rather than opt-out, much like the GDPR has. However, we are aware of the potential legal challenges to an opt-in regime in the U.S., and the CCPA may not be the best avenue by which to make this challenge. At the same time, it is exactly this form of data collection and tracking that consumers dislike the most, and it does not appear that the CCPA, as currently conceived, will have a meaningful effect on this problem.

5. The 'Deletion' and 'Do Not Sell' rights that the CCPA creates run the risk of not being effectively enforced.

While consumers are given the right to civil action in security-related cases, they do not have such a right when businesses do not comply with their consumer right requests. The only sanction those businesses face is a civil penalty of a maximum of $7,500 per violation, asserted by the Attorney General. Given that there is no formal mechanism for consumers to lodge a complaint with the Attorney General, it is unlikely that even in the event a business categorically ignores consumer right requests and therefore commits multiple violations, such a civil penalty would significantly multiply. Under the current sanction regime of the CCPA it is—at least for bigger companies—cheaper to simply not comply with most provisions of the law and pay an occasional penalty than it would be to

comply with them. This not only renders the law itself ineffective and poses a risk to the rule of law, but also disadvantages smaller businesses. These upfront calculations of intermittently paying a small penalty rather than actually abiding the privacy law is what had been happening in the EU for decades, and which led to the sensible and dynamic fines under GDPR.

We would therefore recommend amending the CCPA to (1) re-introduce the right to civil action for consumers who have suffered any kind of violation of the CCPA; (2) increase the maximum civil penalty to an amount that will reasonably deter violations; (3) re-introduce the right to lodge a complaint with the Attorney General; (4) and, re-introduce enforcement by additional public entities.

6. Further harmonization of CCPA with the GDPR.

After having spent immense efforts into complying with the GDPR over the last years, many California businesses have a significant interest in capitalizing on the synergies between the CCPA and the GDPR. Though the CCPA does entail concepts inspired by the GDPR, it often comes short of the GDPR's full force of effect This becomes particularly apparent in regard to the right to deletion. In order to improve the CCPA, in addition to addressing the specific concerns we list above, we therefore also suggest the following, non-conclusive alignments:

A. Extend the right of deletion to personal information irrespective of its origin.

Other than the GDPR, the CCPA only allows for consumers to request the deletion of their personal information from businesses that themselves collected the information. Once a consumer's information is sold to or shared with a third party, the consumer has no means of having it deleted. With the objective of the CCPA being to give consumers more control over the use of their personal information, the current wording remains largely ineffective to achieve this goal.

B. Introduce joint liability.

While a business has to direct its service providers to delete personal information after receiving a deletion request, it is not liable for the non-compliance of its service provider with this direction. Therefore, there is no incentive for a service provider to actually follow this direction. Following the GDPR's example, we would suggest the incorporation of a joint liability of the business and its service providers for the deletion in order to ensure the effectiveness of the provision.

C. Narrow the exceptions for compliance with deletion requests.

Currently, there are three exceptions to the obligation to delete personal information that seem to bear the risk of being excessively invoked by businesses and therefore hinder the provision to grant consumers an effective right of deletion, namely Section 1798.105(d)(1), (7) and (9). Again drawing from the GDPR, we would suggest to instead introduce the concept of 'legitimate interest' as an exception for when a business may deny a deletion. This way, businesses would have to consider the implications of a continuous processing of personal information on the right to privacy of the

consumer. Only where the individuals' interests and fundamental rights and freedoms are outweighed by the businesses' legitimate interests, they would be exempted from fulfilling deletion-requests.

7. California can be a leader in shifting the paradigm of notice and consent.

While there is much debate about how best to legislate privacy, there is nearly universal agreement that how we inform the public about the use of their data is ineffectual at best and misleading at worst. We know that privacy policies are generally unread by the public; they are too long and written for lawyers, by lawyers; their language is often ambiguous and elides over specific uses of consumer data. In sum, they are unhelpful for providing consumers with clear, actionable data for making informed decisions. It is no wonder that researchers have documented a sense of resignation among the public regarding the use of their personal data.[4]

While California led the U.S. by passing CalOPPA in 2003 and requiring that websites post privacy policies for California consumers (and, by default, most of the globe), at the same time it gave companies a minimum standard with which to comply that has proven to be ineffective at providing the public with clear, actionable knowledge by which to make informed decisions. As written, CCPA does nothing to address or improve this state of affairs, and in fact enshrines existing flawed notice and consent principles into new law.

There are two approaches we suggest here: the first makes specific suggestions with regards to notice and consent to aid CCPA as written. The second makes big-picture recommendations as to how California can lead in shifting the paradigm around privacy disclosures.

A. CCPA-Specific Suggestions

1. Pursuant to Section 1798.185(a)(6) ("*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.*"), we recommend that the Attorney General and the Legislature consider engaging directly with academic researchers, civil society organizations, and Human-Computer Interaction/User Experience Design practitioners to solicit recommendations as to how best to design and implement the notices required by this statute following principles of user-centered design. This engagement could take the form of a formal working group or advisory committee, or a design challenge, for example. The critical requirement is to initiate a formal process that these communities can respond to with a goal of influencing policy; absent this incentive, these communities are not likely to engage in the policymaking process, given that

[4] See: Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. New Media & Society. https://doi.org/10.1177/1461444819833331

academic publishing generally does not reward policy-focused research, and practitioners are unlikely to engage in *pro bono* work without a specific client. Relatedly, the State could also directly commission a research study to achieve these ends.

2. Require that all businesses post standardized language (titles and text) that describe the 'Do Not Sell' right, the process for making a request, and any additional information for consumers. Absent these requirements, companies may be incentivized to use language that misleads consumers. However, we suggest that this language is developed based on a user-centered design process as suggested in (1) above.
3. Amend the definition of "homepage" in Section 1798.140(l) to include the following: "The application's platform page or download page (within an online store and/or on a website), a link within the application" to ensure that apps that are available both through online stores such as Google Play as well as directly on company or personal websites are included.
4. Amend Section 1798.135(a)(1) to include all of a company's digital interfaces (e.g. all mobile applications and mobile websites, in addition to standard websites), and to include information about the right in printed materials accompanying any Internet connected hardware or devices that lack interfaces (e.g., connected devices, such as appliances, or 'smart speakers') or where presenting a link is impracticable.

B. Fundamental changes to the Notice and Consent Framework

While researchers have been examining the problems with notice and consent for nearly two decades, there has been neither federal or state-level efforts to distill these findings and create either recommendations or actual legislation that translates this research into a new framework that aims to make notice standardized, clear and consumer friendly, and gives consumers substantive and meaningful consent options. While the Federal Trade Commission has held workshops[5] exploring the issues around notice design and consent, and has issued guidance for design issues related to disclosures generally,[6] they have not issued guidance beyond their 2012 *Protecting Consumer Privacy in an Era of Rapid Change* report, where they suggested "[p]rivacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices."[7]

California could take a lead in this challenge, by following the suggestions in 7(A)(1) above to commission expert guidance and feedback that addresses both the CCPA specifically and to spark action towards rethinking how we can improve notice and consent mechanisms that effectively inform consumers and give them real and significant choices over their personal information. In order to create a truly privacy-forward law that provides the public with meaningful, actionable rights, the CCPA's notice requirements should not rest on an existing framework that fails to properly inform consumers and provide them with substantive consent processes. Should we eventually see

---

[5] https://www.ftc.gov/news-events/events-calendar/2012/05/short-advertising-privacy-disclosures-digital-world

[6] See the FTC's Dot Com disclosures guide: https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf

[7] https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

action on these issues at the federal level, California's work in this area would serve as a model as to how to reconstitute how we provide notice and obtain consent in the digital world.

In closing, we appreciate this opportunity to submit our comments and provide the Attorney General's office with feedback on this important law.

Sincerely,

Dr. Jennifer King*
Director of Consumer Privacy
Center for Internet and Society
Stanford Law School
[redacted]

Jana Gooth, MLE*
Visiting Research Scholar
Center for Internet and Society
Stanford Law School
[redacted]

*Affiliation provided for identification purposes only. These comments are not submitted on behalf of the Center for Internet and Society.

Message

From: Privacy Regulations [redacted]

Sent: 3/20/2019 1:15:20 PM

To: Tyler Crabtree [redacted]

Subject: FW: [WEB FORM] GENERAL COMMENT OR QUESTION

-----Original Message-----
From: Robert Rutkowski [redacted]
Sent: Tuesday, March 19, 2019 3:20 PM
To: PIUWebform <piuwebform@doj.ca.gov>
Subject: [WEB FORM] GENERAL COMMENT OR QUESTION

Below is the result of the feedback form.
It was submitted by [redacted]

========== DOJ USE ONLY ==========
NEW_TYPE:
========== DOJ USE ONLY ==========

TYPE: PL
First Name: Robert
Middle Initial:
Last Name: Rutkowski
Address Line: [redacted]
Address Line 2:
City: [redacted]
State [redacted]
Zip: [redacted]
Zip4: [redacted]
Area Code: [redacted]
Phone Number: [redacted]

Comment Or Question Message: Attorney General Xavier Becerra
Attorney General's Office
California Department of Justice
Attn: Public Inquiry Unit
P.O. Box 944255
Sacramento, CA 94244-2550
https://oag.ca.gov/contact/general-comment-question-or-complaint-form

Re: Comment on CCPA regulations

Dear Attorney General:

The California Consumer Privacy Act (CCPA) requires the California Attorney General to take input from the public on regulations to implement the law, which does not go into effect until 2020.

The Electronic Frontier Foundation has filed comments on two issues: first, how to verify consumer requests to companies for access to personal information, and for deletion of that information; and second, how to make the process of opting out of the sale of data easy, using the framework already in place for the Do Not Track (DNT) system.

Verification of Requests

When it comes to verifying requests that users make of businesses to access their own data, carefully balance the interest of the consumer in obtaining their own personal information without undue delay or difficulty, with their interest in avoiding theft of their private data by people who might make fraudulent CCPA requests for data.

