



December 6, 2019

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

Dear Attorney General Becerra,

The protection of the free press is enshrined in the First Amendment to the U.S. Constitution. More than 120 million adults read a daily or Sunday print newspaper. The free press is on the front lines helping the American people hold accountable those who hold positions of power within our democracy and around the world. Digital advertising is a significant source of revenue to media outlets, large and small, and helps keep the press free from government control and affordable. With a well-designed privacy law, the press can continue to do its job as intended in the U.S. Constitution, and consumers can continue to have access to cost-efficient news sources and control of the use and exchange of their personal information.

The News Media Alliance (the “Alliance”) represents over 2,000 media outlets and is composed of nationally recognized organizations, international organizations, and hyperlocal organizations. The Attorney General’s proposed Regulations promulgated pursuant to the California Consumer Privacy Act (“CCPA”), while helpful on a number of levels, impose certain additional burdens on publishers that will render compliance difficult and provide no added benefit to consumers. Indeed, the Regulations may further confuse and convolute consumer control over personal information.

The Alliance believes in giving consumers more transparency and control regarding the use and collection of personal data. In an effort to be more fully compliant with the CCPA and the Regulations and to protect consumer personal information, the Alliance, joined by the California Newspaper Publishers Association, respectfully submits the following comments.

I. The Attorney General Should Clarify the New “Notice at Collection” Requirement.

Section 999.305 imposes new obligations on businesses to make additional disclosures above and beyond the privacy policy when collecting personal information. These new obligations are unclear with respect to what needs to be disclosed, and how, where, and when the notice should be appear.

A. The Attorney General Should Not Require the Posting of a “Notice at Collection” Until January 1, 2021.

The “notice at collection” is a new obligation set forth in the Regulations that is not required by the statute. While the CCPA goes into effect January 1, 2020, the anticipated effective date for the Regulations is sometime before July 1, 2020. The notice at collection obligations were revealed less than three months before the law’s effective date, and they are ambiguous and need clarification.

Because the notice at collection is a new obligation and consumers are likely to see inconsistent implementations that only create confusion, rather than transparency, the Attorney General should clarify that the notice at collection obligation is not effective until January 1, 2021.

B. The Attorney General Should Clarify the Required Placement of the “Notice at Collection.”

The Regulations provide:

The notice [at collection] shall “use a format that draws the consumer’s attention to the notice and makes the notice readable, including on smaller screens, if applicable.”¹

Because this is a new obligation and because other requirements such as the “Do Not Sell My Personal Information” button more clearly indicate where and how they should be presented to the consumer, it is difficult for businesses to understand, operationally, how the “notice at collection” should appear and where it should be placed. To remain consistent with existing consumer expectations, the Attorney General should permit businesses to use a link that conspicuously alerts California consumers of the notice on the homepage by being in close proximity to the existing privacy policy link in the website footer or mobile app menu.

C. The Attorney General Should Eliminate Inconsistent Language Regarding the Point in Time When Consumers Must See the “Notice at Collection.”

The Regulations provide:

The notice [at collection] shall...Be visible or accessible where consumers will see it before any personal information is collected.²

This subdivision is inconsistent with the statute³ and even other portions of the Regulations⁴ that permit disclosures regarding privacy practices to happen **at or before** the time of collection.

¹ 11 CCR §999.305(a)(2)(b).

² 11 CCR §999.305(a)(2)(e).

³ CIV. CODE §1798.100(b). “A business that collects a consumer’s personal information shall, *at or before* the point of collection, inform consumers as to the categories of personal

The Attorney General should revise §999.305(a)(2)(e) to be consistent with the CCPA and the other language in the Regulations and provide that the “notice at collection” can be provided **at or before** the time of collection.

II. The Attorney General Should Provide Further Clarification on How to Properly Post the Notice at Collection, Privacy Policy, and “Do Not Sell My Personal Information” Links on Mobile Applications.

The Regulations provide that the notice at collection,⁵ the privacy policy,⁶ and the “Do Not Sell My Personal Information”⁷ links must be conspicuously posted on the mobile application’s download or landing page.

From an operational standpoint, this is problematic because many mobile applications do not have footers, as is the case with actual websites viewed on a device. Often times, the links to the privacy policy and other applicable notices are found in a hamburger menu or gearbox, which consumers have come to associate with being a location for important additional information.

The Alliance requests that the Attorney General clarify that posting the notice at collection, the privacy policy, and the “Do Not Sell My Personal Information” links in the application’s hamburger menu or gearbox will be deemed conspicuous for purposes of by the Regulations.

information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.” (*emphasis added*).

⁴ 11 CCR §999.301(i). “‘Notice at Collection’ means the notice given by a business to a consumer *at or before* the time a business collects personal information from the consumer as required by Civil Code section 1798.100(b) and specified in these regulations.” (*emphasis added*). *See also* 11 CCR §999.305(a)(5) (“If a business does not give the notice at collection to the consumer *at or before* the collection of their personal information, the business shall not collect personal information from the consumer”) (*emphasis added*).

⁵ 11 CCR §999.305(a)(2)(e). “The notice shall...[b]e visible or accessible where consumers will see it before any personal information is collected. For example, when a business collects consumers’ personal information online, it may conspicuously post a link to the notice on the business’s website homepage or the mobile application’s download page, or on all webpages where personal information is collected.”

⁶ 11 CCR §999.308(a)(3). “The privacy policy shall be posted online through a conspicuous link using the word ‘privacy,’ on the business’s website homepage or on the download or landing page of a mobile application.”

⁷ 11 CCR §999.315(a). “A business shall provide two or more designated methods for submitting requests to opt-out, including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled ‘Do Not Sell My Personal Information,’ or ‘Do Not Sell My Info,’ on the business’s website or mobile application.”

III. The Attorney General Should Not Require a Notice of Right to Opt-Out of Sale of Personal Information for Businesses Not Currently Selling Personal Information.

The Regulations provide:

The purpose of the notice of right to opt-out of sale of personal information is to inform consumers of their right to direct a business that sells (*or may in the future sell*) their personal information to stop selling their personal information, and to refrain from doing so in the future.⁸

The emphasized portion of this subdivision implies that even businesses that do not currently sell personal information, but may possibly sell personal information in the future, are also required to provide a notice of right to opt-out of sale of personal information. This is inconsistent with the CCPA itself,⁹ which only requires businesses that are currently selling personal information to provide the notice of opt-out of sale of personal information.

The Alliance strongly recommends the Attorney General remove “or may in the future sell” from §999.306(a)(1) of the Regulations in order to avoid consumer confusion. The purpose of the CCPA is to provide transparency with respect to company practices regarding the collection, use, and disclosure of consumer personal information. If any business that does not currently sell personal information but that might theoretically sell personal information in the future is required to provide an opt-out notice, a consumer will never be sure, from the moment that consumer visits a website or sees the notice in a store, whether or not a site is selling personal information.

IV. The Regulations Should Not Require Businesses to Treat Unverified Requests to Delete as Requests to Opt-Out of Sale of Personal Information.

The Regulations provide:

For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified and shall instead treat the request as a request to opt-out of sale.¹⁰

⁸ 11 CCR §999.306(a)(1) (*emphasis added*).

⁹ CIV. CODE §1798.120(b). “A business that sells consumers’ personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the ‘right to opt-out’ of the sale of their personal information.”

¹⁰ 11 CCR §999.313(d)(1)

This new requirement (not found in the statute) to treat an unverified request to delete as a request to opt-out of sale is problematic on multiple levels, most obviously in situations where a business is not selling personal information in the first place, and in situations where the business does not have sufficient information to identify the consumer. There is also a major concern that businesses will be flooded with unverified deletion requests by simply taking names from a telephone book and inputting them into the request for deletion form, or by using an automated bot. The Attorney General should eliminate this requirement.

V. The Attorney General Should Support the Development of Industry Frameworks for a Consistent Opt-Out Approach Under the CCPA And Provide Time for Organizations to Implement Those Frameworks.

Many members of the Alliance are hyperlocal news organizations that cannot afford to build their own opt-out solutions for the CCPA. These businesses welcome the efforts of self-regulatory groups that have been working, across the advertising ecosystem, to develop proposed frameworks to support and facilitate consumer opt-out rights.¹¹ The Attorney General should support these industry efforts and provide additional time for organizations that choose to participate therein to implement those technical specifications.

The BEAR Study included in the Attorney General’s Initial Statement of Reasons points out that the costs associated with developing technological systems to meet the compliance standards of the CCPA are likely to be significant. Even the largest data owners in the world are struggling to figure out how to make the “Do Not Sell My Personal Information” button operational on their platforms, with no long-term viable solution in sight.

Members of the Alliance and others in the advertising ecosystem are engaged in a significant good-faith effort to comply with the CCPA. Given this new legal regime, and the challenges of implementing the opt-out requirements in the ad tech space, the Alliance asks the Attorney General to set forth a compliance grace period for such implementation, up to and including January 1, 2021.

VI. The Attorney General Should Not Restrict a Service Provider’s Ability to Use Information Collected from One Business to Benefit Another Business.

The Regulations provide:

A service provider shall not use personal information received either from a person or entity it services or from a consumer’s direct interaction with the service provider for the purpose of providing service to another person or entity.¹²

¹¹ See, e.g., *IAB CCPA Compliance Framework for Publishers and Technology Companies* (available at <https://www.iab.com/guidelines/ccpa-framework/>).

¹² 11 CCR §999.314(c).

This provision would have severe negative implications for publishers' ability to use any service provider that provides analytic services. Many technology service providers use a single piece of information such as an IP address, received from multiple businesses, to provide services to many different businesses. For example, frequency capping or sequencing functions are extremely helpful to consumers because they limit the number of times consumers see the same ad. Service providers are only able to bring this benefit to consumers if they are able to take information they receive from several businesses and use that information collectively. Another example is Google Analytics. Google Analytics provides a service that allows businesses to track consumer traffic on their websites and mobile applications. It provides insight as to how consumers landed on their website, what consumers did once they were on the website, and how long they stayed on the website. Google Analytics uses all this information from various businesses to provide businesses with online marketing plans that allow them to track and gauge their return on investment in a meaningful way when the Advertising Feature is turned on.

The Alliance recommends the following revised provision:

A service provider shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose of providing services to another person or entity, **unless the service provider is using the information solely for business purposes and provided those business purposes are disclosed to consumers when responding to requests to know.**

VII. Businesses that Honor Opt-Out Requests Through a "Do Not Sell My Personal Information" Link Should Not Also be Required to Treat the Ad Hoc Use of User-Enabled Privacy Controls as "Do Not Sell" Requests.

The Regulations provide:

If a business collects personal information from consumers online, the business shall treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.¹³

Given the existing requirement that businesses selling personal information include a "Do Not Sell My Personal Information" button on the homepage with direct access to methods to opt-out of the sale of personal information, adding user-enabled privacy controls as another method only exacerbates the complexity facing consumers as they seek to opt-out of sale of personal information. Without a clear delineation between an opt-out of sale and existing user-enabled privacy controls, a consumer may feel he or she must enable and disable privacy-setting controls prior to and after each visit to any number of websites through which he or she does want to

¹³ 11 CCR §999.315(c).

allow the businesses to sell their personal information. This is not the experience consumers want and it does not provide further transparency or control.

Further, under the Regulations as drafted, a business will not know how to reconcile a consumer's use of user-enabled privacy controls with a consumer's action or inaction vis-a-vis a "Do Not Sell" button. In addition, in this scenario, a business has no way to contact a consumer to confirm that it contacted all third parties to which it sold data in the previous 90 days.¹⁴ And if a consumer uses specific user-enabled controls, rather than a global opt-out, a business has no mechanism for contacting the consumer to provide the option to globally opt-out.¹⁵

Additionally, there are currently no standards for "Do Not Track" or other possible browser plug-ins. Requiring publishers to follow various standards created every day is an impossible burden with which small and large publishers will not be able to comply, but which unfairly enhances the power of browser manufacturers.

The Alliance recommends that the Attorney General remove the references to user-enabled privacy controls from the Regulations as they are unnecessary, provide no additional transparency for consumers, and impose undue burdens on businesses.

VIII. The 90-Day Lookback Requirement Exceeds the Scope of the Attorney General's Rulemaking Authority and Should be Eliminated.

The Regulations provide:

A business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the consumer's request that the consumer has exercised their right to opt-out and instruct them not to further sell the information. The business shall notify the consumer when this has been completed.

This proposed regulation is problematic for two reasons. First, it would require retroactive application to information collected up to 90 days before the effective date of the CCPA. Second, it would also require retroactive application generally of the do not sell obligation and thereby exceed the scope of the Attorney General's power to regulate. "New statutes are presumed to operate only prospectively absent some clear indication that the Legislature intended otherwise." *Elsner v. Uveges*, 34 Cal. 4th 915, 936 (2004). Here, there is no clear indication that the Legislature intended the do not sell obligation to apply retroactively. Moreover, the statute only requires a prospective obligation on businesses that honor do not sell requests.¹⁶

¹⁴ 11 CCR §999.315(f).

¹⁵ 11 CCR §999.315(d).

¹⁶ CIV. CODE 1798.135(a)(4) and (5). "For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer...[and] respect the consumer's decision to opt-out for at least 12

In order to avoid any retroactive application of the CCPA, the 90-day lookback should be eliminated.

IX. Businesses Should Have 45 Days from the Date a Request to Know or a Request to Delete is Verified to Fulfill or Deny that Request.

The Regulations provide:

Businesses shall respond to requests to know and requests to delete within 45 days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request.¹⁷

There are a number of verification requirements that must be followed for both requests to know and requests to delete. Because of the extensive nature of these requirements, it is clear that each request will need to be verified on a case-by-case basis.¹⁸

The Alliance recommends that the Regulations be revised such that the 45-day window to substantively respond to requests to delete and requests to know begins to run on the day the request is verified.

X. The Attorney General Should Not Require Publication of Metrics in the Privacy Policy for Businesses That Are Required to Maintain Consumer Request Metrics.

The Attorney General has proposed explicit metrics reporting requirements for businesses “that alone or in combination, annually buy[], receive[] for the business’s commercial purposes, sell[], or share[] for commercial purposes, the personal information of 4,000,000 or more consumers.”¹⁹

While the record-keeping requirements are sensible, publication of such metrics is more likely to confuse consumers, particularly if businesses are denying large volumes of frivolous or even fraudulent requests. The numbers themselves will not elucidate for consumers the underlying reasons for the denial, and will only further extend the length of already lengthy privacy policies.

The Alliance would strongly recommend that the Attorney General strike Section 999.317(g)(2) from the Regulations to remove the obligation to post the metrics publicly, and instead require that businesses in this category maintain such records internally and make them available to the Attorney General upon request.

months before requesting that the consumer authorize the sale of the consumer’s personal information.”

¹⁷ 11 CCR §999.313(b).

¹⁸ See generally 11 CCR §§ 999.323-999.326.

¹⁹ 11 CCR §999.317(g).

XI. The Attorney General Should Provide Clarity on How Businesses Should Operationalize the Obligation to Provide Aggregated Household Data in Response to Household Requests for Personal Information.

The Regulations provide:

Where a consumer does not have a password-protected account with a business, a business may respond to a request to know or request to delete as it pertains to household personal information by providing aggregate household information, subject to verification requirements set forth in Article 4.²⁰

The average household size is 2.6 people.²¹ It is unclear how any business could provide household information on an aggregated basis for 2.6 people. It is fundamentally inconsistent with the language and the spirit of the CCPA.

In addition, it is unclear whether “household” means any household in the United States or if it is restricted to requests that come from households located in California.

As numerous businesses have pointed out to the legislature and to the Attorney General, allowing one member of a household to obtain information about other individuals in the household – even in “aggregated” form – actually puts the privacy and safety of those household members at risk. The Attorney General should remove subsection (a) and instead require that all consumers of a household jointly request information (as provided in subsection (b)). In the alternative, if the Attorney General is not inclined to remove subsection (a), the Alliance strongly encourages the Attorney General to provide businesses who comply with subsection (a) a safe harbor in the event of a data breach regarding such household information.

The Attorney General should also make clear that this provision of the Regulations is intended to include only those requests received from households located in California.

XII. The Attorney General Should Provide Additional Guidance on the Two Steps Required for Opt-In for Minors, Opting-In After Opting-Out, and Requests to Delete.

The Regulations provide:

For consumers 13 years and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.²²

²⁰ 11 CCR §999.318(a).

²¹ Pew Research on the Increase in Household Size available at <https://www.pewresearch.org/fact-tank/2019/10/01/the-number-of-people-in-the-average-u-s-household-is-going-up-for-the-first-time-in-over-160-years/>

²² 11 CCR §999.301(a).

A business shall use a two-step process for online requests to delete where the consumer must first, clearly submit the request to delete and then second, separately confirm that they want their personal information deleted.²³

Requests to opt-in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.²⁴

This is a new obligation that does not appear in the statute and it lacks substantial compliance guidance. The Attorney General should use this opportunity to provide, at a minimum, examples of sufficient two-step opt-ins. The Alliance provides the following examples of what might be sufficient for purposes of two-step verification:

Example 1: If a business is responding to a verified request to delete via the toll-free number method, the business may ask the consumer to provide an email address. The business will then send a confirmation email to that account for the consumer to confirm they would like their personal information deleted.

Example 2: If a business receives an opt-in request from a minor between 13 and 16 years old via a webform, the business may give the minor an email with a deep link to click onto verify that they would like to opt-in to the sale of personal information.

Example 3: If a business receives a request to opt-in after opting-out via a webform, the business may give the consumer two separate screens – first filling out a request on a webform, and second clicking on a button on a confirmation page that states “confirm my request.”

XIII. The Attorney General Should Provide Guidance on How a Business Can Conclude that Any Given Visitor is a California Resident.

The CCPA and Regulations are both silent regarding how a business determines whether a visitor to a website is a California resident and therefore has certain rights under the CCPA.

The Alliance requests that the Attorney General provide businesses with the ability to use a website visitor’s IP address to determine if such visitor is a California consumer.

²³ 11 CCR §999.312(d).

²⁴ 11 CCR §999.316(a).

XIV. The Attorney General Should Provide Insight into What Constitutes “Reasonable Security” Measures.

The CCPA and the Regulations set forth obligations on businesses, and consequences associated with failing, to provide either “reasonable security procedures and practices” or “reasonable security measures” regarding the transmission,²⁵ verification,²⁶ and protection of personal information.²⁷ However, the Regulations offer no guidance regarding the appropriate standard for reasonable security measures and/or procedures and practices.

The Alliance strongly recommends the Attorney General explicitly set forth in the Regulations that the Center for Internet Security Controls, set forth in the California Attorney General’s 2016 Data Breach Report,²⁸ constitute the applicable baseline standard for reasonable security under the CCPA and the Regulations.

²⁵ 11 CCR §999.313(c)(6). “A business shall use reasonable security measures when transmitting personal information to the consumer.”

²⁶ 11 CCR §999.323(d). “A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer’s personal information.”

²⁷ CIV. CODE §1798.150(a)(1). “Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following...”

²⁸ *California Data Breach Report*, February 2016, available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>.

XV. The Attorney General Should Offer Regulations on the CCPA Amendments.

Governor Newsom signed additional amendments to the CCPA on October 11, 2019. These included, among other things, a business to business exemption and an employee exemption. Because the amendments were signed after the publication of the Regulations, the Attorney General should promulgate regulations on how to operationalize the above-mentioned exemptions, both of which are scheduled to sunset on January 1, 2021, only six months after the Attorney General begins enforcement of the law.

Sincerely,

A handwritten signature in black ink, appearing to read "David Chavern". The signature is written in a cursive style with a large, looped initial "D" and a smaller "C" that extends to the right.

David Chavern
President & CEO
News Media Alliance

Message

From: Monticollo, Allaire [REDACTED]
Sent: 12/6/2019 8:25:28 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Signorelli, Michael A. [REDACTED]
Subject: Advertising Trade Associations' Joint Submission of Comments on the Proposed CCPA Regulations
Attachments: Joint Ad Trade Comments on Proposed CCPA Regulations.pdf

Dear Attorney General Becerra:

Please find attached joint comments from the following advertising trade associations on the content of the proposed regulations interpreting the California Consumer Privacy Act: the Association of National Advertisers, the American Association of Advertising Agencies, the Interactive Advertising Bureau, the American Advertising Federation, and the Network Advertising Initiative.

If you have any questions, please feel free to reach out to Mike Signorelli at [REDACTED] or by phone at [REDACTED].

Best Regards,
Allie Monticollo

Allaire Monticollo, Esq. | Venable LLP

[REDACTED]
600 Massachusetts Avenue, NW, Washington, DC 20001

[REDACTED] | www.Venable.com

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



December 6, 2019

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

Dear Attorney General Becerra:

As the nation's leading advertising and marketing trade associations, we provide the following comments to offer input on the California Office of the Attorney General's ("OAG") proposed regulations implementing the California Consumer Privacy Act ("CCPA"). We and our members support the objectives of the CCPA and believe consumers deserve meaningful privacy protections supported by reasonable government policies. However, we have certain concerns about negative consequences the proposed regulations could create for consumers and businesses alike. Additionally, we are concerned that many of the proposed rules' provisions impose entirely new requirements on businesses that are outside of the scope of the CCPA and do not further the purposes of the law.

The undersigned organizations collectively represent thousands of companies in California and across the country, from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies, is responsible for more than 85 percent of the U.S. advertising spend and drives more than 80 percent of our nation's digital advertising spend. Locally, our members help generate some \$767.7 billion dollars for the California economy and support more than 2 million jobs in the state.¹ The companies we represent desire to comply with the CCPA by offering consumers robust privacy protections while simultaneously continuing to be able to do business in ways that benefit California's employment rate and its economy.

We provide the following comments to draw the OAG's attention to certain parts of the proposed regulations that are unsupported by statutory authority and other provisions that may have detrimental consequences for consumers and businesses alike. Below we provide a list of suggested updates to the proposed rules to bring them into conformity with the text of the CCPA and to rectify certain negative results they could cause for consumers and businesses. We also highlight certain provisions in the proposed regulations that we support for providing helpful clarity to the advertising and marketing industry. Some of the undersigned trades will file additional comments to the OAG.

¹ IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at <https://www.ana.net/magazines/show/id/rr-2015-ihs-ad-tax>.



I. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth

Today, the U.S. economy is increasingly fueled by the free flow of data. One driving force in this ecosystem is data-driven advertising. Advertising has helped power the growth of the Internet for decades by delivering innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet's largest players.

As a result of this advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.² Calculating against those figures, the interactive marketing industry contributed \$1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.³

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to create their own platforms to reach millions of other Internet users. Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored experience. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. Indeed, as the FTC noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.⁴ It is in this spirit—preserving the ad supported digital and offline media marketplace while helping to design privacy safeguards—that we provide these comments.

² John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017) <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>.

³ *Id.*

⁴ Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018) https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.



II. The OAG Should Ensure the Proposed Regulations' Definitions Conform with the Text of the CCPA and Are Given Consistent Meaning

Although the OAG has provided definitions for several new terms in the proposed regulations, some of the definitions contradict the text of the CCPA itself and others are used inconsistently throughout the proposed regulations, thereby obscuring the meaning of the defined terms. For example, the OAG defined “request to know” in a way that departs from the text of the CCPA. In addition, the use of the defined term “request to delete” in at least one section of the proposed regulations is at odds with its definition in the proposed regulations as well as the text of the CCPA. We respectfully ask the OAG to update the proposed regulations so that the defined terms conform with the text of the CCPA and are given consistent meaning throughout the entirety of the draft rules.

The OAG defined “request to know” as “a consumer request that a business disclose personal information that it has about the consumer... [including] [s]pecific pieces of personal information that a business has about a consumer...”⁵ This definition differs from the text of the CCPA, which states that “[a] consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer...” the categories and specific pieces of personal information “it has *collected about the consumer*.”⁶ To reduce business and consumer confusion and align the proposed regulations with California legislators’ intent and the text of the CCPA, the OAG should update the proposed rules so a “request to know” is defined as “a consumer request that a business disclose personal information that it has collected about the consumer... [including] [s]pecific pieces of personal information that a business has collected about a consumer.”

In addition, the OAG defined “request to delete” as “a consumer request that a business delete personal information about the consumer that the business has collected from the consumer...”⁷ This definition aligns with the deletion right as it is set forth in the CCPA, which states that “[a] consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.”⁸ However, in the section of the proposed regulations discussing the information that must be included in a privacy policy, the draft regulations note that a business must “[e]xplain that a consumer has a right to request the deletion of their personal information *collected or maintained* by the business.”⁹ The expression of the right to delete in the privacy policy section of the proposed regulations therefore contradicts with the CCPA’s stated expression of the right and the proposed regulations’ defined term “request to delete.” The OAG should update the privacy policy section of the CCPA so it states that a business must explain that consumers have the right

⁵ Cal. Code Regs. tit. 11, § 999.301(n)(1) (proposed Oct. 11, 2019).