If a consumer already has a password-protected account, mandate use of that password to verify the account. Further, the business must ensure that the requester really knows the password, and didn't just steal a laptop with an open app, by requiring the requester to log out of the account and present the

password again. Also encourage, but not require, two-factor authentication as a form of verification in cases where doing so poses no risk to the user.

If a consumer does not have a password, the company must be as certain as is reasonably possible that the requester is the subject of the personal information being requested.

Opting Out of Sales

I also encourage you rely on the existing Do Not Track (DNT) system when issuing rules about consumer requests to opt-out of data sales. The DNT system combines a technology (a browsing header that announces the user prefers not to be tracked online) with a policy framework (how companies should respond to that signal).

The DNT header is already widely supported by most major web browsers, including Google Chrome, Mozilla Firefox, and Opera. EFF proposes that the Attorney General require any business that interacts with consumers directly over the Internet to treat a browser's DNT request as a request to opt-out of data collection.

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://www.majorityleader.gov/content/email-whip

[redacted]
P/F: 1[redacted]
E-mail: [redacted]

Re: EFF's comments: https://www.eff.org/document/eff-consumer-data-privacy-comment-california-attorney-general

Affirm Information Accurate: Yes

Email: [redacted]
Confirm Email: [redacted]
Referrer: https://oag.ca.gov/consumers

[End of comment or complaint information]

Message

From: Lara Larramendi [redacted]
Sent: 4/18/2019 2:44:35 PM
To: Privacy Regulations [redacted]
Subject: Fwd: California Consumer Privacy Act of 2018 (CCPA, 2018) - Concerns
Attachments: CCPA_AGBecerra_03-27-2019.pdf; CCPA_AGBecerra_03-27-2019.pdf

Good afternoon.

Attached please find BizFed's letter, addressed to AG Becerra, stating our concerns regarding the potential impacts of the California Consumer Privacy Act of 2018 (CCPA).

If you have any questions, please do not hesitate to contact us. Thank you for your time and consideration to our letter.

Sincerely,

Lara L. Larramendi

P.S. How is government helping or hurting your business growth? What do you want our elected officials, media and BizFed to focus on?
VOICE YOUR OPINIONS, take #BizFedPulsePOLL today! **bizfedlacounty.org/poll**

Lara L. Larramendi, Goverment Relations Director
[redacted]
BizFed.org
Los Angeles County Business Federation
A grassroots alliance of 180 diverse business groups mobilizing 400,000 employers

---------- Forwarded message ---------
From: **Lara Larramendi** [redacted]
Date: Wed, Mar 27, 2019 at 3:01 PM
Subject: California Consumer Privacy Act of 2018 (CCPA, 2018) - Concerns
To: [redacted]
Cc: Liz Saldivar [redacted], De'Andre Valencia [redacted]

Good afternoon.

Attached please find BizFed's letter, addressed to AG Becerra, stating our concerns regarding the potential impacts of the California Consumer Privacy Act of 2018 (CCPA).

If you have any questions, please do not hesitate to contact us. Thank you for your time and consideration to our letter.

Sincerely,

Lara L. Larramendi

P.S. How is government helping or hurting your business growth? What do you want our elected officials, media and BizFed to focus on?
VOICE YOUR OPINIONS, take #BizFedPulsePOLL today! **bizfedlacounty.org/poll**

Lara L. Larramendi, Goverment Relations Director
[redacted]
BizFed.org
Los Angeles County Business Federation
A grassroots alliance of 180 diverse business groups mobilizing 400,000 employers

Los Angeles County Business Federation

Strengthening the Voice of Business Since 2008

March 27, 2019

The Honorable Xavier Becerra
California Attorney General
Department of Justice
1300 "I" St. #1740
Sacramento, CA 95814

RE: California Consumer Privacy Act of 2018

Dear General Becerra,

We are contacting you on behalf of BizFed, a grassroots alliance of more than 180 business organizations, representing more than 400,000 employers with 3.5 million employees in Los Angeles County. As a united federation, we advocate for policies and projects that strengthen our regional economy. I am writing to share our very significant concerns regarding the potential impacts of the California Consumer Privacy Act of 2018 (CCPA).

Los Angeles County has one of the strongest economies in the world and is a primary driver of California's economy. We lead the country in technology, manufacturing, and international trade, and are home to world-class healthcare, entertainment, creative, and design industries. In the last decade, Southern California has become the intersection of content and technology, with both established companies and innovative startups bringing a great, competitive edge to the County -- including hubs like Silicon Beach.

As we learn more about the CCPA through public hearings and rulemaking workshops, we are troubled by the growing evidence that the law may stifle our robust local business environment after the law takes effect January 1, 2020.

We have three primary concerns with the CCPA:

First, Southern California businesses could be limited in their ability to identify and reach customers and clients if the implementation of the law discourages individuals from using technology in their everyday activities.

Virtually all businesses, whether global or local, use the internet in some fashion to function, enhance revenue, provide offerings, and reach new customers. But the vast majority of companies do not "sell" data; rather, they use data to develop and deploy products, tools, and services consumers want, need and expect in today's fast-paced global economy. Businesses don't know personal information about potential customers but certainly, want to provide information about their goods and services to those who may be interested.

Accordingly, the CCPA could impede the ability of smaller enterprises to reach potential customers. The Los Angeles advertising market is large and costly. Television and newspaper advertising is beyond the means of smaller businesses, so the internet has provided an affordable means for small businesses to reach potential customers in their community and also in places far from Los Angeles. These capabilities have fostered real dynamism in, and reach for, our Southern California economy. CCPA's blunt, one-size fits all requirements could take a severe toll on us.

While the CCPA may have been aimed at data-brokers, it misses the mark and unintentionally hurts all businesses that are "data-dependent." If consumers are convinced to "opt-out" from an overly broad notion of "sale of personal information" -- which seems to cover almost any sort of movement of data between two commercial entities -- they may

unwittingly restrict their access to products and services they want and need. If businesses -- particularly online content creators -- that utilize the internet to provide relevant content could lose customers and revenue as the internet marketplace becomes a less effective place to find customers.

Second, the success of the creative community, technology startup companies, advertising agencies and the small- and medium-sized businesses that supply those industries, may be at risk if the privacy law reduces online advertising and other revenue generation. If this new law impacts the success of the creative community, the Southern California community will be disproportionately impacted. Consumer privacy should be achieved without disrupting content platforms, consumer apps, loyalty programs and a host of products and services that rely on a robust online economy.

Third, companies that qualify under the CCPA, could be subject to significant compliance costs to hire lawyers, technology consultants and meet ongoing operational requirements. A small boutique that simply wants to communicate with residents in their area and service existing customers may find the compliance burdens of the CCPA are simply too costly and complicated. Small companies that have found major benefits in free online tools and resources to help streamline their business operations, may be facing new subscription costs or other fee-based models to access the same tools they currently receive for free. California businesses are experiencing significant cost increases, and we certainly do not need to make it even more expensive or add another layer of mandates to the list of obligations.

We're now hearing that instead of fixing the problems with the CCPA, considerations in Sacramento (Legislature and Attorney General) are underway to add massive, untenable litigation hooks to the law that would not only increase compliance costs but could drive companies out of business altogether. That can hardly be a desirable outcome from well-intended efforts to protect consumer data and privacy.

With millions of jobs hanging in the balance, sustaining robust local economic growth is critical for both Los Angeles County and the State of California. We are unwilling to trust that the CCPA will have only positive impacts and urge you and your colleagues to pursue a rigorous examination of its potential pitfalls before it takes effect on January 2020, to avoid significant negative economic impacts on our local businesses.

Please contact us with any questions.

Sincerely,

Steve Bullock
BizFed Chair
Cerrell Associates

David Fleming
BizFed Founding Chair

Tracy Hernandez
BizFed Founding CEO
IMPOWER, Inc.

Los Angeles County Business Federation

Strengthening the Voice of Business Since 2008

BizFed Association Members

Action Apartment Association
AIA - Los Angeles
Alhambra Chamber
American Beverage Association
American Hotel & Lodging Association
Antelope Valley Board of Trade
Angeles Emeralds
Apartment Association, California Southern Cities
Apartment Association of Greater Los Angeles
Arcadia Association of Realtors
AREAA North Los Angeles SFV SCV
Asian Business Association
Association of Independent Commercial Producers
Azusa Chamber
Beverly Hills Bar Association
Beverly Hills Chamber
Beverly Hills / Greater LA Association of Realtors
BNI4SUCCESS
Burbank Association of Realtors
Building Industry Association, LA / Ventura Counties
Building Owners & Managers Association, Greater LA
Business & Industry Council for Emergency Planning & Preparedness
CalAsian Chamber
California Apartment Association, Los Angeles
California Asphalt Pavement Association
California Bus Association
California Business Roundtable
California Cannabis Industry Association
California Construction Industry and Materials Association
California Contract Cities Association
California Fashion Association
California Gaming Association
California Grocers Association
California Hotel & Lodging Association
California Independent Oil Marketers
California Independent Petroleum Association
California Life Sciences Association
California Metals Coalition
California Restaurant Association
California Small Business Alliance
California Sportfishing League
California Trucking Association
Carson Chamber of Commerce
Carson Dominguez Employers Alliance
CDC Small Business Finance
Central City Association
Century City Chamber of Commerce
Cerritos Chamber
Citrus Valley Association of Realtors
Commerce Industrial Council/Chamber of Commerce
Construction Industry Air and Water Quality Coalitions
Council on Trade and Investment for Filipino Americans
Covina Chamber of Commerce
Culver City Chamber of Commerce
Downey Association of Realtors
Downey Chamber of Commerce
Downtown Long Beach Alliance
El Monte/South El Monte Chamber
Employers Group
Engineering Contractor's Association
F.A.S.T.-Fixing Angelenos Stuck In Traffic
FilmLA
FuturePorts
Gardena Valley Chamber of Commerce
Gateway to LA
Glendale Association of Realtors
Glendale Chamber
Glendora Chamber
Greater Antelope Valley AOR
Greater Lakewood Chamber
Greater Los Angeles African American Chamber
Greater Los Angeles New Car Dealers Association
Harbor Trucking Association
Historic Core Bid
Hollywood Chamber
Hong Kong Trade Development Council
Hospital Association of Southern California
Hotel Association of Los Angeles
Industry Business Council
Inglewood Airport Area Chamber of Commerce
International Warehouse Logistics Association
Irwindale Chamber
La Canada Flintridge Chamber
LAX Coastal Area Chamber
League of California Cities
Long Beach Area Chamber
Los Angeles Area Chamber
Los Angeles County Medical Association
Los Angeles County Waste Management Association
Los Angeles Gateway Chamber of Commerce
Los Angeles Gay & Lesbian Chamber of Commerce
Los Angeles Latino Chamber

Los Angeles Parking Association
Maple Business Council
Motion Picture Association of America
MoveLA
NAIOP Southern California Chapter
National Association of Royalty Owners
National Association of Tobacco Outlets
National Association of Women Business Owners
National Association of Women Business Owners, LA
National Hispanic Medical Association
National Latina Business Women's Association
Nederlands-America Foundation
Orange County Business Council
Pacific Merchant Shipping Association
Pacific Palisades Chamber
Panorama City Chamber
Paramount Chamber of Commerce
Pasadena Chamber
Pasadena-Foothills Association of Realtors
PhRMA
Planned Parenthood Southern California Affiliates
Pomona Chamber
PropelLA
Rancho Southeast Association of Realtors
Recording Industry Association of America
Regional Black Chamber - San Fernando Valley
Regional San Gabriel Valley Chamber
Rosemead Chamber
San Gabriel Chamber
San Gabriel Valley Civic Alliance
San Gabriel Valley Economic Partnership
Santa Clarita Valley Chamber
Santa Clarita Valley Economic Development Corp.
San Pedro Peninsula Chamber
Santa Monica Chamber
Santa Monica Junior Chamber
Sherman Oaks Chamber of Commerce
South Bay Association of Chambers
South Bay Association of Realtors
Southern California Contractors Association
Southern California Golf Association
Southern California Grantmakers
Southern California Leadership Coalition
Southern California Minority Supplier Development Council Inc.
Southern California Water Coalition
Southland Regional Association of Realtors
The Young Professionals at the Petroleum Club
Torrance Area Chamber
Town Hall Los Angeles
Tri-Counties Association of Realtors
United Chambers San Fernando Valley
United States-Mexico Chamber
Unmanned Autonomous Vehicle Systems Association
US Resiliency Council
Valley Industry & Commerce Association
Vernon Chamber
Vietnamese American Chamber
Warner Center Association
West Hollywood Chamber
West Los Angeles Chamber
West San Gabriel Valley Association of Realtors
West Valley/Warner Center Chamber
Western Manufactured Housing Association
Western States Petroleum Association
Westside Council of Chambers
Westwood Village Rotary Club
Wilmington Chamber
World Trade Center
Young Professionals in Energy - LA Chapter

Los Angeles County Business Federation

Strengthening the Voice of Business Since 2008

March 27, 2019

The Honorable Xavier Becerra
California Attorney General
Department of Justice
1300 "I" St. #1740
Sacramento, CA 95814

RE: California Consumer Privacy Act of 2018

Dear General Becerra,

We are contacting you on behalf of BizFed, a grassroots alliance of more than 180 business organizations, representing more than 400,000 employers with 3.5 million employees in Los Angeles County. As a united federation, we advocate for policies and projects that strengthen our regional economy. I am writing to share our very significant concerns regarding the potential impacts of the California Consumer Privacy Act of 2018 (CCPA).

Los Angeles County has one of the strongest economies in the world and is a primary driver of California's economy. We lead the country in technology, manufacturing, and international trade, and are home to world-class healthcare, entertainment, creative, and design industries. In the last decade, Southern California has become the intersection of content and technology, with both established companies and innovative startups bringing a great, competitive edge to the County -- including hubs like Silicon Beach.

As we learn more about the CCPA through public hearings and rulemaking workshops, we are troubled by the growing evidence that the law may stifle our robust local business environment after the law takes effect January 1, 2020.

We have three primary concerns with the CCPA:

First, Southern California businesses could be limited in their ability to identify and reach customers and clients if the implementation of the law discourages individuals from using technology in their everyday activities.

Virtually all businesses, whether global or local, use the internet in some fashion to function, enhance revenue, provide offerings, and reach new customers. But the vast majority of companies do not "sell" data; rather, they use data to develop and deploy products, tools, and services consumers want, need and expect in today's fast-paced global economy. Businesses don't know personal information about potential customers but certainly, want to provide information about their goods and services to those who may be interested.

Accordingly, the CCPA could impede the ability of smaller enterprises to reach potential customers. The Los Angeles advertising market is large and costly. Television and newspaper advertising is beyond the means of smaller businesses, so the internet has provided an affordable means for small businesses to reach potential customers in their community and also in places far from Los Angeles. These capabilities have fostered real dynamism in, and reach for, our Southern California economy. CCPA's blunt, one-size fits all requirements could take a severe toll on us.

While the CCPA may have been aimed at data-brokers, it misses the mark and unintentionally hurts all businesses that are "data-dependent." If consumers are convinced to "opt-out" from an overly broad notion of "sale of personal information" -- which seems to cover almost any sort of movement of data between two commercial entities -- they may

unwittingly restrict their access to products and services they want and need. If businesses -- particularly online content creators -- that utilize the internet to provide relevant content could lose customers and revenue as the internet marketplace becomes a less effective place to find customers.

Second, the success of the creative community, technology startup companies, advertising agencies and the small- and medium-sized businesses that supply those industries, may be at risk if the privacy law reduces online advertising and other revenue generation. If this new law impacts the success of the creative community, the Southern California community will be disproportionately impacted. Consumer privacy should be achieved without disrupting content platforms, consumer apps, loyalty programs and a host of products and services that rely on a robust online economy.

Third, companies that qualify under the CCPA, could be subject to significant compliance costs to hire lawyers, technology consultants and meet ongoing operational requirements. A small boutique that simply wants to communicate with residents in their area and service existing customers may find the compliance burdens of the CCPA are simply too costly and complicated. Small companies that have found major benefits in free online tools and resources to help streamline their business operations, may be facing new subscription costs or other fee-based models to access the same tools they currently receive for free. California businesses are experiencing significant cost increases, and we certainly do not need to make it even more expensive or add another layer of mandates to the list of obligations.

We're now hearing that instead of fixing the problems with the CCPA, considerations in Sacramento (Legislature and Attorney General) are underway to add massive, untenable litigation hooks to the law that would not only increase compliance costs but could drive companies out of business altogether. That can hardly be a desirable outcome from well-intended efforts to protect consumer data and privacy.

With millions of jobs hanging in the balance, sustaining robust local economic growth is critical for both Los Angeles County and the State of California. We are unwilling to trust that the CCPA will have only positive impacts and urge you and your colleagues to pursue a rigorous examination of its potential pitfalls before it takes effect on January 2020, to avoid significant negative economic impacts on our local businesses.

Please contact us with any questions.

Sincerely,

Steve Bullock
BizFed Chair
Cerrell Associates

David Fleming
BizFed Founding Chair

Tracy Hernandez
BizFed Founding CEO
IMPOWER, Inc.

Los Angeles County Business Federation

Strengthening the Voice of Business Since 2008

BizFed Association Members

Action Apartment Association
AIA - Los Angeles
Alhambra Chamber
American Beverage Association
American Hotel & Lodging Association
Antelope Valley Board of Trade
Angeles Emeralds
Apartment Association, California Southern Cities
Apartment Association of Greater Los Angeles
Arcadia Association of Realtors
AREAA North Los Angeles SFV SCV
Asian Business Association
Association of Independent Commercial Producers
Azusa Chamber
Beverly Hills Bar Association
Beverly Hills Chamber
Beverly Hills / Greater LA Association of Realtors
BNI4SUCCESS
Burbank Association of Realtors
Building Industry Association, LA / Ventura Counties
Building Owners & Managers Association, Greater LA
Business & Industry Council for Emergency Planning & Preparedness
CalAsian Chamber
California Apartment Association, Los Angeles
California Asphalt Pavement Association
California Bus Association
California Business Roundtable
California Cannabis Industry Association
California Construction Industry and Materials Association
California Contract Cities Association
California Fashion Association
California Gaming Association
California Grocers Association
California Hotel & Lodging Association
California Independent Oil Marketers
California Independent Petroleum Association
California Life Sciences Association
California Metals Coalition
California Restaurant Association
California Small Business Alliance
California Sportfishing League
California Trucking Association
Carson Chamber of Commerce
Carson Dominguez Employers Alliance
CDC Small Business Finance
Central City Association
Century City Chamber of Commerce
Cerritos Chamber
Citrus Valley Association of Realtors
Commerce Industrial Council/Chamber of Commerce
Construction Industry Air and Water Quality Coalitions
Council on Trade and Investment for Filipino Americans
Covina Chamber of Commerce
Culver City Chamber of Commerce
Downey Association of Realtors
Downey Chamber of Commerce
Downtown Long Beach Alliance
El Monte/South El Monte Chamber
Employers Group
Engineering Contractor's Association
F.A.S.T.-Fixing Angelenos Stuck In Traffic
FilmLA
FuturePorts
Gardena Valley Chamber of Commerce
Gateway to LA
Glendale Association of Realtors
Glendale Chamber
Glendora Chamber
Greater Antelope Valley AOR
Greater Lakewood Chamber
Greater Los Angeles African American Chamber
Greater Los Angeles New Car Dealers Association
Harbor Trucking Association
Historic Core Bid
Hollywood Chamber
Hong Kong Trade Development Council
Hospital Association of Southern California
Hotel Association of Los Angeles
Industry Business Council
Inglewood Airport Area Chamber of Commerce
International Warehouse Logistics Association
Irwindale Chamber
La Canada Flintridge Chamber
LAX Coastal Area Chamber
League of California Cities
Long Beach Area Chamber
Los Angeles Area Chamber
Los Angeles County Medical Association
Los Angeles County Waste Management Association
Los Angeles Gateway Chamber of Commerce
Los Angeles Gay & Lesbian Chamber of Commerce
Los Angeles Latino Chamber