⁶ Cal. Civ. Code §§ 1798.110(a)(1), (5) (emphasis added).

⁷ Cal. Code Regs. tit. 11, § 999.301(o) (proposed Oct. 11, 2019).

⁸ Cal. Civ. Code §§ 1798.105(a).

⁹ Cal. Code Regs. tit. 11, § 999.308(b)(2)(a) (proposed Oct. 11, 2019) (emphasis added).



“to request personal information about the consumer that the business has collected from the consumer” to align the section with the defined term “request to delete” and the CCPA.

As described above, we suggest that the OAG take steps to alter certain definitions in the proposed regulations so that they match and support the text of the CCPA and are used consistently throughout the draft rules. Such updates would help create certainty for businesses and consumers and would ensure that the text of the CCPA and the proposed regulations interpreting its terms are not in conflict.

III. Allow Flexibility for Businesses that Do Not Collect Information Directly to Provide Notice of Sale and an Opportunity to Opt Out

The CCPA states that a “third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out....”¹⁰ Through the proposed regulations, the OAG has provided that the business must: (1) contact the consumer directly to provide notice of sale and notice of the right to opt out, or (2) confirm the source provided a notice at collection to the consumer; obtain signed attestations from the source describing how it gave notice at collection, including an example of the notice given to the consumer; retain such attestations and sample notices for two years; and make them available to consumers upon request.¹¹ The OAG should change this provision of the draft rules so businesses are not required to maintain and make available examples of the notice provided to a consumer at the time of collection.

Requiring businesses to maintain sample notices creates a substantial new business obligation that was not contemplated by the legislature when it passed or amended the law. Requiring examples of the notice that was provided to a consumer at the time of collection constitutes a requirement that is beyond the text, scope, and intent of the CCPA, as the law itself only requires a third party to ensure a consumer has received explicit notice of sale and an opportunity to opt out. Second, little if any additional consumer benefit is provided through this new business duty to maintain example notices. The requirement to obtain attestations from data sources confirming that a notice at collection was given and describing how the notice was given provides consumers with the same transparency benefits as requiring businesses to obtain and maintain samples of the notice that was given to consumers.

Finally, mandating that businesses must maintain examples of notices provided to consumers at the time of collection is unreasonable, significantly burdensome, and could place a considerable strain on normal business operations. For example, it is possible the proposed regulations could be interpreted to require businesses to pass example notices from original sources of data to third party businesses who may later receive personal information. This obligation would impose significant new recordkeeping obligations on third party businesses and could stifle the free flow of information that powers the Internet. We therefore ask the OAG to

¹⁰ Cal. Civ. Code § 1798.115(d).

¹¹ Cal. Code Regs. tit. 11, § 999.305(d) (proposed Oct. 11, 2019).



remove the requirement for businesses to obtain examples of the notices at collection that were given to consumers to enable more flexibility for businesses to comply with the requirements the CCPA places on third parties who engage in personal information sale.

IV. Remove the Requirement to Respect Browser Signal Opt Outs so Consumers' Are Provided with Consumer Choice

The draft rules require businesses that collect personal information from consumers online to “treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt out of the sale of their personal information as a valid request...”¹² This requirement is extralegal and goes beyond the text and scope of the CCPA by imposing a substantive new requirement on businesses that was not set forth by the legislature and does not have any textual support in the statute itself. For this reason and others we describe below, we ask the OAG to eliminate this requirement, or, at a minimum, give businesses the option to either honor browser plugins or privacy settings or mechanisms, or decline to honor such settings if the business includes a “Do Not Sell My Personal Information” link and offers another method for consumers to opt out of the sale of personal information.

The browser-based signal requirement in the proposed rules has no textual support in the CCPA itself. The California legislature could have included a browser-based signal mandate when it initially passed the CCPA, or when it amended it via multiple bills thereafter,¹³ but the legislature never chose to impose such a requirement. Moreover, the California legislature already considered imposing a similar browser setting requirement in 2013 when it amended the California Online Privacy Protection Act.¹⁴ The legislature ultimately decided against imposing a single, technical-based solution to enabling consumer choice and instead chose to offer consumers multiple avenues through which they may communicate their preferences. Together, these decisions reveal that the California legislature had the opportunity to enact a browser-based signal requirement on multiple occasions, but never chose to do so, and as such, the proposed regulation mandating that such signals be treated as verifiable consumer requests does not further legislative intent and is outside the scope of the CCPA.

If the OAG ultimately maintains this requirement, we suggest that the OAG modify it so that a business engaged in the sale of personal information must *either* abide by browser plugins or privacy settings or mechanisms, or may not honor such settings if the business includes a “Do Not Sell My Personal Information” link and offers another method for consumers to opt out of personal information sale by the business. The latter approach is more consistent with the spirit of the CCPA and the intentions of the legislature, as it affords consumers with robust choice and control over the sale of personal information. In contrast, browser-based signals or plugins would broadcast a single signal to all businesses opting a consumer out from the entire data

¹² *Id.* at § 999.315(c).

¹³ See AB 1121 (Cal. 2018); AB 25 (Cal. 2019); AB 874 (Cal. 2019); AB 1146 (Cal. 2019); AB 1355 (Cal. 2019); AB 1564 (Cal. 2019).

¹⁴ AB 370 (Cal. 2013).



marketplace. It is not possible through these settings for a consumer to make discrete choices among businesses allowing the consumer to restrict certain businesses while permitting other businesses to transfer data to benefit the consumer. Furthermore, it is not possible for a business to verify if a consumer set the browser setting or some intermediary did so without the authorization of the consumer.

In addition, certain intermediaries in the online ecosystem stand between consumers and businesses and therefore have the ability to interfere with the data-related selections consumers may make through technological choice tools. These intermediaries, such as browsers and operating systems, can impede consumers' ability to exercise choices via the Internet that may block digital technologies (*e.g.*, cookies, javascripts, and device identifiers) that consumers can rely on to communicate their opt out preferences. This result obstructs consumer control over data by inhibiting consumers' ability to communicate preferences directly to particular businesses and express choices in the marketplace. The OAG should by regulation prohibit such intermediaries from interfering in this manner.

We ask the OAG to eliminate the requirement to honor browser plugins or privacy settings or mechanisms, or, alternatively, revise the draft rules so that businesses have the option of honoring such settings or providing a "Do Not Sell My Personal Information" link along with another method for consumers to opt out of the sale of personal information by the business. We also ask the OAG to update the proposed rules to prohibit intermediaries from blocking or otherwise interfering with the technology used to effectuate consumer preferences in order to protect the opt out signals set by consumers via other tools.

V. Enable Effective Opt Out Mechanisms for Businesses that Do Not Maintain Personally Identifiable Personal Information

The proposed regulations require businesses to offer consumers a webform through which they may opt out of the sale of personal information.¹⁵ However, webforms may not work to facilitate opt outs for online businesses that do not maintain personally identifiable information about consumers. Many businesses in the online ecosystem may maintain personal information that does not identify a consumer on its own, for example, IP addresses, mobile advertising identifiers, cookie IDs, and other online identifiers. For businesses that maintain this non-identifying information, webforms may not work to facilitate consumer requests to opt out, because the consumer's submission of identifying information such as a name, email address, or postal address may not be easily matched to the non-personally identifiable information the business does maintain. This provision could undermine the privacy-protective elements of the CCPA by forcing companies to attempt re-identification techniques which are widely avoided by industry in its efforts to enhance consumer privacy.¹⁶ Consequently, the proposed rules should provide businesses with flexibility to offer mechanisms for consumers to opt out of personal information sale. The OAG has indicated it may issue another button or logo to enable a

¹⁵ Cal. Code Regs. tit. 11, § 999.315(a) (proposed Oct. 11, 2019).

¹⁶ See Fix CCPA, *Don't Force Companies to Connect Online Identities to Real Names*, located at <https://www.fixccpa.com/>.



consumer to opt out of the sale of personal information.¹⁷ We encourage the OAG to consider industry leading implementations that already have consumer recognition in crafting another acceptable opt out mechanism. We also ask the OAG to clarify that online businesses that do not maintain personally identifying information may use an effective method to enable a consumer to opt out other than a webform.

VI. Clarify Businesses Are Not Required to Collect or Maintain More Personal Information to Verify a Consumer

Pursuant to the draft regulations, “[a] business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, and for security or fraud-prevention purposes.”¹⁸ The AG should clarify by regulation that businesses are not required to collect data they do not maintain or collect in the regular course of business in order to verify a consumer’s identity.

Some businesses may maintain personal information in a manner that is not associated with a named actual person. For example, IP addresses and cookie IDs are kinds of personal information that could be associated with or linked to information from many consumers rather than information from a single consumer. Moreover, businesses often keep information that could identify a consumer’s identity separate from other information that may not be identifying on its own. This practice is privacy protective, as it separates consumer identities from certain information collected about the consumer. The draft rules’ current text could require businesses that do not maintain information that is associated with a named actual person to collect additional information from consumers in order to verify their identities. While the draft regulations acknowledge that “fact-based verification process[es]” may be required in such circumstances,¹⁹ this provision of the proposed regulations could force businesses to investigate consumer identities by procuring more data than they normally would in their normal course of business in order to verify consumers.

A business should not be required to obtain additional information from consumers in order to comply with the CCPA. The purpose of the law is to enhance privacy protections for consumers, and forcing businesses to collect data they would not otherwise collect, maintain, or normally associate with a named actual person has the potential to undermine consumer privacy rather than enhance it.²⁰ The OAG should clarify that while businesses *may* collect additional

¹⁷ Cal. Code Regs. tit. 11, at § 999.306(e) (proposed Oct. 11, 2019).

¹⁸ *Id.* at § 999.323(c).

¹⁹ *Id.* at 999.325(e)(2).

²⁰ For example, this mandate would force businesses to collect more information from consumers than they typically do in their normal course of business. Reports on the General Data Protection Regulation (“GDPR”) in Europe have revealed that unauthorized individuals can exploit the law to access personal information that does not



information from a consumer to verify the consumer's identity, the business does not need to do so to comply with the law.

VII. Ensure that Businesses May Provide User-Friendly Privacy Policies to Consumers

The proposed regulations set forth certain requirements for businesses in providing privacy-related notices to consumers. Some of these requirements, such as the obligation to provide relevant disclosures with respect to *each category of personal information collected*, represent new obligations that are not expressly included in the text of the CCPA and may force businesses to produce excessively long and confusing privacy notices that would do little to further consumers' understanding of business data practices. Other notice-related requirements in the draft rules are unclear. For example, the draft regulations do not clearly state whether the required notice at collection, notice of right to opt out, and notice of financial incentive may be provided to consumers in a privacy policy. We urge the OAG to update the draft rules so that consumers may receive understandable privacy notices and so that businesses may provide all required privacy-related notices in a single privacy policy disclosure.

According to the proposed regulations, in privacy policies business must list the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties with whom the business shares personal information “[f]or *each category of personal information collected*...”²¹ However, the terms of the CCPA itself do not require businesses to make disclosures relevant to each category of personal information collected, but rather require businesses to make disclosures with respect to all personal information collected. As such, requiring granular, category-by-category disclosures for each type of personal information collected imposes a significant new substantive requirement on businesses that has no textual basis for support in the CCPA.

Additionally, requiring granular disclosures for each category of personal information collected could impede businesses from ensuring privacy policies are “written in a manner that provides consumers [with] a meaningful understanding of the categories listed.”²² If businesses must make disclosures about sources, purposes, and third parties for each category of personal information collected, privacy notices could be excessively complicated, lengthy, and incomprehensible for consumers, thereby impeding the purpose of providing an informative and understandable consumer privacy notice. Moreover, consumers would be less likely to read and understand such lengthy notices, which could impede the CCPA's goal of enhancing the transparency of business data practices. The OAG should align the regulations with the text of the CCPA by removing the “for each category of personal information collected” language. This change would enable consumers to receive meaningful privacy policies that sensibly disclose

belong to them, causing risks of identity theft. See BBC News, *Black Hat: GDPR privacy law exploited to reveal personal data* (Aug. 9, 2019), located at <https://www.bbc.com/news/technology-49252501>.

²¹ Cal. Code Regs. tit. 11, § 999.308(b)(1)(d)(2) (proposed Oct. 11, 2019).

²² *Id.*



required information in an undaunting and clear format and would advance California legislators' aim of enabling comprehensible, workable consumer notices more effectively than requiring disclosures pertaining to each category of personal information collected.

VIII. Allow Businesses to Satisfy All CCPA-Related Notice Requirements in a Privacy Policy

Pursuant to the proposed rules, businesses must provide a privacy policy and certain other particular notices to consumers. Specifically, in addition to a privacy policy, businesses must provide a notice at collection, a notice of the right to opt out of the sale of personal information, and a notice of financial incentive.²³ However, the proposed rules do not clearly state whether the notice at collection, notice of the right to opt out of the sale of personal information, or notice of financial incentive may be offered to consumers through the privacy policy. The OAG should clarify that all required notices may be provided in a privacy policy.

The draft rules state that a notice at collection may be provided through a conspicuous link on the business's website homepage, mobile application download page, or on all webpages where personal information is collected, which represent typical methods through which privacy policies are normally offered to consumers.²⁴ However, the draft rules do not expressly confirm that a notice at collection may be provided through the privacy policy. Similarly, while a notice of the right to opt-out must include certain particular information or link to the section of the business's privacy policy that contains such information, there is no explicit confirmation that the opt out notice requirement may be satisfied by providing the necessary information in a privacy policy.²⁵ Finally, if a business offers a financial incentive or price of service difference online, the business must link to the section of the business's privacy policy that contains the required information, but it is unclear whether making such a disclosure counts as the required notice of financial incentive that must be offered to consumers.²⁶

We ask the OAG to update the proposed rules so they remove the requirement to provide disclosures with respect to each category of personal information collected, and so that they explicitly state that the notice at collection, notice of right to opt-out, and notice of financial incentive may be provided to consumers in a privacy policy. These updates would lessen the possibility for consumer notice fatigue by enabling more concise, readable notices. They would also be consistent with consumer expectations and would enable more effective and less confusing consumer disclosures, as all privacy-related information could be housed in a unified location. Moreover, such a rule would help businesses in their efforts to meet the CCPA's requirements, because business would be able to focus on reviewing and updating one notice as needed instead of multiple notices. The OAG should clarify that all required notices may be

²³ *Id.* at §§ 999.305, 306, 307.

²⁴ *Id.* at § 999.305(a)(2)(e).

²⁵ *Id.* at § 999.306(b)(1).

²⁶ *Id.* at § 999.307(a)(3).



provided in a privacy policy, because such a clarification would reduce confusion for consumers and better enable CCPA compliance for businesses.

IX. Clarify that Requesting Verifying Information from a Consumer Pauses the Time Period Within Which a Business Must Respond to the Request

The proposed regulations set forth a risk-based process by which businesses may engage in efforts to verify consumers before acting on their requests to delete and requests to know.²⁷ We support the non-prescriptive, risk-based framework for verifying consumer requests that is outlined in the proposed regulations. It provides businesses the flexibility they need to create verification mechanisms that fit their business models while being robust enough to accurately identify consumers submitting CCPA requests. However, despite the beneficial nature of the risk-based approach for verifying consumer requests that is outlined in the proposed rules, we are concerned that the draft rules do not provide businesses with enough time to verify consumers before they are responsible for effectuating CCPA requests.

The draft rules require a business to comply with requests to know and delete within 45 days of receiving the request regardless of the period of time it takes for the business to verify the request.²⁸ We ask the OAG to reconsider this requirement and update the draft rules so a business's request for information to verify a consumer's identity before effectuating a consumer request tolls or pauses the 45-day window within which the business must respond to the request. Consumer verification is necessary for businesses to accurately effectuate consumers' CCPA rights. Robust and accurate verification is in the interest of consumers, because without it, businesses run the risk of erasing or returning data that does not pertain to the requesting consumer. Such a result could have two distinct consumer harms: first, it would fail to fulfill the wishes of the consumer who actually submitted the request, and second, it could impact personal information about a consumer that did not make the request. Consequently, we urge the OAG to update the proposed rules so a business's request for verifying information tolls or pauses the 45-day period within which the business must respond to consumer requests to know and delete.

X. Clarify that a Business May Provide a General Toll-Free Number for Receiving CCPA Requests

According to the draft rules, a business must enable consumers to submit requests to know via a toll-free number and may provide a toll-free number to receive requests to delete and opt out of personal information sale. The proposed rules as currently drafted do not clarify if a business may offer its general toll-free number to receive CCPA requests or if a business must create a separate, CCPA-specific number through which it should receive consumer requests under the law. We ask the OAG to clarify that a business may offer consumers its general toll-free number to receive consumer CCPA requests and does not need to create or staff an entirely new phone number for such requests. Such an update to the proposed rules would decrease consumer confusion by funneling all business-related inquiries through one contact phone

²⁷ *Id.* at §§ 999.323, 324, 325.

²⁸ *Id.* at § 999.313(b).



number. It would also help businesses by refraining from imposing an unnecessary cost on them to staff and maintain a separate number for CCPA requests. Consequently, we urge the OAG to update the draft rules to clarify that a business can provide its general consumer telephone number as the toll-free phone number through which it may receive consumer CCPA requests.

XI. Remove the Requirement to Flow Down Opt Out Requests to Third Parties to Whom the Business has Sold Personal Information in the Prior 90 Days

The proposed rules would require businesses to pass on the opt out requests they receive to third parties. Specifically, a business must “notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business’s receipt of the consumer’s request that the consumer has exercised their right to opt out and instruct them not to further sell the information.”²⁹ This requirement does not further meaningful consumer choice, as it takes a consumer’s opt out selection with respect to one business and propagates it throughout the ecosystem without the consumer’s express consent to do so. Furthermore, it represents a departure from the text of the CCPA by imposing a brand-new requirement on businesses that was not contemplated by the text of the law itself.

Requiring businesses to pass on opt out requests to third parties that received the consumer’s personal information in the prior 90 days could impede a consumer’s ability to exercise specific choices that are effective against particular businesses. A consumer’s choice to opt out of one business’s ability to sell personal information does not mean that the consumer meant to opt out of every business’s ability to sell personal information. This proposed rule has the potential to cause consumers to lose access to online offerings and content that they did not expect or choose to lose by submitting an opt out request to a single business. The law should not require businesses to understand a consumer’s opt out choice as a decision that must apply throughout the entire Internet ecosystem. In addition, requiring businesses to communicate opt out requests to third parties is a substantial new obligation that does not give businesses enough time to build processes to comply with the requirement before January 1, 2020.³⁰ The CCPA, as passed by the Legislature, already provides a means for consumers to control onward sales by third party businesses. The law requires that consumers be provided explicit notice and opportunity to opt out from sale.³¹ The new obligation to pass opt out requests on to third parties that received the consumer’s personal information within the past 90 days moves beyond the text and intent of the CCPA by imposing material and burdensome new obligations on businesses

²⁹ *Id.* at § 999.315(f).

³⁰ The Standardized Regulatory Impact Assessment (“SRIA”) analyzing the proposed regulations’ economic effect on the California economy is also deficient on this point. *See* SRIA at 25-26. The SRIA indicates “[t]he incremental compliance cost associated with this regulation is the extra work required by businesses to notify third parties that further sale is not permissible.” *Id.* at 25. This comment overlooks the ripple effect that the requirement to pass opt out requests on to third parties that have received a consumer’s personal information in the past 90 days would have throughout the Internet ecosystem and the economy. Under the draft rules, a consumer’s single opt out of sale request would restrict beneficial uses of personal information, including those generally occurring subsequent to the initial sale. The OAG should consider how restricting the sale of personal information by third parties in this way can “increase or decrease... investment in the state.” *See* Cal. Gov. Code § 11346.3(c)(1)(D).

³¹ Cal. Civ. Code § 1798.115(d).



without textual support in the CCPA. We therefore encourage the OAG to update the proposed rules so businesses are not required to pass opt out requests along to third parties. Alternatively, the OAG should limit the requirement to information the business actually sold to third parties in the previous 90 days.

XII. Align the Draft Rules with Consumer Choices by Removing the Requirement to Convert Unverifiable Requests to Delete into Requests to Opt Out

If a business cannot verify a consumer who has submitted a request to delete, the proposed rules would require the business to “inform the requestor that their identity cannot be verified and... instead treat the request as a request to opt out of personal information sale.”³² Compelling businesses to convert unverifiable consumer deletion requests into opt out requests could hinder or even completely impede meaningful consumer choice in the marketplace. This mandate has the potential to force a result that the consumer neither intended nor approved. Consequently, we ask the OAG to update the proposed rules so that businesses are not forced to transform unverified deletion requests into opt out requests unless the consumer specifically asks the business to do so.

The CCPA provides separate consumer rights for deletion and opting out of personal information sale because these two rights achieve different policy aims and consumer goals. While deletion is structured to erase the consumer’s personal information from the databases and systems *of the business to which the consumer communicates the request*, the opt out right empowers consumers to stop the transfer of data to *other businesses* in the chain. Because these two rights achieve two different objectives, the law should not compel consumers to opt out of personal information sale if a business cannot verify their request to delete. This outcome, which would be legally required by the proposed regulations, it is not likely to reflect the consumer’s desires in submitting a deletion request.

To illustrate this point, the OAG’s proposed rule requiring businesses to communicate opt out requests to third parties to whom they have sold personal information in the prior 90 days and instruct them not to further sell personal information could cause a consumer’s unverified deletion request to be transformed into an opt out request that is imposed on many other parties other than the business that is the recipient of the request. As a result, a business may be required to transform a deletion request a consumer may have thought she served on one business alone into an opt out request by that business and pass that opt out request along to other businesses without obtaining the consumer’s consent to take this action. This obligation therefore has the potential to unknowingly expose the consumer to potential loss of products and services she did not wish to lose. This result deprives consumers of the ability to make particularized selections about businesses who may and may not sell personal information. We therefore respectfully ask the OAG to align the draft rules with consumer choices by removing the requirement to convert unverifiable requests to delete into requests to opt out unless the consumer affirmatively requests that the business take such an action.

³² Cal. Code Regs. tit. 11, § 999.313(d)(1) (proposed Oct. 11, 2019).



* * *

Thank you for the opportunity to submit input on the content of the proposed regulations interpreting the CCPA. We look forward to continuing to engage with your office as it finalizes the draft rules. Please contact us with any questions you may have regarding these comments.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
[REDACTED]

Dave Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
[REDACTED]

Christopher Oswald
SVP, Government Relations
Association of National Advertisers
[REDACTED]

Alison Pepper
Senior Vice President
American Association of Advertising
Agencies, 4A's
[REDACTED]

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
[REDACTED]

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
[REDACTED]

CC: Mike Signorelli, Venable LLP

Message

From: Michael Pepson [REDACTED]
Sent: 12/6/2019 7:53:38 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: AFPP Coalition Comment on CCPA Regulations
Attachments: 2019.12.06 AFPP Coalition CCPA Regulatory Comment.pdf

To whom it may concern:

Please see the attached AFPP Coalition Comment pertaining to the proposed CCPA regulations.

Thank you for your attention to this matter.

Sincerely,

Michael Pepson

December 6, 2019



Via E-Mail

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

Re: Proposed California Consumer Privacy Act Regulations

To whom it may concern:

On behalf of the undersigned organizations, we appreciate the opportunity to comment on the California Attorney General's ("AG") proposed California Consumer Privacy Act ("CCPA" or "the Act") Regulations. As discussed below, we believe that although consumer data privacy is an important subject that should be addressed at the national level, the U.S. Constitution categorically bars individual states from seeking to regulate the Internet on a national level, as California has sought to do here. The Internet is a subject requiring national uniformity that can only be regulated by the federal government, as opposed to through a burdensome and conflicting patchwork of flatly unconstitutional extraterritorial state laws like the CCPA.

In January 2019, a coalition of privacy experts warned the California Legislature about the CCPA's fatal constitutional flaw: "The CCPA's purported application to activity outside of California raises substantial Constitutional concerns and potentially exposes the state to expensive and distracting litigation."¹ They urged the California Legislature to "clarify the CCPA's applicability to activities outside of California."² The California Legislature has not heeded these privacy experts' clarion call for amendments to the CCPA to bring it in line with constitutional limits on the scope of California's regulatory authority.

The CCPA specifically directs the AG to adopt regulations "[e]stablishing any exceptions [to the CCPA]

¹ Letter from Professor Eric Goldman *et al.* to The Honorable Toni Atkins *et al.*, 3 (Jan. 17, 2019), <http://bit.ly/2DgP0by>.

² *Id.*

necessary to comply with state or federal law,”³ which includes the federal Constitution. Accordingly, we urge you to amend the CCPA regulations to formally, and permanently, disavow any intention of bringing enforcement actions under the CCPA outside of California, due to the statute’s blatant unconstitutionality,⁴ as well as permanently prohibit private parties from any attempt to sue companies outside California for alleged violations of the CCPA. Businesses and California’s sister States should not be forced to sue in federal court to protect their federal constitutional rights.

I. EXECUTIVE SUMMARY

The CCPA is California’s misguided attempt to regulate privacy on a national level to impose its vision of public policy on the entire country. As the California Department of Justice has acknowledged in connection with this rulemaking: “California standards often become national standards because, given the size of the California economy, companies find it easier to adopt a uniform approach rather than differentiating their offerings.”⁵ So too here.

The Act imposes draconian compliance obligations on a host of companies, has a sweeping extraterritorial effect, subjects businesses to an inconsistent patchwork of regulations, and threatens to stifle not only technology and innovation but also free speech. The CCPA is also unconstitutional. *First*, the CCPA is invalid because it has the practical effect of regulating wholly out-of-state conduct and burdening interstate commerce in violation of the dormant Commerce Clause. *Second*, the CCPA’s restrictions on free speech violate the First Amendment. *Third*, the CCPA violates due process for failure to give fair notice of prohibited or required conduct.

II. STATUTORY AND REGULATORY BACKGROUND

A. Overview of CCPA

In 2018, pursuant to a deal struck with the California real estate developer responsible for the ballot initiative, California enacted Assembly Bill 375 (AB 375), now known as the CCPA. In return, the developer pulled the ballot initiative.⁶

The CCPA is an unprecedented state privacy law that will impose sweeping restrictions on the handling of California residents’ data that will affect most businesses with any online presence, imposing draconian compliance costs.⁷ As the Standardized Regulatory Impact Assessment

³ Cal. Civ. Code § 1798.185(a)(3).

⁴ *Cf. Lockyer v. City & Cnty. of S.F.*, 95 P.3d 459, 501–02 (2004) (Moreno, J., concurring) (arguing “there are at least three types of situations in which a local government’s disobedience of a[n] unconstitutional statute would be reasonable”).

⁵ Cal. Dep’t of Justice, Notice of Proposed Rulemaking Action [hereinafter “NPRO”], at 13 (Oct. 11, 2019), available at <http://bit.ly/33jGZxl>; accord Cal. Dep’t of Justice, Office of the Attorney General, Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations [hereinafter “SRIA”], at 32 (Aug. 2019) (“Given the size of the California economy, previous legislation that was unique to California has in turn set national standards[.]”), available at <http://bit.ly/2qItKJ2>.

⁶ See SRIA at 7 (“Before reaching the ballot however, the California legislature offered AB 375 in exchange for the withdrawal of the ballot measure.”).

⁷ The Act grants California residents a number affirmative rights, which covered businesses must accommodate at their expense, including the right to request that a business that sells consumer information or discloses it for a business purpose discloses to the consumer the categories of information collected or disclosed, Cal. Civ. Code § 1798.115;

(“SRIA”) explains, the CCPA and its implementing regulations impose a diverse array of costly new obligations, including:

1. Legal: Costs associated with interpreting the law so that operational and technical plans can be made within a business.
2. Operational: Costs associated with establishing the non-technical infrastructure to comply with the law’s requirements.
3. Technical: Costs associated with establishing technologies necessary to respond to consumer requests and other aspects of the law.
4. Business: Costs associated with other business decisions that will result from the law, such as renegotiating service provider contracts and changing business models to change the way personal information is handled or sold.⁸

The SRIA correctly recognizes that the legal “costs can be quite large”; the “[o]perational costs . . . can include substantial labor costs”; and that “[t]echnology costs, which cover the websites, forms, and other systems necessary to fulfill the CCPA compliance obligations, are also quite substantial due to passage of the CCPA.”⁹ “Small firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises. . . . Another significant risk to small businesses is uncertainty.”¹⁰

Accordingly, as the California AG found, the CCPA and its implementing “regulations may have a significant, statewide adverse economic impact directly affecting business[.]”¹¹ “These businesses fall within most sectors of the California economy, including agriculture, mining, utilities, construction, manufacturing, wholesale trade, retail trade, transportation and warehousing, information, finance and insurance, real estate, professional services, management of companies and enterprises, administrative services, educational services, healthcare, arts, accommodation and food services, among others.”¹² Worse still, the new law was designed to, and will apply, extraterritorially to businesses operating outside of California, so long as there is any nexus to California. Companies that are not prepared to comply with the Act’s onerous requirements will face the threat of severe civil penalties and class action lawsuits.

right to opt out of sale of “personal information,” *id.* § 1798.120; *see also id.* § 1798.135; and right to deletion of “personal information.” *id.* § 1798.105. The CCPA also affirmatively requires covered businesses to provide notice and disclosure of “personal information” they collect, *id.* § 1798.100(b), and effectively mandates an overhaul of consumer-facing websites, micromanaging the content, *id.* § 1798.135. The Act further specifies how businesses are supposed to receive and respond to various requests propounded by California residents and sets a timeline for response. *Id.* § 1798.130. This means that, as a practical matter, covered businesses must revise their websites and privacy policies, undertake the onerous process of determining what data they have about California consumers and where it is located, and pay for the compliance costs associated with responding to various California consumers’ requests under the Act. The Act also imposes training requirements. *See id.* § 1798.130(a)(6).

⁸ SRIA at 10.

⁹ *See id.* at 10–11.

¹⁰ *Id.* at 31.

¹¹ NPRA at 11.

¹² *Id.*

As discussed below, in addition to the CCPA’s policy-related and practical problems, as drafted in its current form, the Act violates the federal Constitution in a several ways.

B. Extraterritorial Scope of Compliance Obligations

The CCPA’s onerous compliance obligations apply to a wide array of commercial entities that in any way “do[] business in the State of California,” if certain threshold requirements are met.¹³ Specifically, companies with any California nexus—regardless of whether they have any physical presence within California—must comply with the Act if any one of the following requirements are met: (A) “annual gross revenues in excess of twenty-five million (\$25,000,000),” regardless of profit margin; (B) any company that “[a]lone or in combination, annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices[]”; or (C) “[d]erives 50 percent or more of its annual revenues from selling consumers’ personal information.”¹⁴ As a practical matter, these definitions, particularly coupled with the Act’s very broad definition of “[p]ersonal information,”¹⁵ threaten to sweep in most companies operating in the United States with any significant online presence.

The Act purports to apply even to companies that do not have any nexus whatsoever with California (including those that do not have a single California customer), such as commonly branded parents and subsidiaries of covered businesses.¹⁶ Thus, for example, a parent company based overseas and conducting no business whatsoever within the United States would be subject to the Act if a subsidiary without any physical presence in California was subject to the Act by virtue of any nexus with California coupled with meeting any of the threshold requirements. Indeed, the Act contains a provision that purports to extend globally to transactions that have no nexus whatsoever to California except for the possession of California residents’ personal information, even if that information was originally received by some other entity located outside of California, by creating a legal fiction: that the out-of-state entity that somehow “received” the “personal information” from some other out-of-state entity that does business in California should be deemed to both do business with California and also “collect” the information.¹⁷ Just as the CCPA applies broadly to a host of commercial enterprises, many of which have tenuous or nonexistent physical contacts with California, the CCPA contains a sweeping and vague definition of “personal information” to which it applies.¹⁸

¹³ See Cal. Civ. Code § 1798.140(c)(1).

¹⁴ *Id.* § 1798.140(c)(1)(A)-(C).

¹⁵ *Id.* § 1798.140(o).

¹⁶ *Id.* § 1798.140(c)(2) (defining “business” to include “Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business”).

¹⁷ *Id.* § 1798.115(d) (“A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out[.]”); *Id.* § 1798.140(w) (broad definition of “third party”); *Id.* § 1798.140(t) (broad definition of “sell”). See also California Senate Judiciary Committee Report, AB 375, at 9 (June 25, 2018). *Cf.* Cal. Civ. Code § 1798.190.

¹⁸ See Cal. Civ. Code § 1798.140(o)(1) (“‘personal information’ means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household” and providing a non-exhaustive list of examples); see also *id.* § 1798.80(e).

Businesses and service providers that are subject to the Act must take a number of affirmative actions or risk civil penalties and class action lawsuits.¹⁹ Importantly, the Act’s civil penalties provision is not limited to “businesses,” as defined in the Act, and purports to broadly apply to a variety of third parties that have no nexus whatsoever with California.²⁰ Indeed, the Initial Statement of Reasons (“ISOR”) admits that CCPA “regulations may be enforceable against businesses located in other states that have their own attorneys general.”²¹ Yet California refused even to attempt to assess the economic effects of its CCPA regulations on out-of-state entities.²²

Perhaps recognizing the extraterritorial effect of the Act—and the attendant constitutional problems with said effect, discussed below—the Act attempts to bring itself within constitutional bounds through a provision that purports to exempt wholly out-of-state conduct from its purview.²³ Similarly, the CCPA only grants rights and privileges to natural persons who are “California residents . . . however identified, including by unique identifier.”²⁴ However, these superficial bows to the U.S. Constitution are woefully insufficient.

III. THE CCPA VIOLATES THE COMMERCE CLAUSE.

A. The CCPA Has the Practical Effect of Regulating Wholly Out-of-State Conduct.

As described above, the CCPA regulates extraterritorially in violation of the dormant Commerce Clause.²⁵ “[S]tate regulation violates the dormant Commerce Clause . . . if it regulates conduct occurring entirely outside of a state’s borders.”²⁶ When a state statute directly regulates interstate commerce, whether facially or in practical effect, the Court generally has “struck down the statute without further inquiry.”²⁷ The dormant Commerce Clause’s bright-line *per se* bar against extraterritorial regulation is rooted in federalism. It is fundamental to our system of federalism that “[n]o state can legislate except with reference to its own jurisdiction.”²⁸ A state’s regulatory authority “is not only subordinate to the federal power over interstate commerce, but is

¹⁹ See Cal Civ Code § 1798.155(b) (civil penalties of up to \$2,500 for each violation and \$7,500 for each intentional violations); Cal Civ Code § 1798.150 (private right of action, including class action, for data breach).

²⁰ See Cal Civ Code § 1798.155(b) (“Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty[.]” (emphasis added)); see also Cal Civ Code § 1798.140(v) (defining “service provider”); Cal Civ Code § 1798.140(w) (broad definition of “third party”).

²¹ ISOR at 3.

²² See SRIA at 21.

²³ See Cal Civ Code § 1798.145(a)(6).

²⁴ See Cal Civ Code § 1798.140(g).

²⁵ See also Jeff Kosseff, *Hamiltonian Cybersecurity*, 54 Wake Forest L. Rev. 156, 193-203 (2019) (state regulation of the Internet may be vulnerable to constitutional challenges); Jennifer Huddleston and Ian Adams, “Potential Constitutional Conflicts in State and Local Data Privacy Regulations,” at 6-9 (Dec. 2019), at <http://bit.ly/2LiRIIK>.

²⁶ *Am. Fuel & Petrochemical Mfrs. v. O’Keefe*, 903 F.3d 903, 911 (9th Cir. 2018); see *Rosenblatt v. City of Santa Monica*, 940 F.3d 439, 445 (9th Cir. 2019) (“A *per se* violation of the dormant Commerce Clause occurs [w]hen a state statute directly regulates or discriminates against interstate commerce[.] . . . A local law directly regulates interstate commerce when it directly affects transactions that take place across state lines or entirely outside of the state’s borders.” (cleaned up)); see also *Legato Vapors, LLC v. Cook*, 847 F.3d 825, 830 (7th Cir. 2017). Courts have held that actual inconsistency between state regulations is not required; “the threat of inconsistent regulation, not inconsistent regulation in fact, is enough[.]” *Id.* at 834.

²⁷ *Brown-Forman Distillers Corp. v. New York State Liquor Auth.*, 476 U.S. 573, 579 (1986).

²⁸ *Bonaparte v. Tax Court*, 104 U.S. 592, 594 (1881).

also constrained by the need to respect the interests of other States.”²⁹ The rule that one state has no power to project its legislation into another state embodies the Constitution’s concern both with the maintenance of a national economic union unfettered by state-imposed limitations on interstate commerce and with the autonomy of the individual States within their respective spheres.³⁰

The CCPA violates this rule. Numerous state statutes regulating the Internet have been found unconstitutional on these grounds.³¹ The CCPA is no different. The Act on its face and in practical effect regulates wholly out-of-state contractual relationships between out-of-state entities and wholly out-of-state sales. For example, the CCPA purports to reach the sale of “personal information” by a covered “business” located in New York to a service provider or third party located in Florida, or the use of “personal information” by a third party located in North Dakota or England that somehow receives it from a “business” located in New Jersey. The only nexus to California is the fact that “personal information” from California residents located in California was “collected” by one of the out-of-state entities involved. This California may not do under Ninth Circuit precedent because both parties to the contract are located out-of-state.³²

“[A] statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State’s authority and is invalid regardless of whether the statute’s extraterritorial reach was intended by the legislature. The critical inquiry is whether the practical effect of the regulation is to control conduct beyond the boundaries of the State.”³³ The Commerce Clause “precludes the application of a state statute to commerce that takes place wholly outside of the State’s borders, whether or not the commerce has effects within the State.”³⁴ Thus, “States and localities may not attach restrictions to exports or imports in order to control commerce in other States.”³⁵ “[T]he Commerce Clause [also] protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State.”³⁶ “[T]he practical effect of the statute must be evaluated not only by considering the

²⁹ *BMW of N. Am., Inc. v. Gore*, 517 U.S. 559, 571-72 (1996) (citations omitted).

³⁰ See *Healy v. Beer Inst.*, 491 U.S. 324, 335-36 (1989); *Baldwin v. G.A.F. Seelig, Inc.*, 294 U.S. 511, 521 (1935); see also *N.Y. Life Ins. Co. v. Head*, 234 U.S. 149, 161 (1914) (territorial constraint is an “obvious[]” and “necessary result of the Constitution”); *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 293 (1980) (“The sovereignty of each State imp[li]e[s] a limitation on the sovereignty of all of its sister States” that is inherent in “the original scheme of the Constitution[.]”).

³¹ See, e.g., *Publius v. Boyer-Vine*, 237 F. Supp. 3d 997 (E.D. Cal. 2017) (O’Neil, J.) (finding First Amendment and dormant Commerce Clause extraterritoriality violations with respect to California statute regulating out-of-state posting of truthful personal information about California legislators on the Internet); *Am. Booksellers Found. v. Dean*, 342 F.3d 96, 104-05 (2d Cir. 2003); *Backpage.com, LLC v. Hoffman*, No. 13-03952, 2013 U.S. Dist. LEXIS 119811, at *33 (D.N.J. Aug. 20, 2013) (“Because the internet does not recognize geographic boundaries, it is difficult, if not impossible, for a state to regulate internet activities without project[ing] its legislation into other States. The Act is likely in violation of the dormant commerce clause, and thus cannot stand.”).

³² See *Sam Francis Found. v. Christies, Inc.*, 784 F.3d 1320, 1322 (9th Cir. 2015) (en banc).

³³ *Healy*, 491 U.S. at 336; see also *BMW of N. Am. v. Gore*, 517 U.S. 559, 572 (1996) (“a State may not impose economic sanctions on violators of its laws with the intent of changing the tortfeasors’ lawful conduct in other States.”). Cf. *C & A Carbone v. Town of Clarkstown*, 511 U.S. 383, 394 (1994) (even a regulation that does not expressly regulate interstate commerce may do so “nonetheless by its practical effect and design”).

³⁴ *Healy*, 491 U.S. at 336 (internal citations omitted).

³⁵ *C & A Carbone*, 511 U.S. at 393 (citing *Baldwin*, 294 U.S. 511).

³⁶ *Healy*, 491 U.S. at 336-37.

consequences of the statute itself, but also by considering how the challenged statute may interact with the legitimate regulatory regimes of other States and what effect would arise if not one, but many or every, State adopted similar legislation.”³⁷

“The mere fact that some nexus to a state exists will not justify regulation of wholly out-of-state transactions. For example, an attempt by California to regulate the terms and conditions of sales of artworks outside of California simply because the seller resided in California was a violation of the dormant Commerce Clause.”³⁸ As the Ninth Circuit explained in *Sam Francis v. Christie’s, Inc.*: “The Supreme Court has held that ‘our cases concerning the extraterritorial effects of state economic regulation stand at a minimum for the following proposition[]: . . . the Commerce Clause precludes the application of a state statute to commerce that takes place wholly outside of the State’s borders, whether or not the commerce has effects within the State.’”³⁹

Under controlling Ninth Circuit precedent, the CCPA violates the dormant Commerce Clause’s ban on regulation of wholly out-of-state conduct. Just as in *Sam Francis*, the Act applies to sales and contracts that are wholly out-of-state. Unlike cases involving “products that are brought into or are otherwise within the borders of the State,”⁴⁰ the CCPA governs what businesses must do with “personal information” that has *left* California’s borders and is physically stored in other states—even businesses that merely receive “personal information” from another out-of-state entity.⁴¹ In *Daniels Sharpsmart v. Smith*, the Ninth Circuit addressed a similar circumstance: “we are faced with an attempt to reach beyond the borders of California and control transactions that occur wholly outside of the State after the material in question—medical waste—has been removed from the State.”⁴² The Ninth Circuit held the fact the medical waste originated in-state did not allow California to “regulate waste treatment” after it was transported outside the state.⁴³

That is exactly what the CCPA does here as applied to certain out-of-state businesses. The mere fact that the “personal information” at issue originated from California is an insufficient nexus to justify California regulating wholly out-of-state conduct. The CCPA’s downstream regulation of data processors and other third parties who contract with out-of-state businesses that “collect” the “personal information” of California residents is unconstitutional because it directly regulates wholly out-of-state commerce, including wholly out-of-state sales where the only contracts are between out-of-state entities. It is an insufficient jurisdictional hook to link this to

³⁷ *Daniels Sharpsmart, Inc. v. Smith*, 889 F.3d 608, 614-15 (9th Cir. 2018) (cleaned up).

³⁸ *Id.* at 615 (citing *Sam Francis Found. v. Christies, Inc.*, 784 F.3d 1320, 1322 (9th Cir. 2015) (en banc)); *Ass’n for Accessible Meds. v. Frosh*, 887 F.3d 664, 674 (4th Cir. 2018).

³⁹ *Sam Francis Found.*, 784 F.3d at 1323-24 (quoting *Healy*, 491 U.S. at 336).

⁴⁰ *See Daniels Sharpsmart*, 889 F.3d at 615.

⁴¹ The Act on its face also appears to regulate contractual agreements between wholly out-of-state entities. *See* Cal. Civ. Code § 1798.140(v). The CCPA also contains a provision that incentivizes covered “businesses” to include provisions in contracts with service providers effectively dictated by the Act. *See id.* § 1798.140(w)(2). It does this to bring these outside entities within the scope the statute by effectively mandating that these “service providers” agree to a contractual term that operates as a jurisdictional hook and ensures that these entities will be held responsible for CCPA compliance.

⁴² *Daniels Sharpsmart*, 889 F.3d at 615.

⁴³ *Id.* at 616. *Cf. Ass’n for Accessible Med.*, 887 F.3d at 672 (striking down Maryland statute that “effectively seeks to compel manufacturers and wholesalers to act in accordance with Maryland law outside of Maryland”).

the mere fact that the truthful information came from a California resident who was at that time located in California when it was collected.

California “may not project its legislation into other states,” and it may not control conduct beyond the boundaries of the State.⁴⁴ Such extraterritorial regulation categorically violates the dormant Commerce Clause.⁴⁵ California may not project its preferred law and policy outside of California to directly regulate the conduct and contractual arrangements between wholly out-of-state entities. California may not control the out-of-state use and sale of lawfully obtained information, regardless of whether the information was sent from California by a California resident. And California may not micromanage the training and record-retention practices of out-of-state entities, particularly those with tenuous, at best, contacts with the state.

B. Only the Federal Government May Regulate the Internet.

The CCPA is also unconstitutional because the U.S. Constitution’s Commerce Clause categorically bars state-level regulation of the Internet. The Supreme Court has long made clear that certain subjects require uniform national regulation.⁴⁶ This strand of case law, whether rooted in the very structure of the federal Constitution or the Commerce Clause, suggests that the power to regulate certain subjects is categorically reserved exclusively for the federal government, *i.e.*, state regulation of these subjects is categorically prohibited.⁴⁷ As numerous federal courts have explained, the Internet is the type of subject that, by necessity, must only be regulated by the federal government.⁴⁸ Put simply, “the unique nature of cyberspace necessitates uniform national treatment and bars the states from enacting inconsistent regulatory schemes.”⁴⁹

⁴⁴ *Brown-Forman Distillers*, 476 U.S. at 582.

⁴⁵ See *Healy*, 491 U.S. at 336 (state statute is invalid per se if practical effect is extraterritorial). Strict scrutiny applies to any State attempt to “control conduct beyond the boundary of the state,” *id.* at 336–37, “whether or not the commerce has effects within the State,” *Edgar v. MITE Corp.*, 457 U.S. 624, 642–43 (1982).

⁴⁶ See *Cooley v. Bd. of Wardens*, 53 U.S. (12 How.) 299, 319 (1852) (“Whatever subjects of this power are in their nature national, or admit only of one uniform system, or plan of regulation, may justly be said to be of such a nature as to require exclusive legislation by Congress.”). See generally *South Dakota v. Wayfair, Inc.*, 138 S. Ct. 2080, 2090 (2018) (discussing *Cooley*); *Korab v. Fink*, 797 F.3d 572, 594 (9th Cir. 2014) (Bybee, J., concurring).

⁴⁷ See *Cooley*, 53 U.S. (12 How.) at 319; *Japan Line, Ltd. v. Cnty. of L.A.*, 441 U.S. 434, 457 (1979) (“The problems to which appellees refer are problems that admit only of a federal remedy. They do not admit of a unilateral solution by a State.”) (cleaned up).

⁴⁸ See, e.g., *Am. Booksellers Found.*, 342 F.3d at 104 (“We think it likely that the internet will soon be seen as falling within the class of subjects that are protected from State regulation because they imperatively demand a single uniform rule.”) (cleaned up); *Am. Libraries Ass’n v. Pataki*, 969 F. Supp. 160, 183 (S.D.N.Y. 1997) (“The Internet . . . requires a cohesive national scheme of regulation so that users are reasonably able to determine their obligations. . . . Haphazard and uncoordinated state regulation can only frustrate the growth of cyberspace. The need for uniformity in this unique sphere of commerce requires that New York’s law be stricken as a violation of the Commerce Clause.”); *ACLU v. Johnson*, 194 F.3d 1149, 1162 (10th Cir. 1999) (“[C]ertain types of commerce have been recognized as requiring national regulation. The Internet is surely such a medium.” (citations omitted)).

⁴⁹ *Am. Libraries Ass’n*, 969 F. Supp. at 184; see also *Huddleston & Adams*, *supra* note 25, at 7–8, 12.

C. CCPA's Burdens on Interstate Commerce Vastly Outweigh Putative Local Benefits.

As the Supreme Court recently reaffirmed: “States may not impose undue burdens on interstate commerce.”⁵⁰ As explained below, even if the CCPA did not violate the dormant Commerce Clause’s *per se* bar against extraterritorial regulations, it should be stricken because the concrete real-world burdens it places on interstate commerce are clearly excessive in relation to its putative local, purely speculative “privacy” benefits to California consumers.⁵¹

1. *The CCPA’s Local Benefits Are Speculative and Illusory.*

Protecting citizens’ privacy is, in the abstract, a legitimate state interest. But the extent to which the CCPA furthers that interest is unclear. To begin with, a host of state and federal statutes already address particularly important privacy-related matters. Examples of such laws include the Gramm-Leach Bliley Act (“GLBA”), Children’s Online Privacy Protection Act (“COPPA”), Fair Credit Reporting Act (“FCRA”), Driver’s Privacy Protection Act (“DPPA”), Health Insurance Portability and Accountability Act (“HIPAA”), the California Financial Information Privacy Act (“CFIPA”), Confidentiality in Medical Information Act (“CMIA”), Student Online Personal Information Protection Act (“SOPIPA”), and the Insurance Information Privacy Act (“IIPA”). In addition, the CCPA may actually facilitate privacy violations. As one commenter explained: “Consider an abusive relationship: A consumer’s safety or confidentiality may be placed at risk if his/her personal information is revealed as part of another consumer’s access request. . . . Scenarios for other compromises to consumer safety and protection are limitless.”⁵²

The CCPA’s alleged local benefits are speculative and abstract. For instance, according to the Initial Statement of Reasons “Summary of Benefits”:

Privacy is one of the inalienable rights conferred on Californians by the state Constitution. The CCPA enumerates specific privacy rights. In giving consumers greater control over their personal information, the CCPA, operationalized by these regulations, mitigates the asymmetry of knowledge and power between individuals and businesses. This benefits not only individuals, but society as a whole. The empowerment of individuals to exercise their rights is particularly important for a democracy, which values and depends on the autonomy of the individuals who constitute it.⁵³

Indeed, the SRIA made no effort to quantify the value California *consumers* place on the privacy rights granted by the CCPA, instead attempting to estimate the value of the data to the companies that collected it using average revenue per user (“ARPU”).⁵⁴ As the SRIA states:

The CCPA’s benefits to consumers derive from the privacy protections granted by the law. These protections . . . give consumers the right to assert control over the use of their personal information. The economic value to consumers of these

⁵⁰ *Wayfair*, 138 S. Ct. at 2091 (citing *Pike v. Bruce Church, Inc.*, 397 U. S. 137, 142 (1970)).