Los Angeles Parking Association
Maple Business Council
Motion Picture Association of America
MoveLA
NAIOP Southern California Chapter
National Association of Royalty Owners
National Association of Tobacco Outlets
National Association of Women Business Owners
National Association of Women Business Owners, LA
National Hispanic Medical Association
National Latina Business Women's Association
Nederlands-America Foundation
Orange County Business Council
Pacific Merchant Shipping Association
Pacific Palisades Chamber
Panorama City Chamber
Paramount Chamber of Commerce
Pasadena Chamber
Pasadena-Foothills Association of Realtors
PhRMA
Planned Parenthood Southern California Affiliates
Pomona Chamber
PropelLA
Rancho Southeast Association of Realtors
Recording Industry Association of America
Regional Black Chamber - San Fernando Valley
Regional San Gabriel Valley Chamber
Rosemead Chamber
San Gabriel Chamber
San Gabriel Valley Civic Alliance
San Gabriel Valley Economic Partnership
Santa Clarita Valley Chamber
Santa Clarita Valley Economic Development Corp.
San Pedro Peninsula Chamber
Santa Monica Chamber
Santa Monica Junior Chamber
Sherman Oaks Chamber of Commerce
South Bay Association of Chambers
South Bay Association of Realtors
Southern California Contractors Association
Southern California Golf Association
Southern California Grantmakers
Southern California Leadership Coalition
Southern California Minority Supplier Development Council Inc.
Southern California Water Coalition
Southland Regional Association of Realtors
The Young Professionals at the Petroleum Club
Torrance Area Chamber
Town Hall Los Angeles
Tri-Counties Association of Realtors
United Chambers San Fernando Valley
United States-Mexico Chamber
Unmanned Autonomous Vehicle Systems Association
US Resiliency Council
Valley Industry & Commerce Association
Vernon Chamber
Vietnamese American Chamber
Warner Center Association
West Hollywood Chamber
West Los Angeles Chamber
West San Gabriel Valley Association of Realtors
West Valley/Warner Center Chamber
Western Manufactured Housing Association
Western States Petroleum Association
Westside Council of Chambers
Westwood Village Rotary Club
Wilmington Chamber
World Trade Center
Young Professionals in Energy - LA Chapter

Message

From: Dwyer, Patrick [redacted]
Sent: 5/1/2019 10:08:44 AM
To: Privacy Regulations [redacted]
Subject: RE: California Consumer Privacy Act of 2018—Pre-Rulemaking Comment Letter
Attachments: Comments on CA Consumer Privacy Act.pdf

Dear Sir or Madam:

Mastercard International Incorporated appreciates this opportunity to submit written comments in response to the preliminary rulemaking activities undertaken by the California Department of Justice prior to the official rulemaking required by the California Consumer Privacy Act of 2018.

Best,

Patrick Dwyer

Patrick Dwyer
Director
State Public Policy

Mastercard | mobile [redacted]

mastercard

April 30, 2019

By Email

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

RE: California Consumer Privacy Act of 2018—Pre-Rulemaking Comment Letter

Dear Sir or Madam:

Mastercard International Incorporated ("Mastercard")[1] appreciates this opportunity to submit written comments in response to the preliminary rulemaking activities undertaken by the California Department of Justice prior to the official rulemaking required by the California Consumer Privacy Act of 2018 ("CCPA" or the "Act").

Discussion

A. Introduction

The CCPA requires that on or before July 1, 2020, the Attorney General ("AG") solicit broad public participation to adopt regulations implementing the CCPA. Cal. Civ. Code § 1798.185(a). The CCPA specifically requires the AG to solicit public participation and adopt regulations to further the purposes of the CCPA with regard to seven enumerated areas. Id. Mastercard's comments are focused on two topics in areas for which the AG is required to solicit public participation and issue regulations as needed: what should (and should not) be included in personal information, id. § 1798.185(a)(1), and exceptions to the Act's coverage to comply with state or federal law relating to trade secrets and intellectual property rights. Id. § 1798.185(a)(3).

Accordingly, as your office prepares to issue regulations in accordance with the CCPA, we respectfully submit the following requests for clarification for your consideration. Mastercard believes these clarifications will better enable all interested parties to comply with

[1] Mastercard is a technology company in the global payments industry. We operate the world's fastest payments processing network, connecting consumers, financial institutions, merchants, governments and businesses in more than 210 countries and territories. Mastercard's products and solutions make everyday commerce activities—such as shopping, traveling, running a business and managing finances—easier, more secure and more efficient for everyone.

the law, provide needed certainty with regard to legally protected proprietary interests, and ensure consistency with the intent of the CCPA.

B. Definition of "Personal Information"

The CCPA requires the AG to solicit public input and issue regulations as needed on what information should be included in personal information. Cal. Civ. Code § 1798.185(a)(1). How personal information is ultimately defined is a key issue under the Act, because the Act establishes various rights of consumers with respect to their personal information that is collected or held by businesses. Similarly, for businesses, the definition of personal information is significant because it defines the scope of the obligations of businesses that collect or hold personal information about consumers. The definition of personal information in the Act includes several vague phrases that do not appear to have been used in a U.S. or major international privacy law, including, for example, the phrase "capable of being associated with." Cal. Civ. Code § 1798.140(o)(1). Such novel and vague language is potentially unlimited in its breadth, which will create significant uncertainty as to the scope of consumer rights and the impact and obligations from the CCPA on businesses. Thus, Mastercard believes that it is important to ensure that the question of what is included, and necessarily what is not included, in the definition of personal information is clear.

In this regard, Mastercard respectfully suggests that the rules issued by the AG should make clear that "personal information" does not include pseudonymous information. Mastercard believes that the exclusion of pseudonymous information from "personal information" is consistent with both the language of the Act and its intent.

For example, the CCPA defines "personal information" to mean "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." Cal. Civ. Code § 1798.140(o)(1). The definition includes a list of eleven types of information that may constitute personal information, including "identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers[,]" but in each case such information falls within the definition 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[.]" Id. While this definition is broad, the Act also recognizes privacy protective data minimization processing by including explicit references and definitions for "deidentified," "aggregate consumer information" and "pseudonymize" or "pseudonymization." Id., at § 1798.140(a), (h) and (r).

Consistent with the basic definition of personal information, the Act defines "pseudonymize" as "the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer." Cal. Civ. Code § 1798.140(r).

Once information is pseudonymized, a business that holds such information should have no obligation to re-link or reidentify the information data that has been disassociated with and is no longer attributable to a particular consumer in order to satisfy a request by a consumer wishing to exercise their rights under the Act. For example, the CCPA provision that entitles a consumer to request that a business disclose personal information that the business has collected about the consumer states explicitly that "this section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information." Cal. Civ. Code § 1798.100(e). Similarly, the CCPA section that lists the information that a business must disclose to a consumer states that the business is not required to "reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information." Cal. Civ. Code § 1798.110(d)(2). Finally, the CCPA contains a general statement of intent making clear that "this title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information." Cal. Civ. Code § 1798.145(i).

Given the existing definitions of "personal information" and "pseudonymize" and the fact that the Act is clear that a business has no obligation to reidentify information, Mastercard believes that the intent of the Act is not to treat pseudonymized information as personal information. However, the Act contains provisions that could create some confusion, which is why Mastercard believes clarification is necessary. In particular, the definition of personal information includes numerous traditional identifiers, as well as "other similar identifiers." Cal. Civ. Code § 1798.140(o)(1)(A). This creates potential ambiguity for pseudonymized data sets which replace attributable identifiers with anonymous identifiers. To avoid confusion, Mastercard respectfully suggests that the AG clarify this point in its rules implementing the Act by expressly stating that pseudonymized information does not constitute personal information, or that a pseudonymized identifier is not an identifier per Cal. Civ. Code § 1798.140(o)(1)(A).

C. Application of the CCPA to Intellectual Property or the Disclosure of Information that would Reveal Data or Infringe on a Third Party's Rights

The CCPA specifically grants the AG the authority 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, within one year of passage of this title and as needed thereafter." Cal. Civ. Code § 1798.185(a)(3).

Federal and state laws provide a variety of protections for intellectual property, including information subject to copyright, patent, service mark and/or trade secret protections. In addition, many businesses hold information the disclosure of which would infringe or adversely effect the rights or freedoms of third parties. Mastercard respectfully suggests that the AG, under the authority noted above, issue rules establishing an exception from the CCPA's access and deletion obligations for those types of proprietary information that are subject to protection under federal or state law. Mastercard respectfully suggests that a business should not be required to disclose or delete any information that is subject to intellectual property protections, including any formula, pattern, compilation, program, device, method, technique, or process

developed to process or analyze personal information, any information derived from such process or analysis, or any other trade secrets, intellectual property or material nonpublic information.