⁵¹ See *Pike*, 397 U.S. at 142.

⁵² Perkins Coie Comments (General Industry) at 8 (CCPA00000966).

⁵³ ISOR at 2.

⁵⁴ See SRIA at 12–15.

protections can be measured as the total value of consumers' personal information, which they can choose to prevent the sale of or even delete. *Although the subjective value of this information to consumers is generally agreed to be great*, it is extremely difficult to quantify the precise value of consumers' personal information in the marketplace and estimates can vary substantially.⁵⁵

Put different, the putative value of the claimed local benefits to the *consumers* who purportedly benefit from the law is entirely subjective and unsupported by empirical research or data. Nor is it even clear how many Californians will exercise their rights under the CCPA. And as the SRIA recognizes: “consumers only receive maximal benefits if they choose to exercise the privacy rights given to them and not everyone is likely to do so[.]”⁵⁶

2. *The CCPA Substantially Burdens Interstate Commerce.*

Any putative privacy benefits flowing from the CCPA are inconsequential in relation to the severe burdens it imposes on interstate commerce. “Balanced against the limited local benefits resulting from the . . . [CCPA] is an extreme burden on interstate commerce. . . . [The CCPA] casts its net worldwide[.]”⁵⁷ The CCPA substantially burdens interstate (and indeed international) commerce in myriad ways, imposing draconian compliance costs on hundreds of thousands of in-state (and out-of-state) businesses and threatening thousands of jobs. Indeed, California's own Economic Impact Statement found that the CCPA will “eliminate[.]” nearly 10,000 jobs in California alone.⁵⁸ As the SRIA found, “[s]ome industries will be forced to completely revise their business models” because of the CCPA.⁵⁹ As the Chief Economist for California's Department of Finance noted, “[t]he SRIA estimates that the initial cost of compliance may be up to \$55 billion”⁶⁰—and that staggering figure is for California alone. The SRIA did not even attempt to evaluate the CCPA's economic impact on out-of-state and overseas businesses.⁶¹ “Small firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises.”⁶² The CCPA regulations also threaten to “creat[e] additional barriers to entry for future [out-of-state] competitors [with California companies] considering entering into the California market.”⁶³

As numerous comments have made clear, the practical compliance challenges are astronomical for both in-state *and* out-of-state businesses that meet the low compliance thresholds.⁶⁴ Even comparatively small businesses (such as convenience stores and restaurants)

⁵⁵ *Id.* at 12.

⁵⁶ *Id.* at 15; see Huddleston & Adams, *supra* note 25, at 5 (explaining that “the potential benefits of . . . [state privacy] laws are not readily calculable as an empirical matter and are, as a result, more difficult to discern.”).

⁵⁷ See *Am. Libraries Ass'n*, 969 F. Supp. at 179.

⁵⁸ Economic Impact Assessment, <http://bit.ly/2OM3PIm>.

⁵⁹ See SRIA at 30.

⁶⁰ Letter from Irena Asmundson, Chief Economist, Cal. Dep't of Fin., to Stacey Schesser, at 2 (Sept. 16, 2019) (Appendix B to ISOR), *available at* <http://bit.ly/2QQozBq>.

⁶¹ SRIA at 21 (“The economic impact of the regulations on these businesses located outside of California is beyond the scope of the SRIA and therefore not estimated.”).

⁶² *Id.* at 31.

⁶³ *Id.* at 32 (Aug. 2019)

⁶⁴ See, e.g., California Chamber of Commerce Comments (CCPA00000067-CCPA00000116); Toy Association Comment (CCPA00000185-CCPA00000196); BakerHostetler Comment (CCPA00000273-CCPA00000284); CTIA

with any significant online presence may be compelled to comply. Among other things, the CCPA creates perverse incentives for out-of-state companies that may potentially have any contact with a California consumer involving the collection of information to avoid expanding beyond the \$25-million-per-year-in-gross-revenue threshold requiring CCPA compliance. Alternatively, CCPA incentivizes out-of-state companies to stop selling to California customers or, alternatively, block California customers from their websites. The CCPA threatens to deter and punish innovation as well, particularly with respect to small startups ill-equipped to bear its compliance costs.

The CCPA's burdens on interstate commerce are compounded by the Sisyphean practical challenges companies face in attempting to comply not only with the CCPA but also GDPR and other state privacy laws, which differ in salient respects from the CCPA. For instance, as the AG has been made aware, the CCPA diverges from GDPR in many material respects.⁶⁵ Indeed, the Initial Statement of Reasons itself highlights the "incompatibility" of CCPA with GDPR, noting that they "have different requirements, different definitions, and different scopes."⁶⁶ In addition, the CCPA is inconsistent with federal law such as COPPA, as commenters have previously explained.⁶⁷ Further, other states have followed in California's footsteps to add their own gloss on state-level Internet regulation.⁶⁸

Comment (CCPA00000393-CCPA00000409); AAF, ANA, IAB, and NAI Comment (CCPA00000432-CCPA00000442); ACRO Comment (CCPA00000444-CCPA00000446); Randall-Reilly Comment (CCPA00000483-CCPA00000484); Mayer Brown Comment (CCPA00000522-CCPA00000527); Mapbox Comment (CCPA00000535-CCPA00000540); Auto Alliance Comment (CCPA00000568-CCPA00000586); SIIA Comment (CCPA00000755-CCPA00000756); ESA Comments (CCPA00000741-CCPA00000747); HERE Comment (CCPA00000850-CCPA00000855); ITIF Comment (CCPA00000873-CCPA00000885); Perkins Coie Comments (Financial Services Industry) (CCPA00000927-CCPA00000951); Perkins Coie Comments (General Industry) (CCPA00000952-CCPA00000968); Engine Comment (CCPA00000991-CCPA00000995); U.S. Chamber of Commerce Comment (CCPA00001108-CCPA00001118); Orange County Business Council Comment (CCPA00001370-CCPA00001371); Software Alliance Comments (CCPA00001373-CCPA00001380); Innovative Lending Platform Association Comment (CCPA00001383-CCPA00001385).

⁶⁵ See Comparing Privacy Laws: GDPR vs. CCPA (CCPA00000782-CCPA00000823); see also Jehl & Friel, CCPA and GDPR Comparison Chart, available at <http://bit.ly/34qefV2>.

⁶⁶ ISOR at 44.

⁶⁷ See Toy Association Comment (CCPA00000185-CCPA00000196); see also ACRO Comment (CCPA00000444-CCPA00000446).

⁶⁸ See IAPP, State Comprehensive-Privacy Law Comparison, <http://bit.ly/2OgTcyl>; Akin Gump, Comparison Chart of Pending CCPA and GDPR-Like State Privacy Legislation (May 2019), available at <http://bit.ly/2OavEv8>; see also Huddleston & Adams, *supra* note 25, at 8.

IV. THE CCPA VIOLATES THE FIRST AMENDMENT.

The CCPA is also unconstitutional because, as First Amendment law scholars and practitioners have explained, some of the CCPA's provisions violate companies' First Amendment rights.⁶⁹ Their insightful commentary on the unconstitutionality of the CCPA under Supreme Court cases such as *Sorrell v. IMS Health Inc.*⁷⁰ is part of the record in this rulemaking.⁷¹

As these First Amendment experts point out, the CCPA “violates settled First Amendment principles by restricting the dissemination of accurate, publicly available information”⁷²:

The CCPA's provisions restricting the dissemination of publicly available information are unconstitutional for three independent reasons. First, these limitations are content-based restrictions on speech that are not justified by a sufficiently weighty governmental interest to satisfy strict scrutiny, or even intermediate scrutiny. Second, the regulation limiting dissemination of information publicly disclosed by government agencies is unconstitutionally vague. Third, the CCPA's restrictions unconstitutionally distinguish among speakers and among different types of speech.⁷³

To date, the California Legislature has refused to legislatively remedy the Act's myriad constitutional shortcomings.

Among other constitutional flaws, “[t]he CCPA on its face favors some speakers and some uses of information while disfavoring others. It also allows consumers to use the power of the State to suppress particular speakers and facts. And it does so in a frankly content-based way[.]”⁷⁴ As these constitutional experts explain: “[T]he law's practical effect is to enable California residents to suppress the communication of particular facts. Moreover, the Act authorizes consumers to ban speech selectively, allowing some businesses to speak about them while silencing others. . . . Indeed, the Act appears designed to encourage . . . [content and viewpoint] censorship.”⁷⁵ “This creates the potential for groups of consumers to burden disproportionately the speech of unpopular speakers, effectively censoring their communications in a manner that violates First Amendment principles.”⁷⁶

As discussed above, the CCPA's purported local privacy benefits are highly abstract and uncertain, at best, and greatly outweighed by the excessive burdens on interstate commerce that California's extraterritorial Internet regulation imposes. Nor can these putative privacy benefits justify the CCPA's unconstitutional restrictions on truthful speech. As First Amendment experts

⁶⁹ See Andrew Pincus, Miriam Nemetz, & Eugene Volokh, *Invalidity Under the First Amendment of the Restrictions on Dissemination of Accurate Publicly Available Information Contained in the California Consumer Privacy Act of 2018* (Jan. 24, 2019) [hereinafter “Mayer Brown Memo”].

⁷⁰ 564 U.S. 552 (2011).

⁷¹ See CCPA00000757-CCPA00000769.

⁷² Mayer Brown Memo at 1.

⁷³ *Id.* at 4.

⁷⁴ *Id.* at 11.

⁷⁵ *Id.* at 12.

⁷⁶ *Id.* at 13.

have explained: “The government cannot defend a speech restriction ‘by merely asserting a broad interest in privacy.’ ‘[P]rivacy may only constitute a substantial state interest if the government specifically articulates and properly justifies it.’ ”⁷⁷ California has utterly failed to do so here.⁷⁸

V. THE CCPA VIOLATES DUE PROCESS FOR FAILURE TO GIVE FAIR NOTICE OF PROHIBITED OR REQUIRED CONDUCT.

Businesses have a due-process right to fair notice of the CCPA’s requirements.⁷⁹ The AG bears the responsibility to promulgate clear, unambiguous standards.⁸⁰ To provide sufficient notice, a statute or regulation must “give the person of ordinary intelligence a reasonable opportunity to know what is prohibited so that he may act accordingly.”⁸¹ Due-process requirements are heightened where, as here, civil penalties may be imposed. Corporations should not be subject to civil penalties that are not clearly applicable by either statute or by regulation.⁸²

The CCPA and its implementing regulations fail this test. To begin with, it is impossible for many companies to predict whether they are even subject to the CCPA. For example, how is a company that currently has an annual gross revenue of \$24 million in 2019 supposed to predict or know whether its annual gross revenue in 2020 will exceed \$25 million, thereby triggering CCPA compliance obligations? Similarly, how are small businesses supposed to reliably determine whether they have received “personal information” from “50,000 or more consumers, households, or devices” on an annual basis and thus must comply with the CCPA? Indeed, as one commenter aptly pointed out:

Without access to geolocation data a business cannot determine if information collected via mobile phone or a portable personal computer was collected while the individual was in California. If an individual in California attempts to shield their location from the business (ex. through use of a virtual private network (VPN)), and the business has no other indication the individual is in California, will the business be in violation of the law if it collects or sells that information? This also raises questions over whether it is constitutionally permissible for California to regulate business that occurs in other states or as part of interstate commerce.⁸³

These problems are exacerbated by the fact that neither the statute nor the regulations define “doing business” in California, leaving companies in the dark as to whether they must meet the CCPA’s onerous compliance requirements or risk enforcement actions. That is flatly unconstitutional.

⁷⁷ *Id.* at 6 (quoting *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1235 (10th Cir. 1999)).

⁷⁸ *See id.* at 6-9.

⁷⁹ *See Fed. Comm’n Comm’n v. Fox TV Stations, Inc.*, 567 U.S. 239, 253 (2012) (“A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required.”); *Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156, 2167 (2012).

⁸⁰ *See Marshall v. Anaconda Co.*, 596 F.2d 370, 377 n.6 (9th Cir. 1979); *see also Ga. Pac. Corp. v. OSHRC*, 25 F.3d 999, 1005–06 (11th Cir. 1994) (ascertainable certainty standard); *Gen. Elec. Co. v. Envtl. Protection Agency*, 53 F.3d 1324, 1329 (D.C. Cir. 1995) (same).

⁸¹ *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972); *see Connally v. Gen. Constr. Co.*, 269 U.S. 385, 391 (1926).

⁸² *See, e.g., United States v. Trident Seafoods Corp.*, 60 F.3d 556, 559 (9th Cir. 1995).

⁸³ AFSA Comment at CCPA00000005.

VI. THE CCPA, IF ENFORCED, WILL IRREPARABLY HARM COVERED BUSINESSES, CONTRARY TO THE PUBLIC INTEREST

The CCPA, if enforced, will cause irreparable harm to businesses, as recognized under equity. *First*, covered businesses will suffer irreparable harm in the form of un-recoupable compliance costs.⁸⁴ *Second*, the CCPA’s violations of the dormant Commerce Clause and businesses’ First Amendment rights is also irreparable harm.⁸⁵ “[E]nforcement of an unconstitutional law is always contrary to the public interest.”⁸⁶ The AG should thus refuse to enforce the CCPA.

For the foregoing reasons, we respectfully submit that the AG should revise the CCPA regulations to comply with statutory and constitutional limits on its authority. If you have any questions about this request, please contact me at [REDACTED]. Thank you for your attention to this matter.

Sincerely,

Americans for Prosperity Foundation
Cardinal Institute for West Virginia Policy
Christopher Koopman
Freedom Foundation of Minnesota
James Madison Institute

Libertas Institute of Utah
Mississippi Center for Public Policy
Mississippi Justice Institute
Pelican Institute
Washington Policy Center

⁸⁴ See *Morales v. Trans World Airlines, Inc.*, 504 U.S. 374, 381 (1992) (holding that a plaintiff would suffer “irreparable harm” if forced to choose to incur either the civil enforcement liability of violating a preempted state law or the costs of complying with the law during the pendency of the proceedings); see also *Chamber of Commerce v. Edmondson*, 594 F.3d 742, 770–71 (10th Cir. 2010) (“Imposition of monetary damages that cannot later be recovered for reasons such as sovereign immunity constitutes irreparable injury.”).

⁸⁵ *Elrod v. Burns*, 427 U.S. 347, 373 (1976) (holding that deprivation of constitutional rights “unquestionably constitutes irreparable harm”); see *Am. Libraries Ass’n*, 969 F. Supp. at 168 (“Deprivation of the rights guaranteed under the Commerce Clause constitutes irreparable injury.”).

⁸⁶ *Gordon v. Holder*, 721 F.3d 638, 653 (D.C. Cir. 2013); see also *Legend Night Club v. Miller*, 637 F.3d 291, 302–03 (4th Cir. 2011) (state “is in no way harmed by issuance of an injunction that prevents the state from enforcing unconstitutional restrictions.”).

Message

From: Matt Kownacki [REDACTED]
Sent: 12/7/2019 12:01:36 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: AFSA-CFSA comment letter
Attachments: AFSA-CFSA comment letter - CCPA Regs.pdf

On behalf of the American Financial Services Association and the California Financial Services Association, attached is a comment letter regarding the proposed CCPA regulations.

Thank you for your consideration of our comments.

Matt Kownacki
Director, State Research and Policy
American Financial Services Association
[REDACTED]



December 6, 2019

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

Re: CCPA proposed regulations

On behalf of the American Financial Services Association (“AFSA”)¹ and the California Financial Services Association (“CFSA”),² thank you for the opportunity to provide comments on the regulations proposed by the Office of the Attorney General (“OAG”) to implement the California Consumer Privacy Act (“CCPA”). We appreciate your consideration of our comments during the preliminary rulemaking process and reiterate our previous concerns about vague terms and the substantial burdens these regulations place on covered entities.

We appreciate the OAG’s efforts to provide guidance to businesses on how to comply and to clarify the law’s requirements through the implementing regulations. However, though our members share the state’s goal of protecting the privacy of consumers, promoting understanding by consumers of the personal information about them that is collected, sold, and shared for a business purpose, and guarding personal information from unauthorized access, we have significant concerns about the regulations as proposed. There are certain areas where we believe consumers and the business community would benefit from increased clarity and certainty.

Enforcement Delay

Although the effective date and issues of enforcement are not addressed directly in the proposed regulations, our members believe that some clarity in this area is warranted. The CCPA was largely effective on September 23, 2018, and will be operative on January 1, 2020, and enforceable by the OAG on July 1, 2020. It appears that the OAG intends for the regulations to also be enforceable on July 1, 2020, which is likely to be the earliest date that the regulations could be made effective. A delayed enforcement date would give affected businesses the opportunity to evaluate the specific requirements set forth in the regulations and implement new systems and processes needed to be fully in compliance with the law.

¹ Founded in 1916, the American Financial Services Association (AFSA), based in Washington, D.C., is the primary trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including direct and indirect vehicle financing, traditional installment loans, mortgages, payment cards, and retail sales finance. AFSA members do not provide payday or vehicle title loans.

² The California Financial Services Association is a non-profit trade association representing major national and international corporations and independent lenders with operations in the State of California to provide a broad range of financial services, including consumer and commercial loans, retail installment financing, automobile and mobile home financing, home purchase and home equity loans, credit cards, and lines of credit.

In addition, we request that the OAG include in the final regulations a statement to the effect that any enforcement actions will be based on conduct that takes place after the statutory enforcement date of July 1, 2020, or such later date as the regulations may become enforceable. In making this request, we note that the proposed regulations address all the major aspects of the CCPA: how to provide notices, content of the privacy policy, the process for handling submitted requests, verification, and calculating the value of consumer data. Without having final regulations in place to govern compliance, businesses lack clarity that the solutions they are readying for January 1, 2020, will, in fact, meet regulatory requirements. We request that businesses have all the applicable rules and requirements, in final form, with a reasonable timeframe to achieve compliance, before their actions can be determined to be unlawful. Recognizing the time necessary for the OAG to draft and implement comprehensive regulations, we believe that the outlined enforcement delay would be consistent with the legislature’s intended delayed enforcement date.

§ 999.301. Definitions

Section 999.301(h) broadly defines “household” as *a person or group of people occupying a single dwelling*. Such a broad definition based merely on temporary occupancy of a dwelling rather than a requirement that persons be related and domiciled, as defined in Section 17014 of Title 18 of the California Code of Regulations, would sweep in groups in living arrangements who should not have access to the personal information of others, such as multiple roommates linked by mutual tenancy, a landlord and tenant, persons using a house sharing app for the weekend, and at the most extreme end, all the residents of a college dormitory. Because this broad access would be contrary to the purpose of the CCPA, we recommend striking the requirement that businesses accept requests from household members—except those from a parent or guardian on behalf of a minor—or, at the very least, that persons whose only relationship is that they share a housing unit should not be included in the definition of household. Instead, we recommend that the OAG consider adopting a definition of household similar to the definition of “family group” used by the U.S. Census Bureau, which defines a family group as “any two or more people (not necessarily including a householder) residing together, and related by birth, marriage, or adoption.”³

Section 999.301(n) provides a definition of “request to know” that includes *any or all of* six categories of information. Section 999.313 describes different processes depending on whether a consumer is requesting specific pieces of information or categories of information. Providing this kind of flexibility was not envisioned in the statute, and many of our members have already started building solutions that do not afford multiple choices of this kind. We request that the OAG clarify that this multi-tier approach is not mandatory and confirm that businesses that build their process to meet the more conservative requirements associated with a request for specific pieces of information will be in compliance with the law.

§ 999.305. Notice at Collection of Personal Information

This section describes a comprehensive, detailed consumer notice, which suggest there may be a specific form notice the OAG might want covered entities to use. If the OAG intends to be more

³ <https://www.census.gov/programs-surveys/cps/technical-documentation/subject-definitions.html#familyhousehold>.

prescriptive regarding the notice requirements, then we request it release a sample form and that the use of such sample form of notice provide a safe harbor for compliant businesses. As many covered entities are likely already working on their own notice in advance of the impending compliance date, we request that notices substantially similar to the sample form notice also be deemed compliant.

Both the statute and the proposed regulation require a collecting business to notify consumers of the categories of personal information to be collected and the purposes for which they will be used. The statute specifies that disclosures required by section 1798.100 must be provided in accordance with the requirements of section 1798.130. The only part of section 1798.130 that a business can look to for instruction on providing the advance notice is section 1798.130(a)(5), which specifies the information that must be in the online privacy policy. Accordingly, businesses that rely on their online privacy policies to provide advance notice should be considered in compliance with the statute. We request that the OAG remove any language from the draft regulations that suggests otherwise.

Section 999.305(a)(2) requires a business present a notice that is “understandable to an average consumer.”⁴ While we support the goal of clear communications to consumers, the proposed standard is vague and requires additional guidance. If the OAG does not intend to provide a sample notice, we request a clearer and more measurable standard.

Section 999.305(a)(3) requires a business to obtain explicit consent from the consumer to use personal information for a new purpose that may not have been originally disclosed. This requirement goes beyond the existing statutory requirements, which require only notice, and as noted above, could be provided through changes to the online privacy policy. Further, a requirement to obtain explicit consent for new uses would unnecessarily encourage covered entities to draft broad disclosure language that would cover as wide a range of uses as possible. Such disclosures would be longer and less meaningful for consumers seeking to truly understand how their personal information may be used.

Section 999.305(d) restricts the sale of personal information collected from a source other than the consumer unless the business provides a notice at collection to the consumer or contacts the source, but this requirement has no statutory basis in the CCPA and is overly burdensome for businesses that share any information with third parties.

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

Section 999.306(a)(1) arguably suggests that a business that does not currently sell personal information must, nevertheless, build an intake function to collect opt outs from consumers who would like to prevent their personal information from being sold in the future.⁵ This is an unreasonable outcome for businesses that do not sell and could create a perverse incentive for businesses to decide to sell since they must build the opt-out infrastructure regardless of their

⁴ This same terminology is repeated in §§ 999.306, .307, .308, and the comment applies equally to each section.

⁵ Stating that “the purpose of the notice of right to opt-out of sale of personal information is to inform consumers of their right to direct a business that sells (or may in the future sell) their personal information to stop selling their personal information, and to refrain from doing so in the future.”

current practices. Further, recognizing that the statute does not speak to such a requirement, the OAG should remove from the proposed regulations all such forward looking obligations.

Section 999.306(b)(2) requires a business that *substantially* interacts with consumers offline to also provide the opt-out notice by an offline method. This vague standard does not define what qualifies as substantially offline to trigger the offline notice requirement.

§ 999.307. Notice of Financial Incentive

We request confirmation that businesses that do not offer financial incentives or a price or service difference in exchange for retention or sale of a consumer's personal information do not have to provide the Notice of Financial Incentive or related information in the privacy policy.

§ 999.308. Privacy Policy

Section 999.308(b)(1)(c) requires that the privacy policy include a description of "the process the business will use to verify the consumer request." For security reasons, this requirement should be removed. Describing the process for verification invites fraudsters to circumvent the measures that businesses must put in place to protect consumers. There is minimal additional consumer benefit to publishing the details of how the verification process works when businesses have a legitimate concern that providing too much information in a publicly facing document will put consumer security at risk.

We recommend removing Section 999.308(b)(1)(d)(2), which requires that the privacy policy include for each category of personal information collected, the categories of sources from which each category was collected, the business or commercial purpose for collecting each category, and the categories of third parties with whom the business shares each category of personal information. This disclosure requirement is overly burdensome, requiring businesses to specifically tie source, use, and recipients to each category of personal information collected, to no good effect, and attempts to impose a requirement on all personal information collected when the statute specifies that this degree of granularity only applies to personal information that the business has sold.⁶

Section 1798.115 treats information that the business sold differently from both the personal information that the business collected and the personal information that the business disclosed for a business purpose. Section 1798.115(a)(2) specifically states with regard to the personal information sold that the business must disclose "the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold." This different treatment is a logical consequence of the fact that the statute gives consumers the right to opt out of sale. A consumer exercising that right has an interest in knowing which information is sold to which third party. Because there is no right to opt out of collection or sharing for a business purpose, a lower level of granularity will provide a less complex and more meaningful disclosure to the consumer.

⁶ Section 1798.110 of the statute lists four categories of information that a business must provide regarding personal information the business has collected. Unlike Section 1798.115, this section does not require that the categories be cross-referenced against each other. In fact, cross-referencing the categories would create a lengthy and confusing document.

Section 999.308(b)(3) requires that the privacy policy for all covered entities disclose that a consumer has a right to opt-out of the sale of their personal information. If a business does not currently sell personal information, it should not be required to include such a disclosure in its privacy policy. The exemption provided in 999.306(d)(1) only applies if the business's privacy policy states that the business "does not and will not sell" the personal information. Without the forward-looking statement, a business that does not currently sell personal information would be required to provide the notice of opt out. This disclosure would be unnecessary, irrelevant to the business, and may lead consumers to wrongly believe that the business does in fact sell personal information when it does not.

Section 999.308(b)(5)(a) requires that a privacy policy explain how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf, but the proposed regulations do not make clear the level of information that a business must provide regarding the designation. For example, it is not clear whether a business must describe the requirements regarding agent request verification found at § 999.326, or whether they may be covered when a request is made. It is also unclear whether businesses may require particular forms or indicia of authority, such as powers of attorney.

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

Section 999.312(f) assigns to businesses the responsibility for redirecting responses that are not submitted through established channels and for advising a consumer how to remedy a deficient request. The section raises practical questions regarding the requirements for timing and tracking and should be removed.

The statute requires that a business implement at least two methods for submitting requests and, importantly, provide notices to consumers explaining how to make requests. Requests submitted outside of the options provided cannot be addressed in an efficient fashion, creating risk that the business cannot meet the deadlines established by the statute. For example, a request e-mailed to a local branch may not be timely routed to the appropriate location for response, but a business has limited options when it cannot provide a response within the 45 days allowed under the statute.⁷ Without the ability to control how requests are submitted, businesses may be challenged both to provide the extension notice within 45 days and to provide the response within 90 days.

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

§ 999.313(c)(5) requires a business, when a request to know is denied based on a conflict with federal or state law, to disclose to the consumer the basis for the denial. There may be times when the precise legal basis cannot be provided to the consumer because such a disclosure would itself violate law. To avoid this potential scenario, we suggest that the OAG include language in this paragraph clarifying that disclosing the existence of the conflict, without detailing the particular law or exception at issue, will be an adequate response under the regulation.

⁷ The regulation specifies that a business must respond to a request within 45 days, beginning on the day the business receives the request. If necessary, the business "may take up to an additional 45 days to respond to the consumer's request, for a maximum total of 90 days from the day the request is received." § 999.313(b).

Section 999.313(c)(6) requires a business to use reasonable security measures when transmitting personal information to the consumer. Our member companies recognize the importance of protecting personal information when it is being transmitted, and we request that compliance with this requirement constitute a safe harbor to any cause of action that alleges that the transmission resulted in unauthorized access, acquisition, destruction, modification or disclosure of personal information. Understanding that some consumers may choose to have their personal information delivered by mail, we request that the OAG confirm that delivery through the mail at the request of the consumer absolves the business of liability for any unauthorized access, acquisition, or disclosure of personal information that may occur after the personal information is placed in the mail. Moreover, we request that the OAG confirm that using security measures that the business uses in standard operating procedures, such as e-mail encryption and Secure Message Delivery, will meet this requirement and constitute reasonable security procedures and practices under the CCPA.

Section 999.313(c)(7) states that if a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal. We request verification that while a financial institution subject to the Gramm-Leach Bliley Act (GLBA) may use the secure portal for this purpose, it would not be required to deliver non-GLBA data through the consumer's GLBA account portal.

Section 999.313(d)(1) requires that if a business cannot verify the identity of a requestor seeking deletion it shall instead treat the request as a request to opt out of sales. This requirement has no statutory basis, and, in fact, runs counter to the CCPA's principles by giving control over consumer data based on unverified requests. The CCPA treats the right to delete and the right to opt out of sale of personal information as separate requests, with different statute sections and different exceptions. There is no legal basis to convert a deletion request to an unrequested, unrelated action because the requestor's identity could not be verified. If an identity cannot be verified, the only required action should be to inform the requestor of that fact.

Section 999.313(d)(3) allows a business to delay compliance with a request to delete, where personal information is stored in an archive or backup, until the archive or backup is next accessed. This requirement fails to recognize the technological complexity of database systems and the purpose of archives and backups. Information is generally archived with an established destruction date, determined by the type of data, when a business needs to retain it to meet business or legal requirements and maintain compliance with other state or federal laws. Backups, primarily used for disaster recovery, may never be accessed but may be overwritten on a regular schedule to retain current information. Without more clarity around the word "access," this language could require deletion when unrelated information is automatically added to the database or the database is accessed for purposes of maintenance or recovery.

A requirement to delete triggered by any access to the archive or backup is overly burdensome for businesses, as the next access to the archive or backup may be for unrelated information and not for the specific personal information requested. Accessing the archive or backup for other business needs wholly unrelated to the data subject to CCPA should not trigger a deletion requirement. We request that the deletion requirement for personal information in an archive or

backup system only trigger in the event that the business accesses such data with the intent to use it in the course of its day to day functions.

Section 999.313(d)(4) requires that a business specify the manner in which it has deleted the requestor's personal information. This requirement is burdensome, vague, and has no statutory basis. Deletion of information, especially in large businesses, can be complicated, involving several systems and business units, and a detailed description of this process does not serve the consumer. We recommend that this section only require a business to inform a consumer that the personal information has been deleted, or if it cannot be deleted, the reason why, consistent with the requirements of Section 999.313(d)(6).

§ 999.318. Training; Record-keeping

Section 999.317(g) requires a business that alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers to compile certain metrics regarding consumer requests and publish these metrics in the business' privacy policy. This section provides no further guidance as to how the 4,000,000 consumer threshold is calculated. We request that the OAG provide such guidance and that the guidance clarify that the calculation should not include consumers whose information is exempt from the CCPA's disclosure and deletion requirements, such as information subject to the Gramm-Leach Bliley Act, as including such information would skew the results and make the data effectively meaningless. Additionally, the public disclosure of these metrics would not further the purposes of the CCPA and could present fraud or cybersecurity risks. Instead, we recommend that these metrics be provided to the OAG upon request.

§ 999.318. Requests to Access or Delete Household Information

Section 999.318(b) requires a business to disclose or delete personal information for all members of a household if jointly requested. Businesses will not, however, be able to verify whether all members of a household agree to the request, particularly because the business has no practical way to know who all the members of the household are and to verify whether a request was actually received from all members. The broad definition of household members, in that it includes individuals of all ages and physical or mental capacity, regardless of relationship, means that a business can never be certain that a request to disclose or delete is made with appropriate authority. As a result, businesses cannot respond affirmatively to such a request, and this provision should be removed from the regulations.

§ 999.325. Verification for Non-Accountholders

Sections 999.325(b)-(d) require different tiers of authentication for right to know requests depending on the specific categories of personal information requested, but most identity verification techniques do not know how many data points will be needed for verification ahead of time, and most third party verification services do not provide this level of differentiation. The multiple verification tiers could increase the potential for mishandling consumer information. The regulations should allow businesses to instead set their own verification standards based on the business' own assessment.

Section 999.325(c) requires that consumers must submit a signed declaration under penalty of perjury to submit a request for specific pieces of personal information. We request further clarification regarding standards for these declarations, including whether the declaration must be notarized.

Accessibility and Language Requirements

The regulations require throughout—999.305(a)(2)c-d; 306(a)(2)c-d; 307(a)(2)c-d; 308(a)(2)c-d—that notices and privacy policies be accessible to customers with disabilities and available in the languages in which the business provides contracts, disclaimers, notices, sales, or other information. For businesses to have more certainty, the OAG should provide some additional clarity on the requirements for accessibility. For example, the regulations should clarify that if the documents are provided on a website that meets accessibility standards such as Web Content Accessibility Guidelines (WCAG) 2.0, it meets this requirement. We further request that the OAG provide additional clarity regarding how to apply the language requirement. For example, financial institutions may take assignment of installment sales contracts negotiated in other languages. Such contracts should not drive the languages for the financial institution’s notices and policies, particularly if the underlying contracts are subject to the GLBA exemption.

Deletion Requests in a 12-month Period

The CCPA, in providing consumers with the right to request their personal information, recognized that identifying and supplying personal data to the consumer places a burden on businesses. The statute requires the business to provide the information not more than twice in a 12-month period.⁸ The information must be provided at no charge to the consumer.⁹ If, however, the consumer makes more than two requests, the business can opt to charge the consumer for the administrative costs of fulfilling the request or refuse to take action if the requests are manifestly unfounded or excessive.¹⁰ This language suggests that more than two requests in a 12-month period can be considered excessive, and a business is not required to take action.

The CCPA does not expressly state that a consumer can only make two deletion requests in a 12-month period. However, for a business, the process of validating a consumer request, searching for personal information, evaluating whether the information is subject to an exception, deleting or destroying data, and responding to the consumer is not less burdensome than the effort that a business must put into responding to a disclosure request, and may actually be more burdensome. Accordingly, we request that the OAG clarify in the regulations that delete requests should be treated in the same manner as disclosure requests, and no more than two in a 12-month period should be required.

Look Back Period

The CCPA provides that a response to a disclosure request “shall cover the 12-month period preceding the business’s receipt of the verifiable request.”¹¹ A business also must include in its

⁸ 1798.100(d), 1798.130(b).

⁹ 1798.100(d); 1798.130(a)(2).

¹⁰ 1798.145(g)(3).

¹¹ 1798.130(a)(2).

online privacy policy “the categories of personal information it has collected about consumers in the preceding 12 months.”¹² This reference to a 12-month look back period is repeated in several other sections of the CCPA as well.

As noted above, the CCPA provides that the law is generally “operative” on January 1, 2020, notwithstanding that many sections became effective immediately upon enactment. The enforcement date adds additional confusion. The various dates for implementation raise questions about how the look back period should be treated when the law becomes enforceable. The OAG’s regulations should clarify that the look back period will not extend farther back than the effective date of the regulations because businesses will not have final and binding guidance for complying with their requirements until that date.

For example, a business is only required to respond to a disclosure request after receiving a verified request. A business cannot receive a verified request until the OAG regulations specify how businesses will determine that a request is valid. Additionally, in response to a disclosure request, a business must identify the information collected in the past 12 months by reference to the definition of personal information.¹³ However, the OAG’s final regulations may modify or expand the definition of personal information and unique identifiers.¹⁴ As a result, businesses will not be able to fully identify and categorize information until final regulations are published. Accordingly, businesses should not be required to look back beyond the effective date of the regulations to respond to a disclosure request.

Thank you in advance for your consideration of our comments. If you have any questions or would like to discuss this further, please do not hesitate to contact Matt Kownacki at AFSA at [REDACTED] or [REDACTED].

Sincerely,

/s/ Matthew Kownacki
Matthew Kownacki
Director, State Research and Policy
American Financial Services Association
919 Eighteenth Street, NW, Suite 300
Washington, DC 20006

/s/ David Knight
David Knight
Executive Director
California Financial Services Association
1127 11th Street, Suite 400
Sacramento, CA 95814

¹² 1798.130(a)(5)(B).

¹³ 1798.130(a)(3)(B); 1798.130(c).

¹⁴ 1798.185(a).



December 6, 2019

Submitted electronically in reference to the matter identified below, via PrivacyRegulations@doj.ca.gov

Subject: Alight Solutions LLC's Comments on:

- **The California Attorney General's ("AG") proposal to adopt sections §§ 999.300 through 999.341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations (CCR) concerning the California Consumer Privacy Act (CCPA) (Published October 11, 2019)**

To Whom It May Concern:

Alight Solutions LLC ("Alight") is a leader in benefits, payroll and cloud solutions, supporting more than 3,250 clients, including 50% of the Fortune 500. On behalf of its clients, Alight serves 26 million people and their family members including more than 5.5 million defined benefit participants, nearly 5 million defined contribution participants, and over 11 million health and welfare plan participants.

We appreciate the Attorney General's effort to provide detailed regulations related to the California Consumer Privacy Act (CCPA), and the opportunity to submit comments. Through the services we provide for our clients and their people we are well-versed in the practical and regulatory factors impacting modern consumers and their data. We believe individual privacy and the security of people's personal information and data are critically important, and support clear standards for all stakeholders. However, we are concerned about cumbersome regulations that will result in confusion for individuals, companies, and regulators. In our view the proposed regulations further complicate the already broad CCPA. The proposed regulations also stretch the applicability of the law beyond the statutory definitions in contravention of California's Administrative Procedure Act ("APA"), CA Gov't Code Sec. 11340 *et seq.* We focus our comments on one of the proposed regulations that we expect could at minimum have unintended negative consequences on businesses, service providers, and consumers.

- I. We urge the AG to strike or clarify Section 999.314(a) related to service providers, which appears to significantly expand who is a covered service provider, create a direct conflict between service providers and any non-"business" client otherwise not covered by CCPA, and potentially subject such non-"business" clients to CCPA's requirements indirectly.**

The definition of "service provider" set forth in Section 1798.140(v) is a person or entity that processes "information on behalf of a **business....**" (emphasis added). Additionally, the term "business" is defined in Section 1798.140(c) to mean a for-profit entity that is covered by CCPA. As a result, an entity providing services to a company that is not a "business" will not be subject to CCPA's service provider requirements. Proposed regulation 999.314(a), however, does away with the "business" limitation in the express terms of the CCPA. As a result, entities not contemplated as "service providers" under the CCPA statute itself may nonetheless be deemed "service providers" for purposes of the regulations. We expect many entities that, for example, provide services to not-for-profits (or state, municipal, or other governmental units), will not be prepared to meet the service provider requirements of CCPA and that there will be conflict and confusion about this expansion. Additionally, the APA, does not seem to grant the AG the authority to enlarge the scope of the CCPA through regulation.

For entities that would not be service providers but for proposed regulation 999.314(a), or entities that are service providers but have clients that are a mix of “business” and non-“business” companies, this provision will either create a conflict with the non-“business” client over the need to comply regarding such client’s population, or effectively subject the non-“business” client to CCPA’s requirements by virtue of the deemed service provider status.

For example, in the event an entity was servicing clients that were not-for-profit companies, those clients may assert that they are not subject to CCPA; which would be accurate under both the text of the CCPA as well as the proposed regulations. The servicing entity would be holding the data of the non-profit clients, but does not own that data and generally would not take independent action regarding that data. However, if the servicing entity were to be deemed a service provider with regards to, in this example, non-profit clients, there may be a conflict between the responsibilities of a service provider under the CCPA and the direction provided by a non-profit client (not subject to the CCPA). The servicing entity would be caught between its own responsibilities under the CCPA and the non-profit client’s position that the CCPA does not apply to the client’s data. If the client directed, for example, that the service provider not respond or take any action on requests related to personal data obtained from that client’s employees, it is unclear how the service provider could assert that such action was required if the CCPA does not apply to the client who owns the data.

In addition to the deemed service provider’s conflicted position, a non-“business” client would be essentially forced to choose between voluntarily following the CCPA requirements despite it not applying or contending with the conflict and challenges described above.

For these reasons, we urge the AG to strike Section 999.314(a) from the proposed regulations and allow the statutory definitions of “business” and “service provider” to control. Although we believe this section should be struck and that failing to do so will have negative consequences, as an alternative, we suggest the AG, at minimum, clarify that when a service provider performs services for an entity that is not a business and to which the CCPA does not apply, the service provider may follow such entity’s otherwise lawful direction deviating from the CCPA with regards to any action otherwise required under the CCPA.

* * * * *

Thank you for the opportunity to submit these comments on the proposed regulations. Alight would welcome the opportunity to meet and discuss our comments in greater detail or to answer any questions that you may have.

Respectfully submitted,
Alight Solutions LLC

M. Garrett Hohimer
Assistant General Counsel & Director, Government Relations



Tola Sobitan
Chief Privacy Officer & Senior Counsel



Message

From: Holden, Robert A. [REDACTED]
Sent: 12/6/2019 8:21:06 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: American Association of Payers, Administrators and Networks Comments
Attachments: AAPAN's Comments to the California Office of the Attorney General on CCPA 12.6.2019.pdf

Please find our comments attached. Thank you for your consideration.

Robert A. Holden
[REDACTED]



December 6, 2019

Via Email to PrivacyRegulations@doj.ca.gov

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

RE: Comments Concerning the Proposed California Consumer Privacy Act Rules

Dear Coordinator:

I am writing on behalf of the American Association of Payers Administrators and Networks ("AAPAN") to comment on the proposed rulemaking implementing the California Consumer Privacy Act (CCPA). AAPAN is the leading national association of preferred provider organizations ("PPOs"), networks, and administrators providing services to health plan enrollees, self-funded employer plans, and injured workers. Through our members, we work on behalf of thousands of California residents. Our comments on the rulemaking are addressed towards gaining greater clarity on how the rules will address information exchanged between covered entities, business associates, and health care providers subject to federal regulations pursuant to the Health Insurance Portability and Availability Act of 1996 (HIPAA).

Clarifications on the Application of Rules Pursuant to CCPA Section 1798.145

AAPAN members would like to seek clarification in the application of CCPA section 1798.145(c)(1) concerning the responsibility of a "Business Associate" as it relates to a "Covered Entity" as both those terms are defined and regulated under 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e). Many AAPAN members are Business Associates under HIPAA and they would like clarification as to the extent of the exemptions provided under CCPA 1798.145, so long as their activities as Business Associates support a Covered Entity's obligation to patients. In particular, would like to understand how these exemptions extend to the exchange of health care provider personal information which may not be considered PHI. This is additionally instructive should the business to business exemptions under the CCPA sunset.

Claims Processing and the Provider Exclusion

Many AAPAN members process claims on behalf of a Covered Entity. This results in two questions as to the application of the exemption under CCPS section 1798.145. First, we would

Message

From: Dan Jaffe [REDACTED]
Sent: 12/6/2019 2:48:04 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: ANA Detailed Comments on Proposed CCPA Regulations
Attachments: ANA Comments on Proposed CCPA Regulations FINAL.pdf
Importance: High

Dear Attorney General Becerra,

Attached please find detailed comments by the Association of National Advertisers (ANA) in response to your office's proposed regulations regarding the California Consumer Privacy Act (CCPA). We hope that you will take this document under careful consideration and work to make the CCPA better for both consumers and businesses.

If you have any questions please feel free to reach me at [REDACTED] or by calling the Washington Office of ANA at [REDACTED]

Best wishes,
Dan Jaffe

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
2020 K Street N.W. Suite 660
Washington DC 20006



Visit my [Regulatory Rumbblings Blog](#)





LEADERSHIP AND
MARKETING EXCELLENCE

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

COMMENTS

of the

ASSOCIATION OF NATIONAL ADVERTISERS

on the

California Consumer Privacy Act Proposed Regulations

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

Counsel:
Stu Ingis
Mike Signorelli
Tara Potashnik
Allaire Monticollo
Venable LLP
600 Massachusetts Ave., NW
Washington, DC 20011
[REDACTED]

December 6, 2019

On behalf of the Association of National Advertisers (“ANA”), we provide the following comments in response to California Office of the Attorney General’s (“CA AG”) October 11, 2019 request for public comment on the proposed regulations implementing the California Consumer Privacy Act (the “CCPA”).¹ We appreciate the opportunity to engage with the CA AG on the important subject of consumer privacy and the content of the rules that will help implement the CCPA.

ANA participated in the CA AG’s preliminary rulemaking public forums in San Marcos on January 14, 2019 and Sacramento on February 2, 2019, and ANA also testified at a February 20, 2019 informational hearing on the CCPA held by the California State Assembly Committee on Privacy and Consumer Protection. In addition, ANA participated in the CA AG’s December 4, 2019 San Francisco public hearing to offer input on the proposed regulations. We and our members are committed to helping ensure that consumers enjoy meaningful privacy protections in the marketplace and that businesses can continue operations that support and sustain the California economy.

The ANA’s mission is to drive growth for marketing professionals, for brands and businesses, and for the industry. Growth is foundational for all participants in the ecosystem. The ANA seeks to align those interests by leveraging the 12-point ANA Masters Circle agenda, which has been endorsed and embraced by the ANA Board of Directors and the Global CMO Growth Council. The ANA’s membership consists of more than 1,600 domestic and international companies, including more than 1,000 client-side marketers and nonprofit organizations and 600 marketing solutions providers (data science and technology companies, ad agencies, publishers, media companies, suppliers, and vendors). Collectively, ANA member companies represent 20,000 brands, engage 50,000 industry professionals, and invest more than \$400 billion in marketing and advertising annually. The vast majority of them are either headquartered, or do substantial business, in California.

The issues and problems we highlight concerning the CCPA and the proposed regulations in the ensuing comments, if not remedied, could have grave and substantial effects on consumers. Every point we discuss below may have significant and detrimental consequences to consumers by threatening their ability to access products and services they enjoy and expect. The CCPA is poised to impose limitations on the free flow of data that has fueled the economy for decades and has empowered consumers to receive appropriate products and services in the right place and at the right time. Data has created untold consumer benefit by enabling free and low-cost services and has directly facilitated consumers’ exposure to new products and offerings that may interest them. The CCPA stands to detrimentally impact this status quo and could curtail the use of data that has improved consumers’ lives and enriched their experiences.

Our members support the responsible use of data and the underlying goal of enhancing consumer privacy that is inherent in the CCPA and the CA AG’s proposed rules. For decades, our industry has championed consumer transparency and choice regarding businesses’ data practices, including by promoting strong codes of conduct and self-regulatory programs. ANA has, for example, supported the Digital Advertising Alliance’s (“DAA”) consumer-centric notice

¹ California Department of Justice, *Notice of Proposed Rulemaking Action* (Oct. 11, 2019), located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf>.

and choice program and its corresponding Self-Regulatory Principles for Online Behavioral Advertising for over ten years.² There have been over 100 million unique visits to the DAA self-regulatory site for consumers to exercise their privacy choices. In addition, ANA is the home of the Guidelines for Ethical Business Practice, a self-regulatory code designed to provide individuals and entities in all media that are involved in data-driven marketing with generally accepted principles of conduct.³ ANA has consistently maintained and reinforced industry standards that place responsible data practices and consumer privacy at the forefront of business considerations.

ANA members also play a significant role in the California economy. For example, in California, advertising helps generate \$767.7 billion or 16.4% of the state's economic activity and helps produce 2.7 million jobs or 16.8% of all jobs in the state.⁴ Moreover, many of our members employ California residents and nearly all of them provide goods and services to consumers in the state. It is no secret that advertising and marketing contribute to the health and growth of the economy overall. ANA-member businesses are committed to affording California consumers robust privacy protections while also continuing to bolster and enrich the state's economic activity and employment.

The underlying principles of transparency, control, and accountability included in the CCPA are aligned with ANA members' values. Several clarifications the CA AG provided in its proposed rules have offered helpful guidance for businesses in furthering CCPA compliance. Other provisions, however, set forth in the proposed rules represent departures from the text and scope of the CCPA as enacted by the legislature and could stand to decrease consumer choice and privacy rather than advance it. Additionally, because the CA AG's own timetable for the rulemaking makes clear that it is highly unlikely to finalize the rules implementing the law before its January 1, 2020 effective date, businesses could have significant difficulties complying accurately with the CCPA without the benefit of the finalized rules. The CCPA represents a highly complex and in many respects ambiguous law, and without final rules to sufficiently clarify its terms in advance of its effective date, the CCPA could prove to be extremely disruptive to consumers and business alike.

The Standardized Regulatory Impact Assessment, put forward by the CA AG's Office, on the CCPA highlights the costs the law could impose on the California economy.⁵ According to the assessment, the initial costs for state businesses to comply with the CCPA could be as high as \$55 billion, equivalent to 1.8% of California Gross State Product in 2018. The report also estimates that the additional costs to comply with the CA AG's regulations implementing the law could reach \$16.454 billion over the next decade, depending on the number of businesses impacted. It is clear from the impact analysis that the CCPA could have a substantial impact on

² DAA, Self-Regulatory Principles for Online Behavioral Advertising (Jul. 2009), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/seven-principles-07-01-09.pdf.

³ ANA, Guidelines for Ethical Business Practice (2017), located at <https://thedma.org/accountability/ethics-and-compliance/dma-ethical-guidelines/>.

⁴ IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at <https://www.ana.net/magazines/show/id/rr-2015-ihs-ad-tax>.

⁵ State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* (Aug. 2019), located at http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

the state's business community and economy, effects that would also be felt elsewhere in the country. The report's wide-ranging estimates of future costs reflect the uncertainty and potential disruption the law presents for businesses, regulators, and consumers. ANA urges the CA AG to work to reduce the economic and operational burdens of the CCPA while maintaining privacy protections for consumers.