D. Conclusions

Mastercard appreciates the opportunity to provide comments regarding the preliminary rulemaking required by the CCPA. If there are any questions regarding our comments, please do not hesitate to contact the undersigned at [redacted] or [redacted] or our counsel at Sidley Austin LLP in this matter, Joel D. Feinberg, at [redacted]

Sincerely,

/s/ Patrick S. Dwyer

Patrick S. Dwyer
Director, Public Policy, U.S. Markets

cc: Joel D. Feinberg, Sidley Austin LLP
Patrick K. O'Keefe, Sidley Austin LLP

Message

From: Patack, Melissa [redacted]
Sent: 4/16/2019 9:01:30 AM
To: Privacy Regulations [redacted]
CC: Stacey Schesser [redacted]
Subject: Suggested Guidelines to be issued by AG
Attachments: 4628_001.pdf

Thank you for your consideration. Please find cover letter and suggested draft guidelines attached.

Melissa Patack

Vice President & Sr. Counsel

State Government Affairs

Motion Picture Association of America, Inc.

W: [redacted] C: [redacted]

From: Copier Scanner
Sent: Tuesday, April 16, 2019 9:03 AM
To: Patack, Melissa [redacted]
Subject: Attached Image

MOTION PICTURE ASSOCIATION OF AMERICA, INC.
15301 VENTURA BOULEVARD, BUILDING E
SHERMAN OAKS, CA 91403
Main: [redacted]

MELISSA PATACK
Vice President & Sr. Counsel
State Government Affairs

[redacted] Direct
[redacted] – Cell
[redacted]

April 16, 2019

The Honorable Xavier Becerra
Attorney General
State of California
P.O. Box 944255
Sacramento CA 94244

Dear Attorney General Becerra:

On behalf of the Motion Picture Association of America, Inc. and our member companies, enclosed please find comments your office has invited with regard to issuing guidelines on business practices and procedures that would be considered compliant with specified provisions of the California Consumer Privacy Act.

If your or your staff has any questions or need further information, please don't hesitate to contact me, or our legislative advocate in Sacramento, Felipe Fuentes, who can be reached at [redacted]

We appreciate your consideration.

Sincerely,

Melissa Patack

cc: Felipe Fuentes, The Apex Group

The California Consumer Privacy Act ("CCPA") requires businesses to establish numerous practices and procedures to comply with the law's requirements. There are several areas in which businesses may have specific practices or procedures in place which are consistent with the purposes of CCPA and should be considered as meeting requirements of CCPA. MPAA urges Attorney General Becerra to issue guidance to businesses confirming that the use of these practices or procedures would be deemed compliant with CCPA. Below are some examples.

Verification of identity

Section 1798.130 (a) (2) requires a business to disclose and deliver required information to a consumer who has made a verifiable consumer request. The Attorney General should provide guidance and examples of acceptable procedures that could be utilized by a business to determine a verifiable consumer request. **Suggested Language:**

The following methods are appropriate, but not exclusive, ways to verify a consumer's identify before providing information:

- *The consumer logs into an online account with their account credentials and follows instructions to make a request for information. This method may include a form of two-factor authentication or other security steps. An example of two-factor authentication is inputting a code that has been sent to an email or phone number associated with the account.*

- *The consumer transmits a copy of a current, government issued identification showing at a minimum name, street address located in California, and date of birth.*

- *The consumer provides one or more data points requested by the business to enable the business to cross-reference for identity verification purposes. Examples of such data points are a verified phone number, verified email address, method of payment, or transaction history.*

- *The consumer correctly responds to a series of knowledge-based questions which only the person being verified can answer. Questions may be, but are not required to be generated through dynamic knowledge-based authentication services.*

- *The customer is able to correctly verify a unique code sent to a previously verified address, telephone number, email account which is associated with the consumer's account with the business.*

The law specifies that a consumer may make a request on behalf of the consumer's minor child. Many businesses are required to comply with the federal Children's Online Privacy Protection Act (COPPA), which addresses online marketing and other online engagement of children under 13. The Federal Trade Commission has promulgated regulations addressing children's privacy and the responsibilities and obligations that businesses must assume and undertake in engaging children online. See CFR Title 16 Part 312. Included are specific procedures for obtaining verifiable parental consent, and the right of the parent to review the personal information provided by the child. The Attorney General should issue guidance indicating that the business' compliance with COPPA, with regard to parental consent, verification of the parent's identity to exercise rights on behalf of a child under 13, and review of the minor child's personal information, will satisfy compliance with CCPA. **Suggested Language:**

For a verified consumer request submitted by a consumer on behalf of the consumer's minor child, a business that is compliant with regulations promulgated by the Federal Trade Commission implementing the Children's Online Privacy Protection Act, 16 C.F.R. section 312.1 et seq. ("COPPA") and/or which utilizes or otherwise incorporates parental verification methods consistent with the requirements of COPPA for the purposes of verifying a consumer request submitted by a consumer on behalf of the consumer's child under 13 will be in compliance with the California Consumer Privacy Act.

The CCPA provides that a consumer may authorize a person to act on the consumer's behalf. A person acting as a representative of the consumer is required to register with the Secretary of State. The Attorney General should provide guidance and examples of acceptable procedures that could be utilized by a business to determine a verifiable consumer request. **Suggested Language:**

When a person registered with the Secretary of State has been authorized by the consumer to act on the consumer's behalf ("Authorized Agent"), the following methods are appropriate, but not exclusive, ways for a business to verify the Authorized Agent's identity before providing information:

- *A business may require the Authorized Agent to submit a method of verification as though the consumer were making the request for information directly of the business; and*

- *A business may require the Authorized Agent to submit verification of their own identity and authorization to act on behalf of a consumer, as well as verification of their registration with the Secretary of State.*

Unverifiable Consumer Requests

Section 1798.130 requires a business to provide the required information to the consumer within 45 days of receiving a verifiable consumer request [subject to an additional 90 day extension as provided in Section 1798.145(g)(1)]. This section also specifies that efforts to verify the request would not extend the 45 day required response time frame, absent one extension of the 45 day time period. The Attorney General should provide guidance that if a business is unable to verify the consumer within the 45 day time frame using any of the above procedures, the business will not be in violation of the CCPA for failure to provide the requested information. **Suggested Language:**

A business that has attempted to utilize one or more of the procedures specified in ____, or an equivalent procedure, to identify a consumer but has been unable to determine, within 45 days of receiving the consumer request, that the request is a verifiable consumer request, shall not be required to provide information to the consumer, pursuant to Sections 1798.110 and 1798.115.

Format of response to verifiable consumer requests

Section 1798.130 (a)(2) requires a business to deliver required information to a consumer in a "readily usable format that allows the consumer to transmit this information from one entity to another entity without hindrance." The Attorney General should provide guidance on what formats would be acceptable and provide examples. **Suggested Language:**

"Readily usable" shall include any structured, commonly used and machine-readable format, at the business' discretion. Examples include, but are not limited to, .csv, .pdf and JSON files.

Message

[redacted]

From: Greg Campbell [redacted]
Date: May 3, 2019 at 1:32:15 PM PDT
To: Laura Stuber [redacted]
Subject: Thank you

Laura-

Just following up with you from our meeting yesterday. I really appreciate the time you spent with us.

As promised here is the document we went through at the meeting.

Please let me know if you need any clarification or further context on any of these issues.

We look forward to having future discussions. I hope you enjoy your weekend.

Greg Campbell
Campbell Strategy & Advocacy
[redacted]

I. Summary of Key Background and Recommendations for AG

A. Background

1. The protection of consumer privacy is a core value of Comcast. It is essential to maintain our customers' trust regarding the protection and responsible processing of their personal data.
2. We take this responsibility seriously and are diligently working toward compliance with the many new requirements of the CCPA, as enacted.
3. We also appreciate the challenges the AG office faces in implementing this new law, and we are committed to remaining constructive in our suggestions on establishing a reasonable regulatory path forward that best serves consumers and facilitates compliance by CA businesses.

B. Recommendations for AG

1. *Focus on a few discrete rules and clarifications.*

a) There are several key areas where the AG's adoption of rules would provide necessary guidance to businesses that will assist in their compliance efforts.

b) These include (i) defining the acceptable methods and parameters of what constitutes "verifiable consumer requests;" (ii) the timing for compliance with such requests; and (iii) setting an effective date for the AG's rules that gives businesses sufficient time to implement them.

c) We have included below and in the Appendix specific recommendations and proposed rule language to address these issues.

2. *Beyond the above and any other required discrete rules, the AG should allow time to assess how businesses are implementing the new requirements and whether further definitional or other regulatory adjustments are needed after the law is operationalized.*

a) The AG should refrain from adding more requirements at this early stage (e.g., new categories of personal information or unique identifiers). Instead, it should monitor how the law is operationalized, including (i) businesses' responses to consumer requests for access, deletion, and opt-out, and (ii) whether consumers' rights are adequately addressed by the existing broad definitions and other provisions contained in the CCPA.

b) This measured, incremental approach is especially warranted given that the CCPA is actively undergoing an amendment process, and many of the issues the AG is authorized to update may change later this year.

3. *Adopt a "reasonableness" test for compliance*.

   a) If a business has a good system in place for compliance, the AG should encourage remediation, system improvements, and greater compliance as opposed to fines for a technical violation.

   b) This "reasonableness" standard is consistent with the APA's and CCPA's requirements that an agency consider:

      (1) The public benefits of a regulation and alternatives that may be less burdensome and equally effective in achieving the purpose. (Government Code Section 11346.2(b)(1));

      (2) The potential adverse economic impact of each regulation on California businesses and individuals, with the goal of "avoiding the imposition of unnecessary or unreasonable regulations or reporting, recordkeeping, or compliance requirements." (Government Code Section 11346.3(a)); and

      (3) The "obstacles to implementation" and "the goal of minimizing the administrative burden on consumers" and "the burden on business." (CCPA Section 1798.185(a)(1), (2) and (7)).