As our members continue to design systems, policies, and technical processes to operationalize the CCPA, the industry would benefit from additional clarity surrounding certain provisions in the law and the proposed regulations so businesses can facilitate the regime's consumer rights and provide notice and choice consistent with its requirements. Moreover, the CA AG should take steps to ensure the final regulations, when promulgated, align with the text and scope of the CCPA. We provide the following suggestions to the CA AG to clarify certain points of the CCPA and proposed regulations, and we encourage the office to update parts of the proposed rules to better align with the CCPA itself and to ensure consumers have the ability to make meaningful choices. Our comments first address three issues of paramount importance that we raised in San Francisco at the CA AG's December 4, 2019 public hearing on the content of the proposed rules. The remainder of our comments are organized thematically, addressing several topics in a number of general issue areas. Our comments proceed by discussing the following:

- I. Issues ANA Addressed in its December 4, 2019 Verbal Testimony
- II. Consumer Requests to Opt Out and Opt In to Personal Information Sale
- III. Consumer Requests to Know and Delete
- IV. Service Providers
- V. Consumer Verification
- VI. Privacy Policies
- VII. Other Required Notices
- VIII. Provisions of the Proposed Regulations that ANA Supports

I. Issues ANA Raised in its December 4, 2019 Verbal Testimony

a. Clarify Requirements Surrounding Loyalty Programs So Businesses May Continue to Offer Such Programs to Consumers

Per the proposed rules, a business may offer a price or service difference, *i.e.*, a loyalty program, to a consumer if the difference is reasonably related to the value provided to the business by the consumer's data.⁶ The proposed regulations also require businesses to include a good-faith estimate of "the value of the consumer's data," which is defined as "the value provided to the business by the consumer's data," in addition to the method of computing such value, in a notice of financial incentive before they may offer loyalty programs.⁷ The CA AG should clarify how a business may justify that a price or service difference is reasonably related to the value provided to the business by the consumer's data. The CA AG should further clarify that a business does not need to provide the method of calculating the value of a consumer's data or a good faith estimate of such value in a notice of financial incentive if this information would constitute confidential, proprietary business information or put the business's competitive position at risk. At a minimum, the CA AG should clarify that a business may provide an estimate of the aggregate value of consumer data instead of an estimate of the value of data pertaining to an individual consumer to satisfy this requirement.

Consumers participate in loyalty and rewards programs on an opt-in basis. Consumers understand that as they provide data to businesses in order to participate in loyalty programs, they obtain value through those programs by gaining access to lower prices and special offers. Loyalty programs take many different forms. For example, gas dollar programs, frequent flyer programs, grocery "valued customer" rewards, and many other similar offerings constitute loyalty programs that could be hindered in California due to the CCPA. Consumer data makes loyalty programs possible, but consumers who make deletion or opt out requests restrict the very data that allows them to participate in loyalty programs. The proposed regulations' requirement for businesses to ensure that any price or service difference offered to consumers is reasonably related to the value they receive from consumer data constitutes a requirement that may be impossible for businesses to meet. As a result, this requirement has the potential to impede the offering of loyalty programs that consumers enjoy and have come to expect. Without clarification on how businesses may reasonably justify that a price or service difference is reasonably related to the value provided to the business by the consumer's data, many loyalty programs could cease altogether when the CCPA becomes effective on January 1, 2020.

In addition, if a business offers a financial incentive or a price or service difference to a consumer, the business must provide a notice of the financial incentive that offers (1) "a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and" (2) "a description of the method the business used to calculate the value of the consumer's data."⁸ While the proposed regulations clarify that "the value of the consumer's data" is the value provided to the business by such data, the requirement to provide an estimate of such value is unworkable. It is unclear whether a financial incentive

⁶ Cal. Code Regs. tit. 11, §§ 999.336(b), 337(a) (proposed Oct. 11, 2019).

⁷ *Id.* at §§ 999.307(b)(5)(a), 337(a).

⁸ *Id.* at § 999.307(b)(5).

must justify the price or service difference offered to consumers on a product-by-product basis (e.g., discounts for coffee must be justified independently and separately from discounts for pastries), or if businesses may justify their price or service differences for CCPA purposes in a more holistic sense. The method by which a business values personal information associated with a consumer may vary based on the situation at hand, the discount being offered at a particular time or in a particular place, and a variety of other factors. Additionally, the actual value the business attributes to such data may, in many cases, be difficult to quantify.

From an operational standpoint, the value provided to a business by data pertaining to consumers may be calculated on an aggregate basis rather than an individual consumer basis. The proposed regulations do not clarify whether a business may satisfy the nondiscrimination and financial incentive requirements by providing an estimate of the *aggregate value* of data as opposed to an estimate of the value of data pertaining to an individual consumer. The proposed regulations also do not account for how businesses should quantify nontangible value created in terms of fostering consumer loyalty and goodwill. Several varying and proprietary considerations make these calculations complex and have the potential to confuse consumers rather than enlighten them to business practices. ANA encourages the CA AG to revise the draft rules to explicitly state that a business may satisfy the nondiscrimination and financial incentive requirements by providing an estimate of the aggregate value of consumer data as opposed to an estimate of the value of data pertaining to an individual consumer.

Moreover, the requirement to include an estimate of “the value of the consumer’s data” and the method of calculating such value could reveal confidential information about a business that could jeopardize the business’s competitive position in the marketplace. Information about the value the business attributes to the consumer’s data and the method of calculating the value could constitute proprietary information about businesses’ commercial practices. A requirement to divulge this information risks distorting the market by forcing companies to reveal confidential data. In many instances, such calculations could harm businesses if divulged, as they would reveal proprietary or confidential information to competitors. Consequently, the requirement to disclose a reasonable estimate of the value of the consumer’s data and the business’s method for calculating such data presents significant risks to competition and business proprietary information. The CA AG should clarify how a business may justify that a price or service difference is reasonably related to the value provided to the business by the consumer’s data so that businesses may continue to offer loyalty programs to consumers. In addition, we ask the CA AG to clarify that businesses need not provide the method by which they calculate “the value of the consumer’s data” or the actual estimated value if such a disclosure could lead to anticompetitive consequences in the marketplace, or, at the very least, businesses may satisfy this requirement by providing an estimate of the aggregate value of consumer data instead of an estimate of the value of data pertaining to an individual consumer. Consumers clearly see the value of loyalty programs as demonstrated by the broad participation in such programs by both California consumers and the country at-large. Therefore, rules in regard to these programs should be carefully calibrated so as to not undermine their value to consumers.

b. Clarify that Intermediaries Must Allow Consumers to Express Opt Out Choices Through Browsers and May Not Block Opt Out Selections

According to the proposed regulations, a business that collects personal information from consumers online must treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt out of the sale of personal information as "a valid request submitted... for that browser or device, or if known, for the consumer."⁹ This requirement goes beyond the intent of the legislature and scope of the CCPA. It represents an entirely new business duty that does not further the purposes of the CCPA, but rather exceeds the law's scope by imposing material obligations on businesses that have no textual support in the statute. The legislature previously considered browser settings when it amended California Online Privacy Protection Act ("CalOPPA") in 2013, and at the time chose to not mandate a single, technical-based approach to effectuating consumer choice.¹⁰ Instead, the legislature offered alternative approaches, which is best for consumer and businesses. The legislature could have included such a mandate when it passed the CCPA and amended the law in September of 2018 and 2019, but each time chose not to. The CCPA itself does not direct the CA AG to implement such rules or such an approach. ANA believes that mandating that businesses honor the suggested signals undermines consumer choice and could harm consumers. Such tools are a blunt instrument broadcasting a single signal to all businesses. Consumers are not provided an option to set granular choices, business-by-business selections, allowing certain business to sell data while restricting others. This does not allow a consumer to maximize their enjoyment and participation in the data economy. In addition, a business is not able to authenticate whether a consumer has affirmatively set such signals. Such tools are ripe for intermediary tampering.

If the CA AG nevertheless pursues this approach, we suggest that the CA AG adopt a rule that requires a business engaged in the sale of personal information to either: (1) honor browser plugins or privacy settings or mechanisms, or (2) not be required to honor such settings where the business includes a "Do Not Sell My Info" link and offers another mechanism or protocol for opting out of sale by the business. This approach would be consistent with CalOPPA and the CCPA, as passed by the legislature. It would also provide consumers with meaningful choices.

Regardless of the mechanism offered to effectuate a consumer opt out, the CA AG's rules should protect the signals set by the consumer. Some browsers, operating systems, and other intermediaries have the ability to interfere with consumers' ability to use choice tools via the Internet. This interference can occur when these intermediaries block the technology that is used to signal an opt out (*e.g.*, cookies, JavaScript, mobile ad identifiers, etc.), often through default settings. When browsers take cookie and other technological opt out tools out of the equation, consumers are ultimately harmed because their opt out preferences fail to be communicated to the business. If consumers are unable to deliver a choice signal to a business due to an intermediary's blockage of the technology used to signal that choice, meaningful consumer choice would be removed from the marketplace.

c. Remove the Requirement For Businesses to Pass Consumer Opt Outs to Parties to Whom They Sold Personal Information in the Prior 90 Days

⁹ *Id.* at § 999.315(c).

¹⁰ AB 370 (Cal. 2013).

Per the proposed rules, upon receipt of a consumer opt out request, a business must: (1) “notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business’s receipt of the consumer’s request that the consumer has exercised their right to opt-out,” and (2) “instruct [the third parties] not to further sell the information.”¹¹ This provision places requirements on businesses to communicate opt out requests to third parties and instruct those third parties not to further sell information, which are obligations that are not included in the CCPA. To avoid regulatory provisions that are not within the scope of the statutory text of the CCPA and could cause significant unintended consequences that could result from these entirely new business obligations, the CA AG should update the proposed regulations to align with the CCPA such that businesses are not required to pass opt out requests along to third parties. At a minimum, the CA AG should clarify that businesses are not required to pass opt out requests along to third parties if such third parties are contractually prohibited from selling personal information received from the business.

First, requiring businesses to communicate opt out requests to third parties is a significant new requirement imposed by the CA AG after businesses have spent over a year designing novel, resource-intensive, and costly processes and technical controls for the CCPA. The requirement exceeds the law’s scope by levying entirely new substantive obligations on businesses without a basis in the CCPA to do so, and it does nothing to “further the purposes of the title,” which the California legislature has required of all regulations implementing the CCPA. As a result, the CA AG’s implementation of a new requirement to pass opt outs along to third parties represents a substantial change from the text of the CCPA and is outside of the scope of the law. It does not provide businesses with enough time to build the systems necessary to accomplish this requirement before the law’s January 1, 2020 effective date. Moreover, the new requirement to pass opt out request to third parties is unclear and may be contrary to consumers’ actual preferences. The requirement is also superfluous and unnecessary, as the CCPA itself already addresses downstream data sales by requiring third parties that receive personal information from a sale to ensure the consumer has received explicit notice and an opportunity to opt out of future sales.¹² Consequently, third party businesses are already obligated under the CCPA to offer consumer rights with respect to personal information.

Second, the proposed regulations’ mandate that businesses must communicate opt out requests to third parties does not serve to further meaningful consumer choice. If a consumer opts out of one business’s ability to sell personal information, that business should not be obligated to proliferate that request to other third parties. In addition, if third parties effectuate the opt out requests they receive from a business that the consumer originally directed to the business alone, consumers stand to lose access to products, services, and content that they did not wish to lose access to by sending an opt out request to a business. The outcome the CA AG is proposing with this opt out flow-down provision is not reflective of consumer choice; it would take the consumer’s expressed choice in one instance and apply that choice to others. The CCPA should enable consumers to choose which businesses and third parties can and cannot sell personal information. The law should not structure a system that interprets a consumer’s opt out choice with respect to one business as a choice that should apply across the entire marketplace.

¹¹ Cal. Code Regs. tit. 11, § 999.315(f) (proposed Oct. 11, 2019).

¹² Cal. Civ. Code § 1798.115(d).

Finally, the requirement to pass opt out requests on to third parties is not practical given the modern data-driven advertising ecosystem. This new obligation could require businesses to terminate rights to data they have already passed on to third parties. This limitation would stifle the free flow of data that powers the economy, thereby decreasing consumers' access to products and services. In the context of online commerce, the requirement would threaten to break the Internet by decreasing the amount of advertising revenue available to subsidize the online content consumers enjoy and have come to expect, particularly if third parties must further pass consumers' initial opt out selections down the chain to other third-party businesses. This requirement could also cause economic and valuation issues, as the potential would always exist for a third-party data recipient to lose their rights to use or further sell the data they have lawfully acquired from businesses. Businesses would not be able to reliably quantify their products and services, and the overall economy could suffer as a result. ANA therefore respectfully asks the AG to update the proposed rules so businesses are not required to pass opt out requests along to third parties in the prior 90 day period.

II. Consumer Requests to Opt Out and Opt In to Personal Information Sale

a. Remove the Requirement for Businesses that Do Not Collect Information Directly to Obtain Examples of Notices Provided to Consumers by Data Sources

The proposed regulations state that businesses that do not collect information directly from consumers do not need to provide a notice at collection.¹³ Before selling personal information, however, the proposed rules state that such businesses must: (1) contact the consumer to provide notice of sale and notice of the opportunity to opt out; or (2) obtain signed attestations from the data source describing how it provided notice at collection, including an example of the notice; maintain those attestations for a two-year period; and make them available to consumers upon request.¹⁴ The CA AG should update the proposed rules so that entities may rely on contractual attestations from the business who passed the data along to them and do not need to obtain and maintain examples of the notice provided to consumers before engaging in personal information sale. In addition, a business should not be required to produce the attestations it receives from data sources or any sample notices it may be required to maintain to a consumer in response to an access request.

The CCPA itself only requires third parties to provide consumers with “explicit notice” and an opportunity to opt out of the sale of personal information.¹⁵ Moreover, the consumer benefit achieved by the obligation to maintain examples of the notices provided to consumers is unclear, and this requirement would be extremely burdensome for entities to manage. Mandating that entities must receive contractual attestations from the data source that the consumer was notified before engaging in information sale provides the consumer with the same benefit as requiring businesses to maintain an example of the notice. Both achieve the goal of consumer transparency, and consumers' knowledge of data practices would not be enhanced by requiring businesses to maintain examples of the notice provided to specific consumers.

¹³ Cal. Code Regs. tit. 11, § 999.305(d) (proposed Oct. 11, 2019).

¹⁴ *Id.*

¹⁵ Cal. Civ. Code § 1798.115(d).

Furthermore, this provision could be interpreted to require businesses to pass example notices down the chain from the original source of data to other businesses who may receive personal information as part of the process. This would undermine privacy protections rather than enhance them. In dynamic data markets such as the one that powers the Internet, it is impossible to pass model notices to third parties and provide a taxonomy for tracking notices and tying them to the data source. For instance, in a programmatic market where billions of data transactions are occurring in the matter of seconds, there is no reasonable method of passing along model notices to entities that receive data. This requirement is therefore unclear, unrealistic, and would be difficult if not impossible for businesses to satisfy.

Moreover, businesses should not be required to return the sample notices they may be required to maintain or the attestations they receive from data sources to consumers in response to access requests. This requirement is not based in the CCPA, does nothing to further the purposes of the law, and provides no discernible consumer benefit. In fact, it could expose proprietary business terms to the public, thereby harming businesses' ability to compete or transact in the marketplace. It is also operationally impractical for businesses to be able to link a particular data point to a particular consumer whose data was received under a particular contractual term. The costs that would be associated with such a process far exceed the benefit that would be provided to the consumer. The California legislature determined that businesses are not required to disclose the specific source of data to consumers in response to access requests when it structured the CCPA to require the disclosure of *categories of sources* of personal information only. Any requirement to return attestations from data sources or sample notices to consumers would render this CCPA term moot by having the practical effect of requiring businesses to disclose specific sources of personal information.

If the goal of Section 999.305(d) of the proposed regulations is to provide California consumers with additional notice of their opportunity to exercise rights under the CCPA, this aim can be accomplished in much less burdensome ways. The CA AG should clarify that businesses need not obtain examples of notices provided to consumers by data sources in order to engage in personal information sale under the CCPA and do not need to return the attestations they receive from data sources or the sample notices they may be required to maintain to consumers in response to access requests.

b. Clarify the Requirement to Obtain Parental Consent for Minors “in addition to” Verifiable Parental Consent Under the Children’s Online Privacy Protection Act (“COPPA”)

Per the proposed regulations, a business that has actual knowledge it collects or maintains the personal information of children under the age of thirteen must establish, document, and comply with a reasonable method for determining that a person affirmatively authorizing the sale of personal information about the child is the parent or guardian of the child.¹⁶ Such affirmative authorization must be “in addition to” any verifiable parental consent required under COPPA, according to the proposed rules.¹⁷ ANA asks the CA AG to clarify how this “additional” CCPA

¹⁶ Cal. Code Regs. tit. 11, § 999.330(a)(1) (proposed Oct. 11, 2019)

¹⁷ *Id.*

consent must function in practice by issuing a rule stating that a business may send one consent communication with separate check boxes for CCPA and COPPA-related consents.

In describing the requirement for parents or guardians of children under age thirteen to affirmatively consent to the sale of a child’s personal information, the proposed regulations list acceptable consent mechanisms that mirror the acceptable verifiable parental consent mechanisms that are set forth in the COPPA Rule.¹⁸ However, the proposed regulations explicitly state that any CCPA-related affirmative authorization from a parent or guardian to sell a child’s personal information must be *in addition to* any consents obtained under COPPA. It is therefore unclear how businesses must obtain such additional or separate consents. Moreover, it is unclear the extent to which COPPA could preempt the requirement to obtain affirmative authorization to sell personal information that is included in the CCPA.

The CA AG should permit a business to provide one consent mechanism that is acceptable under both the CCPA and COPPA to a parent or guardian that contains separate consent check boxes pertaining to the activities that require consent under each law. The proposed rules should not require a business to send two, completely separate consent communications or requests to a parent or guardian to obtain verifiable parental consent under COPPA and affirmative authorization pursuant to the CCPA. The “additional” consent requirement in the proposed rules also creates ambiguities when it comes to interpreting parents’ choices, as it is unclear what should happen if a consumer consents to personal information sale under the CCPA but rejects personal information collection, use, or disclosure under COPPA. ANA requests that the CA AG clarify this issue, preferably by stating that a business may send one consent request with separate check boxes for CCPA and COPPA-related consents.

III. Consumer Requests to Know and Delete

a. Ensure the Definition of “Request to Know” Aligns with the Text of the CCPA

The proposed regulations state that a “request to know” (*i.e.*, an access request) is “a consumer request that a business disclose personal information that it *has* about the consumer...”¹⁹ The definition includes a request for “specific pieces of personal information that a business *has* about the consumer.”²⁰ This provision departs from the text of the CCPA, which notes that a consumer has the right to request that a business disclose “[t]he categories of personal information it has *collected* about that consumer” and “[t]he specific pieces of personal information it has *collected* about that consumer.”²¹ ANA requests that, consistent with the text of the CCPA, the CA AG clarify that requests to know apply only to personal information *collected* about a consumer.

The CA AG should clarify that requests to know apply to personal information that a business has collected about a consumer. This update would bring the proposed regulations into conformity with the text of the CCPA. In its Initial Statement of Reasons describing the

¹⁸ *Id.* at § 999.330(a)(2); 16 C.F.R. § 312.5(b).

¹⁹ Cal. Code Regs. tit. 11, § 999.301(n) (proposed Oct. 11, 2019) (emphasis added).

²⁰ *Id.* at § 999.301(n)(1) (emphasis added).

²¹ Cal. Civ. Code § 1798.110(a)(1) (emphasis added).

proposed regulations, the CA AG noted its intent in providing a definition of “request to know.”²² The CA AG did not indicate a desire to alter the requirements of the CCPA in this description of its intent. Instead, the CA AG said it provided a definition of request to know to “allow... the regulations to group together the requirements businesses must follow,” suggesting the intent was to improve convenience and readability rather than substantively change the requirements of the law. The CA AG also stated that it provided a definition of request to know to offer further clarity and to avoid unnecessary confusion. As a result, it does not appear that the CA AG intended to change the meaning of the CCPA or create ambiguity by issuing this provision of the proposed regulations. ANA asks the CA AG to the extent practical to harmonize the language of the proposed rules with the text of the CCPA. This would help reduce confusion for businesses implementing the CCPA’s requirements. Therefore, ANA urges the CA AG to update the proposed rules’ definition of “request to know” so that requests for personal information apply to “personal information that a business has *collected* about the consumer” and “specific pieces of personal information that a business has *collected* about a consumer.” ANA submits this suggested clarification to the CA AG to help ensure that the regulations align with the text of the CCPA.

b. Clarify Required Methods for Submitting Requests to Know for Businesses that “Primarily Interact” with Customers at Retail Stores

The proposed regulations state that a business that operates a website but primarily interacts with customers in person at a retail location must offer three methods to submit requests to know: a toll-free number, an interactive webform accessible through the website, and a form that can be submitted in person at the retail location.²³ This directive is unclear and presents major challenges to businesses for two primary reasons.

First, the proposed regulation provides no guidance about how to determine the way a business “primarily” interacts with consumers. Today, very few businesses may “primarily” interact with consumers in retail locations, as most purchases and commercial interactions occur online. Second, requiring retail businesses to allow consumers to submit such requests in person through a physical form would create excessive burdens in terms of employee training and could cause customer service issues and disruptions to consumers through long lines at retail stores. In the retail industry, many employees are seasonal and may not have enough institutional knowledge or training to effectively and efficiently facilitate these in-person CCPA requests.

The CA AG should clarify that businesses that have websites but interact with customers in retail locations need to provide a toll-free number and a webform only for consumer requests and may direct consumers to such methods of submitting requests if they receive an inquiry about submitting CCPA requests in person at a retail store. The toll-free number and webform method of submitting requests would allow retail companies to cultivate employees with an expertise in managing CCPA requests received by phone or online and would allow for more well-trained individuals to provide accurate and helpful responses to consumer inquiries.

²² Office of the California Attorney General, *Initial Statement of Reasons for Proposed Adoption of California Consumer Privacy Act Regulations 6-7* (Oct. 2019) (hereinafter, “ISOR”), located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf>.

²³ Cal. Code Regs. tit. 11, § 999.312(c)(2) (proposed Oct. 11, 2019).

c. Ensure the Definition of “Request to Delete” Aligns with the Requirements Businesses Must Meet in Describing Such Requests

According to the section of the proposed regulations that addresses information a business must include in its privacy policy, a business must “[e]xplain that the consumer has a right to request the deletion of their personal information collected *or maintained by the business*.”²⁴ This provision is inconsistent with the proposed regulations’ definition of a “request to delete,” and it appears to require businesses to state in their privacy policies that consumers have a different right than the CCPA and proposed regulations afford them. We ask the CA AG to clarify that a business must provide a privacy policy disclosure regarding requests to delete that is consistent with the proposed regulations’ definition of the term and with the CCPA itself.

The proposed regulations state that a “request to delete” is “a consumer request that a business delete personal information about the consumer that the business has *collected from* the consumer....”²⁵ This definition matches the formulation of the deletion right in the CCPA itself, which states that “[a] consumer shall have the right to request that a business delete any personal information about the consumer which the business has *collected from* the consumer.”²⁶ The CA AG’s Initial Statement of Reasons for adopting draft CCPA regulations also mirrors this construction of the deletion right.²⁷ However, per the proposed regulations, a business must disclose in its privacy policy that a consumer has a right to request deletion of personal information maintained by the business.²⁸ This disclosure is not tied to personal information that was collected from a consumer. This mandated privacy policy disclosure clearly does not track with the language describing the right to delete in the proposed regulations or the CCPA itself.

Consistent with the CCPA and the CA AG’s definition of “request to delete” in the proposed regulations, the CA AG should clarify that a business must disclose that a consumer has a right to request the deletion of personal information about the consumer which the business has *collected from* the consumer in its privacy policy. This change would bring the proposed regulations in line with the text of the CCPA and would refrain from causing unnecessary confusion for businesses in their efforts to create mechanisms to comply with the law’s terms.

d. Remove the Requirement to “Permanently and Completely” Erase Personal Information

The proposed regulations state that a business must comply with a consumer’s request to delete personal information by de-identifying the personal information, aggregating the personal information, or “permanently and completely erasing” the personal information on its existing systems.²⁹ We ask the CA AG to remove the “permanently and completely erasing” language, because it represents a substantive requirement that is not grounded in the text of the CCPA,

²⁴ *Id.* at § 999.308(b)(2)(a) (emphasis added).

²⁵ *Id.* at § 999.301(o) (emphasis added).

²⁶ Cal. Civ. Code § 1798.105(a) (emphasis added).

²⁷ ISOR at 7.

²⁸ Cal. Code Regs. tit. 11, § 999.308(b)(2)(a) (proposed Oct. 11, 2019).

²⁹ *Id.* at § 999.313(d)(2).

does nothing to further the purposes of the law, imposes significant compliance challenges for businesses, and may conflict with other provisions of the proposed regulations.

The “permanently and completely erasing” language sets forth a requirement that goes far above and beyond what is required in the CCPA, which states that a consumer has “the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.”³⁰ In addition, the requirement creates compliance challenges for businesses, because businesses may use certain database systems or architectures that do not allow for “permanent and complete” deletion. Furthermore, the requirement to “permanently and completely” delete personal information could conflict with the proposed regulations’ recordkeeping requirements, which obligate businesses to “maintain records of consumer requests made pursuant to the CCPA and how the business responded to said requests for at least 24 months.”³¹ As such, the “permanently and completely erasing” language is unnecessarily limiting and challenging for businesses to effectuate, and we ask the CA AG to remove this language from the text of the proposed rules.

e. Clarify Businesses May Provide a General Contact Toll-Free Phone Number for Receiving Consumer CCPA Requests

The proposed rules require a business to provide a toll-free phone number as a method for receiving “requests to know” and note that a business may provide one for receiving requests to delete and opt out.³² The CA AG should clarify that a business may provide a toll-free general help or contact number to consumers to make CCPA requests and need not provide a CCPA-specific toll-free number. Requiring businesses to create a separate phone number for CCPA requests would create consumer confusion by forcing them to submit requests unrelated to the CCPA through one phone number and CCPA-related requests through another. It would also increase costs for businesses, which would have to maintain and staff a separate phone number for CCPA-related requests. As such, the CA AG should clarify that a business may provide its main consumer telephone number as the toll-free phone number through which it may receive consumer CCPA requests.

IV. Service Providers

a. Place Reasonable Limits on the Service Provider Requirement to Provide Business Contact Information Upon Receipt of a Request to Know

Per the proposed rules, a service provider that receives a request to know or a request to delete from a consumer must “inform the consumer that it should submit the request directly to the business on whose behalf the service provider processes the information and, when feasible, provide the consumer with contact information for that business.”³³ ANA asks the CA AG to clarify that a service provider does not need to provide a business’s contact information to a consumer if doing so could compromise the service provider’s competitive position in the

³⁰ Cal. Civ. Code § 1798.105(b).

³¹ Cal. Code Regs. tit. 11, § 999.317(b) (proposed Oct. 11, 2019).

³² *Id.* at §§ 999.312(a), (b); 999.315(a).

³³ *Id.* at § 999.314(d).

marketplace or abridge the confidentiality clauses the service provider agreed to in contracts with its business clients.

The proposed regulations' requirement that a service provider must provide a consumer with a business's contact information may be difficult if not impossible for service providers to execute. A service provider may, for example, maintain information about a consumer that came to the service provider from more than just one business. In situations such as these, the service provider may not be in a position to know which business's contact information to provide to the consumer upon receiving a request to know or a request to delete. Moreover, the obligation to provide business contact information to a consumer who submits a request to know to a service provider could have negative effects for business competition by enabling the service provider's competitors to submit requests to know to the service provider to gain confidential or proprietary information about the service provider's client list. Although the draft regulations state that a service provider only must provide contact information "when feasible," it is unclear whether service providers are obligated to provide such information when it might be technically feasible to do so but would violate confidentiality clauses in their contracts with their clients or otherwise expose them to risks to their competitive position in the marketplace. The CA AG should clarify that it is not feasible for a service provider to provide a business's contact information to a consumer if providing such information could violate the service provider's confidentiality agreements with its clients or expose the service provider's client list to a competitor.

b. Allow Service Providers to Use Personal Information to Improve Services

According to the draft rules, a service provider "shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose of providing services to another person or entity."³⁴ This provision could be read to prohibit service providers from using personal information to make general improvements to their services that would benefit consumers, the business that provided the personal information to the service provider in the first place, and other businesses. Although the proposed regulations note that a service provider can combine personal information received from one or more entities to which it is a service provider on behalf of such businesses to the extent necessary to detect data security incidents or protect against fraudulent or illegal activity, this allowance does not enable service providers to combine and use the personal information they receive from businesses to improve their products and services. The use of personal information to upgrade and enrich products and services is important to enable service providers to improve their offerings and provide better services to businesses, which ultimately benefits consumers. The CA AG should therefore revise the draft rules to clarify that service providers may use personal information to make general improvements to services.

V. Consumer Verification

a. Clarify How Businesses Must Respond to CCPA Requests When They Maintain Personal Information In A Manner that Is Not Associated With An Identifiable Person

³⁴ *Id.* at § 999.314(c).

The proposed regulations state that if a business maintains personal information in a manner that is not associated with an actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the non-name identifying information.³⁵ In addition, the proposed rules state that “[i]f a business maintains consumer information that is de-identified,” it is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request.³⁶ The proposed regulations do not clearly explain how businesses may reasonably engage in verification when they do not maintain personal information in a manner that is associated with a named actual person. ANA asks the CA AG to clarify that businesses that do not maintain data sufficient to verify a consumer’s identity are not required to collect additional data from the consumer to do so.

While the proposed regulations state that fact-based verification inquiries may be required when businesses maintain personal information in a manner that is not associated with a named actual person,³⁷ this provision of the proposed regulations forces businesses to act as detectives to verify a consumer who may come to the business by matching them to a non-identifying piece of information. Identifiers businesses may maintain such as cookie IDs and IP addresses, for example, are not sufficient to identify a consumer on an individual level, and identifying information provided by the consumer would do nothing to enable the business to verify the consumer’s identity. As a result, the proposed regulations’ discussion of a consumer providing a certain number of “data points” or “pieces of personal information” in order to allow a business to verify the consumer to the degree of certainty needed to effectuate a request may not be sufficient if the business maintains non-identifiable information such as identifiers.³⁸ Moreover, identifiers may cover entire households, libraries, shared devices, or other places, and they may therefore be linked to personal information from many individuals.

Consequently, it may be difficult if not impossible for a consumer to demonstrate they are the sole consumer associated with non-name identifying information held by a business. It is also unclear how businesses can conduct fact-based verification inquiries when the information they may need to verify an identity is not information the consumer may have readily available to them (*e.g.*, a cookie ID, mobile ad identifier, IP address, or other online identifier). The CA AG should clarify that if a business does not maintain data sufficient to verify a consumer’s identity, the business is not required to collect additional data to verify the consumer. In addition, this type of attempt at identification is likely to undermine consumer privacy rather than enhance it.

b. Clarify that Verification Inquiries to Consumers from Businesses Toll the 45-Day Time Period to Respond to Requests

The proposed regulations require businesses to establish, document, and comply with a reasonable method for verifying consumer requests.³⁹ The proposed rules also require

³⁵ *Id.* at § 999.325(e)(2).

³⁶ *Id.* at § 999.323(e).

³⁷ *Id.*

³⁸ *See id.* at §§ 999.325(b), (c).

³⁹ *Id.* at § 999.323(a).

businesses to respond to requests to know and requests to delete within 45 days.⁴⁰ Consistent with the proposed regulations' verification provisions, a business may require a consumer to submit information to verify his or her identity before responding to a request.⁴¹ The draft rules note that the 45-day time period to respond to requests to know and requests to delete "will begin on the day that the business receives the request, regardless of time required to verify the request."⁴²

The CA AG should clarify that when businesses ask for verifying information from a consumer, such an action tolls or pauses the 45-day time period the business has to respond to the consumer request and resumes only when the consumer responds with the requested verifying information. A similar clarification would be helpful related to the two-step process that is required to process online consumer requests to delete personal information.⁴³ The CA AG should clarify that a business's request for a second, confirming action validating that the consumer wants the personal information the business collected from the consumer deleted, which must be provided pursuant to the proposed regulations, tolls the 45-day time period for responding to a request until the consumer provides the confirmation. Businesses should not be penalized for the public's dilatory responses to requests for verification that are outside the control of a company.

Businesses cannot accurately facilitate CCPA requests without verifying the consumer who is the subject of the request. Without proper verification, businesses risk effectuating a consumer request against personal information that pertains to the wrong consumer, thereby failing to fulfill the wishes of the consumer who submitted the request and taking action that would affect personal information about a consumer that did not make the request. If businesses are required to respond to consumer requests to know and delete within 45 days of receiving them, regardless of the amount of time it takes to verify the consumer's requests, consumers would be at risk of businesses taking action on and making decisions about personal information that does not align with their choices. Accordingly, we encourage the CA AG to clarify that a business's request for verifying information or a request for a second, confirming action validating a request to delete tolls or pauses the 45-day period within which businesses must respond to consumer requests to know and delete.

c. Remove the Requirement that Unverified Requests to Delete Must Be Treated as Requests to Opt Out

The proposed rules state that if a business cannot verify the identity of a consumer submitting a request to delete, it must inform the requestor that their identity cannot be verified and instead treat the request as a request to opt out of personal information sale.⁴⁴ Per the proposed rules, requests to opt out of personal information sale need not be pursuant to verifiable consumer requests.⁴⁵ The requirement to transform unverifiable deletion requests into opt out requests threatens to harm consumers rather than protect their interests, and it represents an

⁴⁰ *Id.* at § 999.313(b).

⁴¹ *Id.* at §§ 999.323(b), (c).

⁴² *Id.*

⁴³ *Id.* at § 999.312(d).

⁴⁴ *Id.* at § 999.313(d)(1).

⁴⁵ *Id.* at § 999.315(h).

entirely new obligation that is not required by the CCPA itself and is outside of the scope of the law. The CA AG's proposed rule requiring businesses to pass along opt out requests to third parties to whom they have sold personal information in the prior 90 days would mean that a consumer's unverified deletion request could have a ripple effect throughout the ecosystem by removing personal information associated with that consumer from the entire online environment. This result may not align with the consumer's desires, particularly if the consumer thought he or she was submitting a deletion request to be effective solely on an individual business. Such an application may not reflect the consumer's preferences and denies them the ability to allow some businesses to sell personal information while restricting others from doing so. The CA AG should therefore clarify that consumers must affirmatively request that a business opt the consumer out from personal information sale before the business may treat a deletion request as an opt out request.

The right to delete information and the right to opt out from sale of personal information are two separate rights that achieve two separate results. Deletion removes the consumer's personal information from the systems of the business that is the subject of the request, while opt out requests have the potential to remove the consumer's information from being transferred by many businesses, thereby inhibiting consumers' ability to receive products, services, and loyalty programs they enjoy and have come to expect. Consumers should not be forced to opt out of personal information sale if a business cannot verify their request to delete. The requirement to transform unverifiable deletion requests into opt out requests may conflict with consumers preferences and places a substantive obligation on businesses that has no textual basis in the CCPA. In addition, it could lead to competitors undermining the system by requesting deletions, that while unverifiable, would force their competitors into unwarranted opt-outs. As such, we ask the CA AG to clarify that if a business cannot verify a consumer's deletion request, the consumer must specifically request that the business opt out the consumer from personal information sale before the business may take such an action.

VI. Privacy Policies

a. Clarify the Required Granularity of Privacy Policies

The proposed regulations state that “[f]or each category of personal information collected...” a business must provide the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties with whom the business shares personal information.⁴⁶ As such, the proposed regulations suggest businesses must state the sources, purposes, and categories of third parties with whom personal information is shared *for each category of personal information*. The CA AG should clarify that businesses do not need to make disclosures for each individual category of personal information collected and may instead provide disclosures with respect to all categories of personal information collected.

If businesses must make disclosures with respect to each category of personal information collected, privacy policies would be significantly longer and more complex, and less understandable for consumers, than they would be if the required disclosures could be made with

⁴⁶ *Id.* at § 999.308(b)(1)(d)(2).

respect to personal information generally. This would detract from the purpose of a robust consumer privacy notice, as it would induce notice fatigue and could discourage consumers from taking the time to read and understand the full privacy notice and its contents. Additionally, requiring granular disclosures for each category of personal information collected could impede businesses from satisfying the requirement that a privacy policy must “be written in a manner that provides consumers [with] a meaningful understanding of the categories listed.”⁴⁷ The CA AG should clarify that businesses may make required disclosures for personal information generally and do not need to make granular disclosures relevant to each category of personal information collected. Businesses should be able to provide consumers with privacy policies that logically disclose required information in a digestible and understandable format, as this approach would further the ultimate goal of robust consumer notice in a more effective way than requiring disclosures pertaining to each category of personal information collected.

b. Enable Flexibility for the Placement of Privacy Policies in Mobile Applications

ANA encourages the CA AG to update the draft rules to provide more flexibility for the placement of privacy policies in mobile applications. The draft rules currently require a business to place a privacy policy “on the download or landing page of a mobile application.”⁴⁸ A business should have the ability to meet the requirement to provide a privacy policy by doing so (1) in a digital distribution platform for computer software applications, such as an application store, *or* on the download or landing page of an application, *and* (2) by making the policy available from an within the application itself, for example, through the application’s settings menu.

Revising the proposed regulations to provide more flexibility for presenting privacy policies in the mobile space would align with industry codes of conduct and past publications from the CA AG’s office on privacy practices in the mobile environment.⁴⁹ For example, the CA AG’s 2013 report titled “Privacy On The Go: Recommendations for the Mobile Ecosystem” states that a business should “[m]ake the privacy policy conspicuously accessible to users and potential users... [and] [l]ink to the policy within the app (for example, on [the] controls/settings page).”⁵⁰ The report therefore contemplated flexible approaches to providing consumers with necessary disclosures and took the unique nature of mobile applications into account in formulating its recommendations. As a result, ANA asks the CA AG to update the proposed regulations so that a business may satisfy the requirement to provide a clear and conspicuous link to a privacy policy by making the privacy policy viewable from within an application store or the download or landing page of an application, and within the mobile application itself.

⁴⁷ *Id.*

⁴⁸ *Id.* at § 999.308(a)(3).

⁴⁹ See, e.g., DAA, Application of Self-Regulatory Principles to the Mobile Environment at 15, 17 (Jul. 2013), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/DAA_Mobile_Guidance.pdf; Kamala D. Harris, Attorney General, California Department of Justice, *Privacy on the Go: Recommendations for the Mobile Ecosystem* at 10 (Jan. 2013) (hereinafter, “Privacy on the Go”), located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf.

⁵⁰ Privacy on the Go at 10.

c. Clarify that Businesses Do Not Have to Make Statements About Minors In Privacy Policies Unless They Have Actual Knowledge They Collect Personal Information From Minors Under the Age of 16

Per the proposed rules, as part of a business's privacy policy, the business must "[s]tate whether or not the business sells the personal information of minors under 16 years of age without affirmative authorization."⁵¹ This obligation could require a business to make a positive statement about a practice in which it does not engage would be both inaccurate and misleading, and potentially harmful to the business. The CA AG should clarify that a business does not have to make such a statement in its privacy policy unless it has actual knowledge that it collects personal information from minors under the age of 16.

Laws in the United States specifying the contents of privacy policies have historically required businesses to make statements about practices in which they do engage.⁵² Businesses typically do not list actions they do not take in their privacy policies. Through the proposed regulations, the CA AG has imposed a new requirement on businesses that was not included in the text of the CCPA itself. A business would now be required to make an affirmative statement about a practice in which it may not engage. This requirement contrasts with longstanding practices and laws regulating privacy notices in the United States. Furthermore, this provision provides consumers with minimal if any benefit.

The requirement to make an affirmative statement in a privacy policy about whether a business sells personal information of minors without affirmative authorization may also force businesses to investigate the ages of their users. This potential indirect obligation of the CCPA may contravene the clear implementation guidance to the contrary that the Federal Trade Commission has provided to businesses surrounding COPPA compliance, as COPPA has been interpreted to not require businesses to investigate the ages of their users.⁵³ To better align with COPPA, only businesses that have actual knowledge that they collect personal information from minors under the age of 16 should have to make a statement regarding affirmative authorization for the sale of that personal information in their privacy policies. The CA AG should clarify that a business does not have to make a statement about its practices of obtaining affirmative authorization to sell personal information in its privacy policy unless it has actual knowledge it collects personal information from minors under the age of 16.

d. Clarify the Privacy Policy Disclosures a Business Must Provide to be Exempt from the Obligation to Provide Notice of the Right to Opt Out

According to the proposed regulations, a business is exempt from the requirement to provide a notice of the right to opt out if "(1) [i]t does not, and will not, sell personal information collected during the time period during which the notice of right to opt-out is not posted; and (2) [i]t states in its privacy policy that it does not and *will not* sell personal information."⁵⁴ ANA

⁵¹ Cal. Code Regs. tit. 11, § 999.308(b)(1)(e)(3) (proposed Oct. 11, 2019).

⁵² See, e.g., Cal. Bus. & Prof. Code §§ 22575-22579; Del. Code Ann. tit. 6, § 1205C; Nev. Rev. Stat. §§ 603A.310-360.

⁵³ See FTC, Complying with COPPA: Frequently Asked Questions, located at <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>.

⁵⁴ Cal. Code Regs. tit. 11, § 999.306(d)(2) (proposed Oct. 11, 2019) (emphasis added).

asks the CA AG to eliminate the requirement for businesses that do not sell personal information to state that they *will not* sell personal information in the future. This revision would benefit consumers by helping to reduce potential confusion about business practices if such practices change in the future.

Requiring a business to state that it will not sell personal information does not take into account the fact that business practices can and often do change over the course of time as offerings evolve and new services are added. Stating that a business will not sell personal information in a privacy policy could give consumers the false impression that a business will never change its practices in the future. The Federal Trade Commission's longstanding position on material changes to privacy policies acknowledges that businesses can change their data practices so long as such changes are communicated to consumers, the information collected is treated according to the terms of the policy that was in place at the time of information collection, and if a business wishes to treat previously collected information according to the terms of the new policy, it must obtain affirmative express consent from consumers before doing so.⁵⁵ The FTC has therefore provided a framework that recognizes business practices may change in ways that are not originally anticipated and offers a method for businesses to implement those changes moving forward. Requiring businesses to state that they will not sell personal information in privacy policies runs the risk of suggesting to consumers that businesses will never change their data practices, even as their offerings and services evolve.

Moreover, as discussed in Section VI(c) above, businesses do not typically make statements in privacy policies about practices in which they do not or will not engage. Laws regulating the contents of privacy policies have typically required businesses to disclose practices in which they do engage to consumers and have not forced them to make statements about practices in which they will not engage. As such, the CA AG should consider eliminating the requirement for businesses that do not sell personal information to state that they will not sell personal information in their privacy policies in order to be exempt from the need to provide a notice of the right to opt out of personal information sale.

e. Clarify the Disclosures Required of Businesses that Buy, Receive, Sell, or Share Personal Information of 4 Million or More Consumers

Pursuant to the proposed rules, “[a] business that alone or in combination, annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers” must make privacy policy disclosures about the number of distinct CCPA requests received, complied with in whole or in part, and denied during the prior calendar year.⁵⁶ The phrase “shares for commercial purposes” could be interpreted to include sharing personal information about a consumer with service providers, which would drastically increase the number of businesses that would be subject to this additional reporting requirement. The CA AG likely did not intend to include sharing personal information with service providers within the scope of the calculation for determining whether a business is subject to the extra reporting requirements for businesses that buy, receive, sell, or

⁵⁵ Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* at 57-60, (Dec. 2010), located at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

⁵⁶ Cal. Code Regs. tit. 11, § 999.317(g) (proposed Oct. 11, 2019).

share personal information of 4 million or more consumers. As a result, we ask the CA AG to clarify that sharing personal information about a consumer with a service provider does not count towards determining whether a business is subject to these additional reporting requirements.

VII. Other Required Notices

a. Affirm that Required Notices May Be Provided in a Privacy Policy

The proposed regulations impose new consumer notices that are not required by the text of the CCPA, and they do not clearly state whether such notices may be provided in a privacy policy. In terms of disclosures, the proposed rules require businesses to provide: (1) a notice at collection; (2) a notice of the right to opt out of the sale of personal information; and (3) a notice of financial incentive in addition to a privacy policy.⁵⁷ The CA AG should clarify that the notice at collection, notice of the right to opt out of the sale of personal information, and notice of financial incentive provided in a privacy policy accessible to consumers where required satisfies the proposed regulations' mandate to provide notice at collection, notice of the right to opt out of the sale of personal information, and notice of a financial incentive.

The proposed regulations do not clearly state whether these additional notices required by the proposed regulations may be provided in a privacy policy. A “notice of right to opt out” is defined as “the notice given by a business informing consumers of their right to opt-out of the sale of their personal information.”⁵⁸ The “notice of right to opt-out” must be provided on the Internet webpage to which the consumer is directed after clicking the “Do Not Sell My Personal Information” link, and must either include certain specific information or link to the section of the business’s privacy policy that contains such information.⁵⁹ Similarly, if a business offers a financial incentive or price of service difference online, the business may provide a “notice of financial incentive” by linking to the section of the business’s privacy policy that contains the required information.⁶⁰ A “notice of financial incentive” is “the notice given by a business explaining each financial incentive or price or service difference.” As a result, the notice of right to opt-out and notice of financial incentive contemplate use of the privacy policy to contain necessary disclosures, but they do not explicitly state whether the notice requirements may be satisfied by providing the required information through a privacy policy alone.

In addition, the “notice at collection,” which is defined as “the notice given by a business to a consumer at or before the time a business collects personal information from the consumer,” may be provided through a conspicuous link to the notice on the business’s website homepage, a mobile application download page, or on all webpages where personal information is collected.⁶¹ The explicitly listed methods for providing the notice at collection are typical methods by which businesses provide privacy policies. As a result, the proposed regulations suggest, but do not explicitly state, that a notice at collection may be provided in a privacy policy.

⁵⁷ *Id.* at §§ 999.305, 306, 307.

⁵⁸ *Id.* at § 999.301(j).

⁵⁹ *Id.* at § 999.306(b).

⁶⁰ *Id.* at § 999.307(a)(3).

⁶¹ *Id.* at § 999.305(a)(2)(c).

The CA AG should clarify that the notice at collection, notice of right to opt-out, and notice of financial incentive may be provided to consumers in a privacy policy, and if such notices are provided in a privacy policy that is made available to consumers where required, they do not need to be provided through any other means. Such a rule would enable business compliance with the CCPA and offer consumers a centralized place through which they may receive required business disclosures. Providing such notices within the privacy policy is consistent with consumer expectations. Consumers have come to expect such disclosures and information to be accessible from a privacy policy. Consumers would benefit from receiving all the necessary information through a single notice, and businesses would benefit from being able to focus privacy-related information in one unified disclosure.

b. Confirm that Notice at Collection Should Not Be Required in the Context of Particular Commonplace Consumer-Business Interactions

The CCPA states that a business that collects “a consumer’s personal information” shall, at or before the point of collection, inform consumers of the categories of personal information to be collected and the purposes for which the categories of personal information shall be used.⁶² The CA AG should clarify that notice at collection is not necessary in the context of certain commonplace and frequent interactions with a business through which consumers expect the business to collect personal information.

Consumers engage in certain interactions with businesses that should not necessitate a notice at collection, because in those interactions consumers often expect businesses to collect personal information. For example, taking a consumer’s payment card information at a cash register in a retail store should not trigger the need to provide a notice at collection. If businesses must provide a notice at collection before taking payment card information at a retail store, consumer shopping experiences could be hindered, and business transactions would take substantially longer to effectuate. Payment card information is often exchanged during retail transactions, and consumers expect businesses to collect this information in order to complete the transaction the consumer wants to effectuate. Another example of a consumer-business interaction that should not require a notice at collection is when a consumer contacts a business’s customer service office. If a consumer contacts a business’s customer service representative over the phone, the customer service representative should not be required to verbally read the consumer information that would satisfy the CCPA’s notice at collection requirement, because it is reasonable for a consumer to expect the business to collect certain personal information in the context of the customer service call.

Requiring businesses to provide a distinct notice associated with everyday and consumer-expected data collection that is necessary to facilitate purchases or respond to consumer inquiries would inhibit consumers’ ability to make purchases efficiently and interact with businesses without substantial interruptions. The CA AG should therefore clarify that businesses need not provide a notice at collection to consumers if the context of the consumer-business interaction is one under which the consumer should reasonably expect that the business is collecting personal information.

⁶² Cal. Civ. Code § 1798.100(b); Cal. Code Regs. tit. 11, § 999.305(a)(1) (proposed Oct. 11, 2019).

c. Grant Online Businesses that Do Not Maintain Personally Identifying Information Flexibility to Provide Effective Opt Out Mechanisms

According to the proposed regulations, a business must provide a webform to enable consumers to opt out of the sale of personal information.⁶³ If a business operates a website, the proposed regulations also state that it must provide a webform to consumers to submit requests to know.⁶⁴ The CA AG should clarify that online businesses that do not maintain information that can identify a consumer do not need to provide a webform, and may use another, equally effective method to enable consumers to submit a request to opt out, such as through email or other standard channels used for customer service.