II. Specific Substantive Rule Recommendations

A. *Verifiable Consumer Requests – Methods* (Section 1798.175(a)(7))

1. Provide **flexibility** and allow businesses to verify requests for access, deletion, or opt out of sale received from a consumer (or authorized person on the consumer's behalf) based on, among other factors, a consumer's relationship with the business, especially given the wide scope of businesses subject to the CCPA.
2. Allow verification methods that many businesses **already utilize to comply with other privacy laws**, such as the GDPR, California Shine the Light Law, Children's Online Privacy Protection Act. (See. e.g., GDPR Art. 15-22; CA Section 1798.83; FTC rules in 16 CFR 312.5).
3. Provide businesses **protection from liability** if an unauthorized disclosure occurs after verifying a consumer (or authorized person on the consumer's behalf) with a method deemed permissible under the rules.
4. Permit a business to (i) **request additional information** from a consumer making a request if the business has any doubts about the requester's identity based on the initial information provided; and (ii) **decline to provide information if the request cannot be verified** after reasonable efforts to do so using approved methods.
5. The specific rules set out in the Appendix address all of the above issues.

B. ***Verifiable Consumer Requests – Timing*** **(Section 1798.175(a)(7))**

1. Section 1798.185(a)(7) provides that AG regulations are required to specify the form and procedures for consumers to submit a request to a business and the rules and procedures for a business to determine that a request received is a "verifiable consumer request."
2. Section 1798.140(y) defines "verifiable consumer request" as a request by a consumer (or authorized person on the consumer's behalf) "that the business can reasonably verify, ***pursuant to regulations adopted by the Attorney General" as required by Section 1798.185(a)(7)***. It further specifies that a business is not obligated to comply with such requests "if the business cannot verify, pursuant to this subdivision ***and regulations adopted by the Attorney General pursuant to [Section 1798(a)(7)]***, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf." (emphases added)
3. The above sections, and the overall statutory scheme, provide that CCPA's requirement for a business to respond to a consumer request is not triggered until *after* the AG has adopted regulations to specify how a business can determine if it is a "verifiable consumer request."
4. It would thus be contrary to the plain language of the CCPA, as well as unreasonable and contrary to the purpose of the CCPA, to require a business to respond to a consumer request *prior* to the AG adopting regulations on a "verifiable consumer request."
5. Notwithstanding the clear provisions noted above, it is possible some may claim that CCPA's operative date of January 1, 2020 means that businesses must respond to consumers' requests any time after January 1, 2020 even if final AG regulations are not yet adopted and in effect.
6. To avoid such confusion and to provide needed certainty to consumers and businesses as to the timing of the obligation to respond to a consumer request, we recommend that the AG adopt the timing rule set out in the Appendix. This rule indicates that a business's obligation to respond to consumer access requests shall apply only after the adoption and effective date of final AG regulations defining the parameters of such requests.

C. ***Effective Date of AG Regulations and Enforcement***

1. The statute does not state the date by which compliance with the AG's rules is required and when failure to comply could constitute a violation.
2. It would be unreasonable to expect compliance starting on the same date or soon after final regulations are published, especially since such regulations might require adjustments to businesses' practices and operations in order to comply with them.
3. Moreover, the APA specifies that agency regulations generally become effective on a quarterly basis and no less than two calendar months after

final regulations are filed with the Secretary of State unless, among other reasons, the authorizing statute specifies otherwise. (Government Code Section 11343.4)

4. In this case, the CCPA specifies a six-month *enforcement* date, which is reasonable to construe as being the same as the *effective* date of the AG's regulations under the language of the APA.

5. Thus, the rule recommended below specifies the effective date of the AG's regulations when compliance is required as six months after publication of the final rules.

Appendix – Proposed Rule Language

Proposed Regulations – Verifiable Consumer Requests – Methods

(a) (1) A business is not obligated to disclose information in response to an access, deletion, opt-out, or other request from a consumer (or authorized person on the consumer's behalf) under Sections 1798.100, 1798.105, 1798.110, 1798.115, or otherwise under the California Consumer Privacy Act, unless the business can verify that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by a consumer to act on that consumer's behalf, which shall be deemed a "verifiable consumer request."

(2) The following methods are appropriate, but not exclusive, ways to verify a consumer's identify before disclosing such information, each of which shall be deemed *per se* reasonable as a verification method:

(A) Submission of a current government-issued identification or an original, notarized request.

(B) The consumer **(or authorized person on the consumer's behalf)** provides one or more data points requested by the business to enable the business to cross-reference for identity verification purposes. Examples of such data points are a verified phone number, verified email address, method of payment, or transaction history.

(C) Verification of identity through the use of a third-party identity verification service.

(D) The consumer logs into a password-protected online account with their account credentials and follows instructions to make a request for such information. This method may include a form of two-factor or multi-factor authentication or other security steps. An example of two-factor authentication is inputting a code that has been sent to an email or phone number associated with the consumer's account by the business.

(E) The consumer correctly responds to a series of knowledge-based questions which only the individual being verified can answer. Questions may be, but are not required to be, generated through dynamic knowledge-based authentication services.

(F) The consumer is able to correctly verify a unique code sent to a previously verified address, telephone number, or email account which is associated with the consumer's account with the business.

(3) For determining whether a request made by a person on behalf of a consumer is a "verifiable consumer request," the requester shall be required to demonstrate that the consumer has knowingly and specifically authorized the requester to make a request regarding that consumer's personal information, or the business may request confirmation of such authorization directly from the consumer. The following methods are appropriate, but not exclusive, ways for a business to verify such requester's identity before providing information, each of which shall be deemed *per se* reasonable as a verification method:

(A) Requiring such requester to be registered with the California Secretary of State as an agent of the other consumer with a registration that includes the authority to make a request related to disclosure of the consumer's personal information pursuant to the California Consumer Privacy Act. When a person registered with the Secretary of State has been authorized by the consumer to act on the consumer's behalf ("Authorized Agent"):

(i) A business may require the Authorized Agent to submit a method of verification as though the consumer were making the request for information directly of the business; and

(ii) A business may require the Authorized Agent to submit verification of its own identity and authorization to act on behalf of the consumer, as well as verification of its registration with the Secretary of State.

(B) Requiring such requester to provide proof of appointment as the consumer's legal guardian, fiduciary, or similar legally authorized and recognized person.

(C) For a consumer request submitted by a person on behalf of the person's minor child, a business that is compliant with regulations promulgated by the Federal Trade Commission implementing the Children's Online Privacy Protection Act, 16 C.F.R. section 312.1 et seq. ("COPPA"), and/or which utilizes or otherwise incorporates parental verification methods consistent with the requirements of COPPA for the purposes of verifying a consumer request submitted by a consumer on behalf of the consumer's child under 13, will be deemed to be a "verifiable consumer request" in compliance with the California Consumer Privacy Act and any implementing regulations.

(4) If a business cannot verify the identity of the requester from the information initially submitted and thus cannot conclude that it is a "verifiable consumer request," the business may request additional information from the consumer or other requester.

(5) A business that utilizes one or more of the procedures specified under subsection 2 or 3 of this section, or an equivalent procedure, to verify the identity of a consumer (or authorized person on the consumer's behalf), shall not be held liable, in any action by the Attorney General or other enforcement authority or in any private action under the California Consumer Privacy Act or related data breach notification laws, for the unauthorized disclosure of personal information in response to a consumer request under the California Consumer Privacy Act or any implementing regulation.

(6) A business that has undertaken reasonable efforts to utilize one or more of the procedures specified under subsection 2 or 3 of this section, or an equivalent procedure, to verify the identity of a consumer (or authorized person on the consumer's behalf) but has been unable to determine, within 45 days of receiving the request, that the request is a verifiable consumer request, shall not be required to provide information to the consumer or other requester pursuant to any section of the California Consumer Privacy Act or any implementing regulation.

(7) For purposes of Section 1798.130(a)(2)'s requirement that a business deliver required information to a consumer in a "readily usable format that allows the consumer to transmit this information from one entity to another entity without hindrance," the term "readily usable" shall include any structured, commonly used and machine-readable format, at the business' discretion. Examples include, but are not limited to, .csv, .pdf and JSON files.

Proposed Regulations – Verifiable Consumer Request – Timing

Any obligation of a business imposed by the California Consumer Privacy Act to respond to a consumer request for access, deletion, or opt-out of the sale of the consumer's personal information, either by the consumer or by an authorized person on the consumer's behalf, shall apply only after the adoption and effective date of final regulations that specify the acceptable methods and procedures for a business to determine that a request received from a consumer (or authorized person on the consumer's behalf) is a "verifiable consumer request."

Proposed Regulations – Effective Date of AG Regulations and Enforcement

(a) These regulations implementing the California Consumer Privacy Act shall take effect and compliance shall be required no later than six months after publication of final regulations.

(b) The Attorney General may bring an enforcement action under the California Consumer Privacy Act and these regulations at any time starting six months after publication of final regulations, but no sooner than 30 days after the business receives notification from the Attorney General describing the business's alleged noncompliance.

From:	Amy Zajac-Hamerton
To:	Privacy Regulations
Subject:	Comments on CCPA From Genentech, Inc
Date:	Friday, March 08, 2019 3:58:26 PM
Attachments:	Genentech_Comment_Letter_March_8_2019.pdf

To Whom it May Concern:

Genentech is submitting the attached comments in regards to the California Consumer Privacy Act (CCPA) of 2018. Should you have any questions or need additional information from Genentech, my contact information is below.

May I please request confirmation of this email. Thank You.

Amy Zajac
State Government Affairs
[redacted]

Genentech
A Member of the Roche Group

Genentech
A Member of the Roche Group

March 8, 2019

LEGAL DEPARTMENT

By Email to: PrivacyRegulations@doj.ca.gov

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

Re: Genentech CCPA Implementation Proposals

Dear Attorney General Becerra:

Genentech, Inc. ("Genentech")[1] submits these comments in furtherance of your office's broad rulemaking authority under the California Consumer Privacy Act ("CCPA").[2] This letter identifies Genentech's priority concerns with certain ambiguous, unclear, incomplete, or overbroad language found in the CCPA and presents preliminary rulemaking recommendations to address those concerns.

Genentech and similarly situated life science companies play a critical role in advancing healthcare in California and throughout the world.[3] Collectively, Genentech and other Roche group companies employ over 13,000 Californians in 10 facilities throughout the state.[4] We strive to enhance personalized patient care and access to innovative medicines through our work, and have a strong commitment to advancing science and improving public health globally. The work of our scientists, clinicians, and other employees encompasses innovative basic and clinical research, biopharmaceutical medicine development and manufacturing, and programs to increase patient access to appropriate medicines and services.

Our primary concerns with the CCPA have to do with its general applicability to biotechnology and life science companies, like Genentech, which currently follow many rigorous privacy laws[5] that do not impact businesses in other industries. Genentech and other biotechnology companies already must commit significant resources, including the implementation of systems, policies and safeguards to ensure that personal data is responsibly protected, and in a compliant manner. In other words, biotechnology companies *already* engage in advanced data protection practices.

---

[1] All references to "Genentech" in this letter refer to Genentech, Inc., with headquarters in South San Francisco, a member of the Roche group of companies, and the California based, United States affiliate of F. Hoffman-La Roche, Ltd.

[2] California Civil Code §§ 1798.185(a) and (b).

[3] The Roche group of companies is active in over 100 countries worldwide.

[4] Figures reported as of February 21, 2019, and reflect Roche group numbers for California.

[5] Existing privacy laws include HIPAA (Health Insurance Portability and Accountability Act of 1996), the CMIA (California's Confidentiality of Medical Information Act), and similar international privacy requirements, including the GDPR (General Data Protection Regulation) in Europe.

GENENTECH, INC. 1 DNA WAY, SOUTH SAN FRANCISCO, CA 94080-4990 USA
Phone [redacted] *Fax* [redacted] *www.gene.com*

Although Genentech understands the importance of privacy guidance for business use of personal data, it will be extremely challenging, absent clarifying regulations, to harmonize the CCPA requirements with other privacy law requirements. Further, as applied to Genentech and similar companies, we believe the CCPA will provide only marginal additional privacy benefit to individuals, and at the expense of unduly burdening companies engaged in critical healthcare related efforts on which Californians and people around the world depend. Consequently, as an overarching principle, we respectfully propose that wherever possible, the Attorney General seek to harmonize CCPA implementation with existing laws, including HIPAA and the GDPR.

We recognize that the CCPA, as amended, includes certain exemptions for data with a nexus to healthcare. Such carve-outs include an exemption for information that is already regulated by HIPAA or the CMIA, as well as information collected as part of a clinical trial. We believe these exemptions reflect two general principles. First, the California legislature recognizes that the CCPA need not regulate data that is already protected under other regulatory regimes. Second, the legislature appreciates that the critical societal benefit that flows from the collection and use of certain data, including information collected as part of a medical clinical trial, may in certain circumstances outweigh an individual's right to fully control what happens with that data.[6]

However, as detailed in this letter, we have identified certain CCPA language that requires clarification to ensure that this apparent legislative intent is honored. For example, the CCPA's HIPAA exemption extends to certain data collected by HIPAA "covered entities" and "business associates," designations that in most cases do not apply to Genentech.[7] As a practical matter, HIPAA covered entities often transmit coded health information to Genentech as authorized under applicable law and upon obtaining patient consent and authorization. Such data is typically labeled with a specific code and does not carry any personal identifiers. The providing party is responsible for maintaining the coding key. This coding is the current standard used in clinical research, including observational studies, and offers additional privacy safeguards to the individual. Before any sharing of such received information, it is further de-identified by Genentech in accordance with applicable privacy laws[8] so that associating the data with any particular individual is unfeasible. Regardless of such de-identification, Genentech securely handles the information in a lawful and appropriate manner, including through systems and processes, such as encryption, system security, internal access restrictions, and other safeguarding protocols. Although Genentech holds this information in compliance with existing applicable privacy laws and standards, the information is not clearly exempt from the CCPA.

---

[6] California Civil Code § 1798.145(c)(1)(C). Under HIPAA, information collected for treatment, payment, or health care operations may generally be de-identified (in accordance with specified standards) and used for secondary purposes without a patient authorization, including research. Additionally, the EU Data Protection Board opined that the use of data for secondary research is legitimate under the GDPR so long as companies implement appropriate safeguards such that a new legal basis need not be established.

[7] Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in certain transactions. Business Associate is a person or entity who, on behalf of a covered entity, performs or assists in performance of a function or activity involving the use or disclosure of individually identifiable health information.[8] HIPAA, the CMIA , or the GDPR, as applicable.

[8] HIPAA, the CMIA , or the GDPR, as applicable.

LEGAL DEPARTMENT, 1 DNA WAY, SOUTH SAN FRANCISCO, CA 94080-4990 USA
Phone [redacted] Fax [redacted] www.gene.com

We are concerned that, as enacted, the CCPA could create unintended barriers to scientific, healthcare related work in the public interest and inhibit otherwise appropriate use of health information to advance science and medicine and enable patient access to necessary treatments. We therefore propose the following recommendations for your consideration, which we believe are within the Attorney General's rulemaking authority, are consistent with legislative intent, and address our identified issues.

I. Priority Issues and Proposed Resolutions.

1. Clinical Trial Exemption and Related Research

Clinical trial research is a central component of Genentech's operations. As of January 2019, Genentech and other Roche group companies have conducted 773 trials involving nearly 35,000 patients in over 3,000 locations across California. As amended, the CCPA exemption for collected clinical trial data remains ambiguous regarding what research standards must be followed to qualify for the exemption.[9] We request that regulations state "clinical trial data is exempt if the research is conducted pursuant to *any* of: (a) the federal Common Rule, [10] (b) the ICH GCP standards, [11] *or* (c) FDA human subject protection standards"[12].

In addition, we propose a regulatory safe harbor for other clinical or human subject research that satisfies *any* of the following, so long as study data is protected under current privacy standards (e.g. coding, pseudonymization, anonymization or de-identification): [13] (d) if approved or granted waiver by an independent review board ("IRB") or is exempt from such IRB approval, (e) if approved or granted waiver by an ethics committee, *or* (f) if conducted pursuant to Good Pharmacoepidemiological Practices, or other accepted industry practice guidelines.

Further, we suggest clarifying that information collected "as part of" a clinical trial includes "any information collected or created (including, without limitation, biospecimens, biometrics, and images), that reasonably relates to, or in any way furthers the purpose of, the conduct of any present or prior qualifying clinical trial or clinical or human subject research."

We propose the above clarifications in the rulemaking process for the following reasons. First, certain CCPA commenters have suggested that the clinical trial exemption language could be interpreted to exempt clinical trial data *only if* it is subject to the federal "Common Rule" (along with other standards), an interpretation that may fail to exempt important privately funded research that is subject to other existing data privacy standards and research controls.

Second, we recommend a regulatory safe harbor for other healthcare-related research and development by private businesses, including research performed *outside* the clinical trial

---

[9] See California Civil Code § 1798.145(c)(1)(C).
[10] Title 45 of the Code of Federal Regulations Part 46.
[11] International Council for Harmonisation Good Clinical Practice guidelines.
[12] United States Food and Drug Administration human subject protection requirements (Title 21 of the Code of Federal Regulations Parts 50 and 56 .
[13] Current privacy standards under HIPAA, the CMIA , and the GDPR.

LEGAL DEPARTMENT, 1 DNA WAY, SOUTH SAN FRANCISCO, CA 94080-4990 USA
Phone [redacted] Fax [redacted] www.gene.com

context, to acknowledge the public health benefits that flow from such research. We request that these research methods be deemed compliant with the CCPA when conducted in accordance with current applicable privacy laws and recognized industry practice guidelines.[14] Although companies generate such research data outside of clinical trials, the research and resulting data promote similar public health benefits, potentially inviting insights and breakthroughs that may otherwise elude alternative research techniques.[15] This research safe harbor would be consistent with the legislature's apparent intent in establishing the clinical trials exemption, by creating a safe harbor for other types of healthcare research conducted in accordance with other recognized research guidelines and standards,[16] and with resulting data protected under current privacy standards, such as de-identification, anonymization, and pseudonymization.[17]

Finally, we note that the CCPA clinical trial exemption does not define or otherwise clarify the phrase "as part of." For example, we are uncertain whether certain secondary research data is exempt under the CCPA, when a company previously collected the data used for such secondary research "as part of" a prior clinical trial in accordance with current applicable laws. Similar questions arise regarding repository biological samples which are not used contemporaneously with a given clinical trial. For those reasons, we recommend the clarifying regulation discussed above.

2. "Consumer" Definition

Although the CCPA applies to California "consumers," this definition is not limited to consumers *in the traditional sense*. Instead, the law broadly defines the term as any "natural person who is a California resident . . .however identified."[18] We propose that regulations clarify this definition to mean "a California resident who uses a product or service *in a personal capacity*." Additionally, we propose that implementing regulations exclude from the "consumer" definition any individuals acting in their capacity as employees, service providers, professionals, or *any other representatives* whose engagement with a business derives from a business-to-business relationship.

As enacted, certain business representatives with whom a company engages are likely considered "consumers" under present CCPA language, including representatives of vendors, healthcare providers, and health plans. Without clarification, it is unclear how a company like Genentech

---

[14] Such research, which is often performed by private parties, involves the collection of medical information where consistent with informed consent, including, without limitation, patient reported data, information gathered from monitoring devices, and electronic health records.

[15] For example, outside research may involve software and the utilization of machine learning in attempting to identify patterns and insights that may otherwise be unidentifiable. The research may also reduce the need for interventional trials and provide significant benefits such as answering research questions, helping with clinical trial design, supporting drug product label expansion, informing payer questions, supporting post-marketing follow-up, and improving knowledge of disease, biology, and individual health.

[16] Examples include, without limitation, IRB review or exemption, Good Pharmacoepidemiology Practices, EMA Good Pharmacovigilance Practices Guidelines, and National Institutes of Health guidelines.

[17] Current privacy standards under HIPAA, the CMIA, and the GDPR.

[18] California Civil Code § 1798.140(g)(emphasis added).

LEGAL DEPARTMENT, 1 DNA WAY, SOUTH SAN FRANCISCO, CA 94080-4990 USA
Phone [redacted] Fax [redacted] www.gene.com

would comply with the CCPA in the case of an employee, vendor representative, or individual healthcare provider who is *also* the company's end-consumer in the traditional sense. In this situation, fulfilling a CCPA request to *delete* information may have unintended consequences. For example, a healthcare provider may invoke CCPA consumer rights to request deletion of his or her personal health information such as diagnosis or test results, and CCPA compliance may require removing all such information on record for the healthcare provider's business entity (potentially including information of more than one individual). For these reasons, we recommend that regulations clarify the definition of "consumer."

3. "Personal Information" Definition

CCPA's broad definition of "personal information" includes 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.* [19] This definition includes identifiers which, taken together, create a more expansive and ambiguous standard than other privacy laws, and may relate to more than one individual.

Consistent with existing privacy laws, we propose that regulations clarify the definition of "personal information" and any identifiers to be specific to a *single individual*, as follows (a) the phrase "a particular consumer or household" refer to an identifiable individual residing at a specific California postal address, excluding any spouse, dependents or others, regardless of household affiliation, and (b) an identifiable consumer be someone identified by name or specific identifiers *by the business collecting such information*, without requiring additional investigational efforts. Also, we propose a regulatory safe harbor clarifying that companies are *not* required to link or re-identify consumer data to satisfy CCPA requirements [20] when following current privacy and data protection standards of de-identification, anonymization, or pseudonymization of personal information, as authorized under applicable laws, [21] and that such privacy standards be recognized as satisfying privacy protection of personal information for CCPA compliance.

Genentech in many circumstances has no way to verify a unique individual based on IP addresses or device IDs, or based on coded (or pseudonymized) information, without receiving other personal information or being required to "re-link" information that had previously been un-linked (or never received) to protect an individual's privacy. Regulatory clarification is needed so that investigative efforts of this type, which are contrary to current privacy practices, are not required to comply with CCPA.

---

[19] California Civil Code § 1798.140(o)(1)(emphasis added).

[20] In making this point, we acknowledge one CCPA exemption indicating that businesses need not "link information" under certain circumstances; however, without further guidance, it is unclear how a company could qualify for this exemption. See California Civil Code § 1798.145(i).

[21] HIPAA, the CMIA , or the GDPR, as applicable.

LEGAL DEPARTMENT, 1 DNA WAY, SOUTH SAN FRANCISCO, CA 94080-4990 USA
Phone [redacted] Fax [redacted] www.gene.com

We also note that responding to certain CCPA "personal information" requests, such as deleting or disclosing certain information, may necessitate that Genentech re-identify an individual and link data when an individual would otherwise remain unidentified following current privacy standards. In practice, extracting a single individual's data *from coded or de-identified datasets* is often not practical, in many instances not readily possible, and could stifle important research objectives.[22] Any of the foregoing circumstances would likely involve the unintended collection or use by Genentech of more identifiable information than would have been necessary absent the consumer request, resulting in a net loss in privacy to the individual.

4. "Sale" Definition

The CCPA broadly defines "sell, selling, sale, or sold" to include selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating personal information to another business or third party for monetary *or other valuable consideration.*[23] As written, this definition implicates several activities beyond mere "sales" in the traditional sense. Further, the CCPA requires that any covered business that "sells" personal information to third parties must provide notice to consumers of such sales, and CCPA consumers have the right to "opt-out" of those sales.

We propose that implementing regulations state that "valuable consideration" means the exchange of data for cash or direct commercial gain, and specifically excludes *any transaction for research or development purposes* that makes available, exchanges, or transfers data (whether or not for limited periods and subject in all cases to applicable existing privacy protection standards for data sharing), even where valuable consideration may be provided in such transaction. This clarification in the regulations is necessary to give assurance that biopharmaceutical and life science companies are permitted under to continue to use privacy-protected data to combine with or link to other data and be used for research purposes, to advance science and public health, or for analysis, development, and commercialization of products to treat and diagnose disease.

"Sale" language should align closely with general consumer understanding, so that consumers fully understand the consequences of their "opt-out" decisions. We also recommend permitting biopharmaceutical companies to explain the various types of sales and allow consumers the choice to opt-out of any *portion* of these types of sales, depending upon indicated business use.

There are several reasons prompting these recommendations. For example, we believe it is critical to allow consumers to designate the sale types for any CCPA opt-out requirement. This is

---

[22] *Illustrative Example:* Genentech continuously conducts retrospective analyses on de-identified patients to understand, for example, optimal treatment patterns and points of intervention to optimize patient outcomes and experience. The CCPA's application may result in the need to "semi-identify" the data, to remove California residents, which would disrupt Genentech's work analyzing large de-identified datasets across a comprehensive sample set, despite underlying intentions of advancing patient care. Such data removal might also inadvertently introduce bias or otherwise distort research results.

[23] California Civil Code § 1798.140(t).

LEGAL DEPARTMENT, 1 DNA WAY, SOUTH SAN FRANCISCO, CA 94080-4990 USA
Phone [redacted] Fax [redacted] www.gene.com

because Genentech offers individuals the opportunity to opt-in and consent to use of their information in order to receive a variety of benefits and services, such as nurse telephone calls and medication access services. Without clarification of the CCPA "opt-out" requirement, an individual's opt-out decision could unintentionally terminate these important services. Genentech also engages third parties to provide coupons, co-pay cards, medical education, and medication adherence programs, each of which require individual information disclosures to third parties that could feasibly fall under the definition of "sale." Without implementing our recommendations regarding the "sale" definition and individual choice for a partial "opt-out," a consumer's opt-out request may unintentionally impede these critical data sharing practices.

Further, Genentech's third party data sharing practices are critical to improving research and personalized patient care. Examples of such arrangements include global data collaboration among researchers,[24] the transfer of patient tissue in connection with individualized cancer treatments,[25] and data purchased from genomics companies to further research initiatives.

II. Additional CCPA Concerns.

In addition to the above described priority issues, Genentech notes the following additional issues with the CCPA that we believe warrant rulemaking consideration:

1. Look-Back Time Periods and Implications. A shortened compliance timeline exacerbates the resource intensive challenges associated with data protection compliance, particularly as businesses await implementing regulations and other guidance. We are particularly concerned regarding whether the 12-month lookback period might cause the CCPA compliance period to begin prematurely. We propose that businesses be given no less than 9 months to bring their organization into

---

[24] *Illustrative Example:* One Company policy requires sharing individual level clinical trial data with other researchers to use for their legitimate research questions under a research plan and under appropriate and compliant data protection conditions. Such sharing may occur on an international scale. The relevant data sharing agreement restricts using data beyond the researcher's identified research plan, restricts the sharing of that data with others, and prohibits attempts to re-identify data subjects. Additionally, the researcher is requested to publish findings, which could serve to further additional research on similar issues, ultimately bestowing a supreme benefit to public health. Under the CCPA, this type of research sharing could be considered a "sale," triggering several data rights for data subjects. Because Genentech does not receive direct identifiers, however, the company has no way of knowing the identity of individuals to be able to comply with the CCPA without further identification efforts. The administrative cost and effort to track the research use of an individual's data could cause the company to restrict or discontinue such broad clinical trial sharing programs, despite intentions to advance science, medicine, and public health globally.

[25] *Illustrative Example:* One innovative Genentech program creates individualized treatments for cancer patients. This requires the transfer of patient tissue to a healthcare provider and then to a Genentech partner, which sequences the patient's DNA. The resulting DNA sequencing data must be transferred once more for analysis. The results of that analysis are then transferred back to Genentech and used to manufacture the individualized treatment, as well as for additional research and improvements to the treatment. It is unclear whether any of these transfers would constitute a "sale" under the CCPA. In the process of analyzing this information and creating data, some or all of these partners would likely use the data to improve their own processes and capabilities, which may or may not constitute "valuable consideration" under the CCPA. This lack of clarity could negatively impact the creation and improvement of important medicines that treat unmet medical needs.

LEGAL DEPARTMENT, 1 DNA WAY, SOUTH SAN FRANCISCO, CA 94080-4990 USA
Phone [redacted] Fax [redacted] www.gene.com

compliance after final regulations are published, and that the CCPA should apply only to personal information collected or disclosed after the effective date of the law.

2. "Homepage" Definition. The CCPA defines "homepage" to include the introductory page of a website, but also potentially *any* web page "where personal information is collected." Genentech recommends clarifying that the definition's "introductory page" language applies to the "homepage" definition universally, rather than imposing certain CCPA homepage requirements for *any* web page where personal information is collected.

3. Data Security Program Safe Harbor. The CCPA's consumer private right of action enforcement mechanism should include a safe harbor for businesses that have implemented a data security program that is reasonable and consistent with recognized industry standards.

Genentech remains committed to collecting and using personal data in a lawful, fair, and responsible manner. We are also committed to advancing the public's interest in science and medicine and access to healthcare, which increasingly depends on the collection and use of personalized healthcare data. We are therefore grateful for your efforts in soliciting public input early in the rulemaking process. We would be happy to meet or discuss the contents of this letter at your convenience, to follow up with specific language proposals to address our concerns, and, if welcome, to work with your staff on regulation wording.

Very truly yours,

GENENTECH, INC.

Sean Johnston

Sean A. Johnston
Senior Vice President
General Counsel and Chief Compliance Officer

cc: Ms. Amy Zajac
Genentech Government Affairs
Phone: [redacted]

LEGAL DEPARTMENT, 1 DNA WAY, SOUTH SAN FRANCISCO, CA 94080-4990 USA
Phone [redacted] *Fax* [redacted] *www.gene.com*