The proposed regulations already recognize that methods for submitting consumer rights requests may need to be different depending on whether the data collection occurs offline or online. As such, similar flexibility should be provided for opt outs involving what has been traditionally referred to as non-personally identifying information. Webform requirements may work efficiently for opt outs or requests to know pertaining to personally identifiable information, such as a consumer's name, email address, or postal address. However, the webform requirements do not adequately address how a webform can facilitate a consumer opt out or request to know for businesses that do not maintain personally identifiable information (such as when such businesses maintain cookie IDs, mobile ad identifiers, IP addresses, and/or other online identifiers). The CA AG should clarify that online businesses that do not maintain personally identifying information do not need to provide a webform and may use another method, such as email or other common channels used for customer service, to enable a consumer to submit a request to opt out.

d. Clarify Discrepancies Between the Content of Required Notices and the Content of Privacy Policies

According to the proposed regulations, businesses must provide a notice at collection, which must specify “[a] list of the categories of personal information about consumers to be collected.”⁶⁵ However, the proposed regulations also state that in a privacy policy, a business must provide “the categories of consumers’ personal information the business has collected about consumers in the preceding 12 months.”⁶⁶ As such, the “notice at collection” requirement is forward-looking, and the privacy policy provision is backward-looking. The CA AG should clarify whether businesses must provide disclosures related to personal information they have collected in the past twelve months or whether they must provide forward-looking disclosures about what they intend to do in the future with collected personal information in required notices.

Requiring businesses to provide disclosures about information they will collect from consumers in addition to information they have already collected about consumers runs the risk of producing excessively long privacy notices that would not provide meaningful disclosures to consumers. The mandate hinders’ businesses ability to provide consumers with a reasonably readable and palatable privacy notice that is presented in a format they can understand.

⁶³ Cal. Code Regs. tit. 11, §§ 999.306(c)(2), 315(a) (proposed Oct. 11, 2019).

⁶⁴ *Id.* at § 999.312(a).

⁶⁵ *Id.* at § 999.305(b)(1).

⁶⁶ *Id.* at § 999.308(b)(1)(d)(1).

Furthermore, this discrepancy between the need to provide information about future practices and information about past practices fails to adequately clarify what information must be provided in required notices. If a business may make all CCPA-required disclosures in one privacy policy, it is not clear whether it must provide a section for categories of personal information to be collected in the future and a section for categories of personal information it collected in the past 12 months. We request that the CA AG clarify this provision by regulation.

VIII. Provisions of the Proposed Regulations that ANA Supports

a. Providing Flexibility For Businesses' Presentation of Opt Out Links to Consumers

The proposed regulations indicate that the CA AG may consider another opt out button or logo during its CCPA rulemaking process.⁶⁷ We support the CA AG's efforts to provide an additional acceptable way to present the opt out button or logo. In lieu of setting forth a specific, prescribed button or logo via regulation, we suggest that the CA AG allow businesses flexibility to decide on an appropriate button or logo, subject to certain guidelines.

The CA AG should require the opt out button or logo to clearly indicate to the consumer that clicking the button enables the consumer to opt out of the sale of personal information. Instead of adopting a third acceptable formulation for the opt out button or logo (in addition to "Do Not Sell My Personal Information" or "Do Not Sell My Info"), the CA AG should set forth reasonable criteria the button or logo must meet, such as clear, meaningful, prominent notice to the consumer of the ability to opt out, and allow businesses flexibility in choosing an acceptable way to implement the opt out button or logo. We ask the CA AG to enable a flexible acceptable method of providing consumers with the ability to opt out of the sale of personal information.

b. Prohibiting Certain Sensitive Specific Pieces of Information from Being Returned to a Consumer in Response to a Request to Know

Per the proposed rules, a business may not at any time disclose a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers.⁶⁸ ANA supports this provision, as many of the data elements that are forbidden from disclosure are elements that, when combined with a first initial or first name and last name, would constitute a data breach under California law if acquired by an unauthorized individual.⁶⁹

The proposed regulations helpfully foreclose the possibility that, in order to comply with the CCPA, a business would be forced to disclose certain particularly sensitive data elements to the wrong recipient, which would constitute a breach. Furthermore, this provision makes practical sense from a data security standpoint, as there are compelling public policy reasons to restrict this particularly sensitive information from disclosure. For example, disclosing such sensitive information could enable identity theft and other non-privacy enhancing consumer

⁶⁷ *Id.* at § 999.306(e)(1).

⁶⁸ *Id.* at § 999.313(c)(4).

⁶⁹ Cal. Civ. Code §§ 1798.82(g), (h).

effects, such as indirectly exposing private details about a consumer’s life. ANA supports the CA AG’s efforts to restrict certain data elements from disclosure all together, as this restriction is privacy protective for consumers and serves to help businesses comply with California law.

c. Adopting a Risk-Based Approach to Verifying Requests to Know and Delete

The proposed rules require a business to establish, document, and comply with a reasonable method for verifying that the person making a request to know or a request to delete is the consumer about whom the business has collected information.⁷⁰ The proposed rules also note that businesses may consider a number of factors to determine a reasonable verification method, such as: the type, sensitivity, and value of the personal information collected and maintained; the risk of harm to the consumer posed by unauthorized access or deletion; the likelihood that fraudulent or malicious actors would seek the personal information; whether the personal information to be provided to verify an identity is sufficiently robust to protect against fraudulent requests; the manner in which the business interacts with consumers; and available verification technologies.⁷¹ ANA supports this flexible, risk-based approach to verification presented in the proposed regulations. This non-prescriptive framework allows businesses to reasonably tailor their verification processes to the sensitivity of the data at issue and their own practices.

* * *

We thank the CA AG for the opportunity to submit comments on the proposed regulations interpreting the CCPA. We look forward to continuing our productive dialogue with the CA AG on this matter and the important issue of consumer privacy. Please do not hesitate to contact us with any questions you may have regarding these comments.

⁷⁰ Cal. Code Regs. tit. 11, § 999.323(a) (proposed Oct. 11, 2019).

⁷¹ *Id.* at § 999.323(b)(3).

Message

From: Kammerer, Susan [REDACTED]
Sent: 12/7/2019 12:05:31 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: APCA Comments - CA CCPA Regulations
Attachments: 19-12-06 CA CCPA Regulations - APCA Comments - Final.pdf

Please see attached.

Thank you,

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

Please Note - My Email address has changed effective January 21, 2019 to: [REDACTED]





December 6, 2019

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

VIA Electronic Mail: PrivacyRegulations@doj.ca.gov

To Whom It May Concern:

The American Property Casualty Insurance Association (APCIA) appreciates the opportunity to provide feedback on the proposed California Consumer Privacy Act Regulations (proposed regulations). APCIA is the preeminent national insurance industry trade association, representing property and casualty insurers doing business locally, nationally, and globally. Representing nearly 60 percent of the U.S. property casualty insurance market, APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers. APCIA represents the broadest cross-section of home, auto, and business insurers of all sizes, structures, and regions of any national trade association.

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

General Observations

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

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

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

Connecting the Business use with Personal Information

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

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

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

Requirement to obtain Affirmative Consent for New Uses of Information

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

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

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

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

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

CCPA Disclosure in the Privacy Policy

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

Right to Opt-Out

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

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

Privacy Notice

Privacy Policy Examples

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

Availability in Multiple Languages

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

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

Webpage Link for CA Specific Consumer Privacy Rights

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

Disclosure of the Verification Process

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

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

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

Notice of Improper Use of Minor's Data

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

Too Many Required Disclosures in the Privacy Policy

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

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

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

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

Responding to Requests to Know and Delete

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

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

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

Requests to Know

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

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

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

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

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

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

Moreover, there is a blanket requirement that if a business could not verify the identity of the requestor it must deny the request to delete and, instead, treat the request as one to opt-out. Our position is that the interest of consumers is poorly served by this provision. For instance, if an ex-spouse tries to request deletion of a current consumer's data, but his/her request cannot be verified, then in practice you are giving the ex-spouse the authority to automatically opt the current consumer out of anything. This appears contrary to the rights that the CCPA advocates for, such as individual control.

Requests to Delete

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

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

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

Service Provider

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

Authorized Agent

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

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

Methods for Submitting Requests

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

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

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

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

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

Requests to Opt-Out

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

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

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

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

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

Definitions

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

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

CCPA Scope

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

APCIA appreciates the opportunity to provide feedback. Please, let us know if you have any questions or would like additional information.

Respectfully submitted,

Message

From: [REDACTED]
on behalf of Katie Kennedy [REDACTED]
Sent: 12/6/2019 11:45:40 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Apple Inc Comments to the California Department of Justice re CCPA
Attachments: Apple Inc Comments to California Department of Justice re CCPA Regulations.pdf

To Whom It May Concern:

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

Please do not hesitate to reach out with any questions.

Thank you,

Katie

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



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

At Apple, we believe privacy is a fundamental human right. We purposely design our products and services to minimize our collection of user data. When we do collect personal information, we are transparent about it and take steps to provide users with choice and control. And we work to disassociate it from the user where possible. The customer is not our product, and our business model does not depend on collecting vast amounts of personal information to enrich targeted profiles on individual consumers marketed to advertisers.

We are proud of our deep commitment to protecting consumer privacy. However, we also recognize that privacy needs to be protected by safeguards that go beyond the commitments of individual companies. Laws and regulations are needed to ensure that individuals can understand how their personal information is used and trust that their privacy will be respected, regardless of the values or business model of the particular company that is processing their data.

As a technology company continuously pushing the bounds of innovation, we understand the immensely important role that user data plays in providing valuable services for consumers. But respect for user privacy and the provision of innovative, data-driven services are not mutually exclusive; you can have great user experiences *and* great privacy. To achieve this, we need a thoughtful privacy law that takes a comprehensive view of the interests at stake and appropriately balances important consumer privacy considerations with the benefits that individuals can derive from transparent and respectful use of their data. To be effective, this law must not only deter harmful uses of personal information, but also encourage businesses to rethink their collection and use of personal information by incentivizing the creation and deployment of privacy-preserving architectures and technologies – including, for example, on-device processing.

We applaud the California Attorney General's office for the work it has done in collecting pre-rulemaking comments and drafting regulations for the California Consumer Privacy Act. We respectfully offer the following comments on certain key issues in the proposed regulations where the Attorney General has the power to make revisions that could clarify ambiguities, encourage privacy-protective and consumer-friendly practices, and mitigate the risk of unintended negative consequences.

As discussed in more detail below, we encourage the Attorney General to clarify the meaning of the "household" definition and limit disclosures of "household" data that may undermine consumer privacy. We also encourage the Attorney General to promote the use of consumer-friendly online CCPA rights request portals by removing unnecessary barriers to the provision of such portals, recognize the importance of encouraging innovation in proper authentication and verification practices, and clarify the role of service providers in the rights request process.

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

Apple
One Apple Park Way
Cupertino, CA 95014



I. The current definition of “household” legislates affiliations among persons and risks violating constitutionally protected privacy rights. The Attorney General should clarify the definition of “household” to help prevent such violations.

Given the CCPA’s unprecedented privacy protections for “household” data, it is important that the definition of “household” be precisely crafted in order to ensure that consumer personal information remains protected from unintentional disclosures and bad actors. Data about public or commonly accessible devices can yield significant amounts of information about people, including, in some cases, potentially sensitive data. Unfortunately, the proposed regulations’ sweeping approach to “households” creates a significant risk that consumers may suffer privacy intrusions both from unrelated and unknown persons *and* from members of their (actual) household.

The proposal to define a “household” around “a person or group of people occupying a single dwelling,” Regulations § 999.301(h), will likely result in unrelated or unaffiliated people being grouped into a single “household.” This broadly scoped definition lacks context or distinction between different types of dwellings, meaning that entire college dorms, retirement homes, apartment buildings, condominiums, or any other multi-family building could potentially be treated as a single “household” under the CCPA. Such an outcome would lead to unintended disclosures of data and, as a result, perversely cause the CCPA to undermine consumers’ privacy. Additionally, the definition’s use of the word “occupying”¹ and the failure to require that the occupants maintain any permanent or extended connection to the dwelling could allow temporary guests to be treated as members of the household. For example, a guest of a family who visits on occasion (*e.g.*, a cousin, family friend) may use the family’s Wi-Fi a few times every year. Under the broad definition of “household,” this pattern of activity could potentially allow a business to conclude that the guest also “occupies” the family’s dwelling and is therefore part of the household and entitled to access the “household” data. This same problem will be present in the short-term rental context, where a number of unrelated persons who occupy the same dwelling at different points over the course of a year may all be considered to be part of the same “household.”

¹ The word “occupy” can be interpreted to cover a guest’s temporary stay in a location. See, *e.g.*, Oxford English Dictionary Online, <https://www.oed.com/view/Entry/130189?redirectedFrom=occupy#eid> (giving as a definition of the verb “occupy” “to be situated, stationed, or seated at or in, to be at or in (a place, position, etc.)”). Certain California laws also treat the word “occupant” as being interchangeable with “guest.” See, *e.g.*, Cal. Health & Safety Code § 18862.30 (“‘Occupant’ and ‘resident’ shall be interchangeable and shall include ‘occupant,’ ‘resident,’ ‘tenant,’ or ‘guest’”). Additionally, while the word “occupant” is sometimes used in California law to refer to persons who live in a dwelling, the definitions of the word in these contexts often do not require a particularly close connection between the persons living in the dwelling. See, *e.g.*, Cal. Code Regs. tit. 17, § 56901 (defining “occupant” as “any individual living in the facility, including consumers and non-consumers, the owner/operator and his/her family members, and live-in staff.”); Cal. Civ. Code § 1946.8 (defining “occupant” as “any person residing in a dwelling unit with the tenant. . . includ[ing] lodgers”).



In addition to its broad scope, the proposed “household” definition also fails to require a close or intentional connection between the members of a “household.” This absence of limiting conditions may lead to violations of the CCPA and consumers’ constitutionally protected right to privacy. For example, unrelated consumers who are grouped in the same broadly defined “household” (e.g., roommates, people who reside in separate units within a multi-unit apartment building) may gain information about other members of their “household.” Such privacy violations may lead to a range of negative consequences, such as, embarrassment, fraud, identity theft, and even physical harm. For example, a household member who is simply interested in learning about the household data that pertains to their own activities may unintentionally obtain data related to other members of the household. The consequences may be more severe if a bad actor seeks to use household data for malicious purposes (e.g., obtaining information about the activities of other members of a “household” for the purpose of stalking another resident of a multi-unit apartment building).

The risks of the harms described above will disproportionately affect economically disadvantaged Californians. While some Californians may reside in “households” with persons whom they have chosen to affiliate, others have less control over their living situations and will not be able to easily relocate to a different “household” to avoid the risks of privacy violations.

Even in the case of closely related consumers who reside in the same household (e.g., spouses, adult children residing with their parents), the broad “household” concept may allow such consumers to violate each other’s privacy in undesirable and unexpected ways. For example, spouses may have separate devices (e.g., computers, mobile phones) and have a reasonable expectation that their spouse will not have access to data related to their non-shared devices. However, a request for the household’s data could yield information about the activities of their shared devices and even non-shared devices if the business views such devices as being tied to the household and not any particular consumer. Such an outcome could effectively force some consumers to partially forgo their privacy and data autonomy merely because they choose to live with other people. In some cases, these privacy violations could even create significant risks of physical harm. For example, an abusive spouse in a two-person household may submit access requests to nearby domestic abuse support centers and family law practices in order to determine whether someone from their household viewed their websites or contacted them (e.g., requesting data that may have been collected about a household device navigating a law firm’s website), and, in some cases, even obtain copies of the communications made from their household.

The CCPA and the draft regulations do not currently include adequate safeguards to protect against the risks noted above. For example, the draft regulations allow businesses to respond to non-account-based requests for household data with aggregate household data. However, access to aggregate household PI still creates significant risks to consumers. For example, aggregate data about a household’s interaction with various websites and services would allow any member of that household to gain insight on the interests and activities of other members of that household. If combined with other information the household member may have (e.g., knowledge about one’s neighbors or roommates), some of this aggregate information could possibly be tied back to particular members of the “household,” thereby effectively revealing



those persons' personal information. In some cases, this information could be used in harmful ways, such as the stalking and domestic abuse scenarios outlined above.

Although the CCPA includes a broad exception that allows for the denial of requests that would "adversely affect the rights and freedoms of other consumers," CCPA § 198.145(l), this provision is not sufficient to protect consumers against the risk of harm created by the proposed regulations' broad definition of household. For example, it puts the burden on individual businesses to determine whether their provision of household personal information in response to a verified request will create risk to consumers, and different businesses may reasonably come to different conclusions. In many cases, businesses will simply not have enough information about the context of the request to know whether such risks exist.

To help mitigate significant risks created by the inclusion of the "household" concept in the CCPA, the definition of "household" should be narrowed to ensure that the benefit of granting consumers access to household information is adequately balanced against the risks that such access may create. At a minimum, "households" should be limited to consumers who: (1) reside at the same address; (2) share a common device or service provided by the business; and (3) are identified by the business by reference to a permanent unique identifier, shared account, or group or family account, if such account type is made available by the business. The combination of these three elements is a more accurate threshold for whether persons actually share a "household" relationship and desire to be viewed as a single, related entity by a business than the existing test of "occupying a single dwelling." Requiring household members to "reside" at the same address would reflect the intent to exclude guests. Requiring that household members share a common device or service may increase the likelihood that the relevant consumers actually view themselves as part of a common household. When two users share a device or account, they are also more likely to understand that other users of the device or account may have access to the information stored on that device or account. Finally, requiring businesses to look to a shared identifier, such as a permanent unique identifier or shared account, may increase the likelihood that the relevant consumers actually view themselves as sharing a household relationship. For example, under this definition, two people who reside at the same multi-unit apartment building and maintain separate accounts with an Internet service provider would not be treated as a single "household." This would be an improvement from the existing definition, which could be interpreted to treat these people as a single household simply because they both occupy the same "dwelling."

II. The regulations should prohibit businesses from disclosing aggregate household data in response to requests made outside of password-protected accounts.

As discussed above, the current definition of "household" is overly broad and creates a significant risk of privacy violations and other harms for consumers. In addition to the changes suggested above, the Attorney General should seek to mitigate these risks further by removing the provision that allows businesses to provide aggregate household data in response to requests made outside of password-protected accounts.



The disclosure of aggregate household data can still provide a great deal of insight about the members of a “household.” This is particularly the case in smaller households. For example, a request from one resident of a two-person household would effectively disclose the personal information of the other household member, as the requestor could deduce how the aggregate data differed from their own data. Despite this risk of harm, the proposed regulations currently allow aggregate data to be provided in response to a request that is not made via a password-protected account. While such requests must still be verified pursuant to section 999.325 of the regulations, such a process would allow one member of the household to submit a verifiable request to obtain aggregate data that pertains to all members of the household. Given the potentially sensitive nature of some aggregate household personal information and the risk of harm posed by its unauthorized disclosure to other members of the “household,” this provision should be removed.

III. The Attorney General should remove certain proposed restrictions on the use of online portals to promote secure and efficient responses to consumer rights requests.

Apple supports the Attorney General’s decision to make self-service portals an acceptable method for allowing consumers to access, view, and receive a copy of their personal information. However, there is a risk that the proposed requirement that such portals “fully disclose[] the personal information that the consumer is entitled to under the CCPA,” Regulations § 999.313(c)(7), may deter businesses from using such portals and thereby deny consumers a convenient and secure means of exercising their rights.

While much of the personal information that consumers are entitled to under the CCPA will likely be producible in file formats and sizes that are deliverable through an online portal, there may be situations where this is not the case. For example, it may be more efficient to provide personal information from certain databases directly to the consumer via email instead of first sending that data to the online portal. It may also not always be feasible to deliver files of certain sizes or formats via the online portal. Provided that a business is transparent about how the consumer will receive their personal information in response to an access request, there is no harm to the consumer from a business’s use of more than one medium of delivery. However, the risk of being found noncompliant with the unnecessarily strict proposed language may deter some businesses from offering otherwise consumer-friendly and secure portals if they cannot guarantee that their portal will be a feasible means of delivery for all information in all instances.

To encourage the use of portals, the Attorney General should remove the requirement that they fully disclose all information required by the CCPA. If such a change were adopted, the regulations would still encourage the use of secure self-service portals, while recognizing that, in some instances, the most efficient and secure way of delivering consumer information will be a combination of portal and non-portal means. Such an approach would be consistent with the EU’s General Data Protection Regulation (GDPR), which encourages the use of portals to fulfill the access right (“[w]here possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal



data”), but does not expressly require that all personal data be provided via the portal. GDPR, Recital 63.

IV. The verification requirements must be flexible enough to allow businesses to adapt in response to future threats and protect consumers by always requiring that businesses verify identities to a “reasonably high degree of certainty.”

To protect consumer privacy, it is essential that the regulations require robust, yet flexible verification standards, so that bad actors cannot take advantage of published processes to steal and exploit consumers’ personal information. At Apple, our experience with protecting consumer data has taught us that bad actors are constantly developing new strategies, and companies need innovative and dynamic strategies to counter these efforts. Including specific verification procedures in the regulations may cause businesses to become reliant on the prescribed processes, even when the prescribed processes may not be sufficient to protect consumers’ personal information from attack. Such an outcome would be harmful to consumers, as the prescribed procedures will likely be ineffective in certain contexts today and are even more likely to become obsolete in the future.

Currently, the proposed regulations describe two specific processes for verifying a request to a reasonable degree of certainty (matching at least two pieces of information) and a reasonably high degree of certainty (matching three pieces of personal information and obtaining a signed declaration). Regulations § 999.323(b). There are many instances in which these processes may not provide for meaningful verification. For example, an increasing availability of compromised payment and identity data have led to increasing e-commerce fraud across the online ecosystem. Some bad actors can easily identify valid billing addresses and certain identity data to pair with compromised accounts to meet the proposed verification methods and violate consumers’ privacy rights. As another example, the FTC has warned about the threat of SIM swap scams, which may defeat security systems that rely on telephone numbers alone as a means of authentication. And many of the most common security questions used to secure online accounts can be answered with a search of public records. Each of these examples demonstrates that many bad actors could likely provide two or three pieces of data that match data held by a business, rendering the prescribed processes ineffective. Additionally, the required signed declaration for “reasonably high degree of certainty” verifications seems unlikely to serve as a meaningful obstacle to fraudulent requests. Bad actors routinely falsify documents, and many businesses may not have a requestor’s authentic signature on file or be able to accurately identify fraudulent signatures.

If the Attorney General adopts the prescriptive matching procedures, businesses and courts will almost certainly gravitate towards viewing them as the standard for determining whether a business has a reasonable verification process. Due to the flaws with these approaches, such an outcome may allow bad actors to frequently use the CCPA process to gain unauthorized access to consumer personal information. These risks will only increase in the future, as bad actors who study the published regulations will no doubt work to develop new techniques for bypassing the two/three data point and signed declaration requirements.



To combat the ever-evolving strategies of bad actors, businesses need to (and should be encouraged to) continually seek out and develop innovative and dynamic approaches to securing consumers' personal information. At Apple, we have implemented a wide range of tools and processes to protect our users and our systems from bad actors, including two-factor authentication. The security tools and processes that we use have changed over time to counter evolving threats, and they will continue to evolve in the future. Instead of cementing prescriptive verification procedures into law, the regulations should aim to encourage additional, evolving approaches to verification, along with robust minimum standards that prioritize consumer privacy.

To support strong minimum standards for identity verification, ongoing enhancements to consumer verification procedures, and deny bad actors inside knowledge of businesses' verification techniques, the Attorney General should revise the proposed regulations to require a reasonably high degree of certainty before disclosing consumer information and remove the specific descriptions of the data point matching verification techniques.

Further, as the right to privacy is fundamental and belongs to the individual, a business should not be required to respond to any request to exercise a privacy right unless it can verify the identity of the requestor. Anything less than that would obligate businesses to take risks with privacy rights and greatly increase the risk that a business grant one person's rights to another. And, attempts to have alternative criteria for different circumstances would leave companies open to an undermining of standards. Additionally, socially-engineered efforts to exploit the differences in verification standards could lead not only to exploited privacy rights but could also be the first step in a bad actor's quest to gain knowledge of certain personal information and leverage that knowledge to gain access to other, more sensitive, personal information. There are no tiers of fundamental rights, we do not believe there should be tiers of acceptable verification.

V. The Attorney General should clarify that service providers shall respond to consumer requests solely by directing the consumer to contact the relevant business(es) on whose behalf the service provider is working.

To promote the accurate and efficient fulfillment of consumer rights requests, the regulations should be revised to clarify that service providers shall respond to consumer requests solely by directing the consumer to contact the businesses on whose behalf the service providers collect personal information. The proposed regulations are not entirely clear regarding the role of service providers in responding to consumer requests. The draft regulations imply that service providers may act on consumer requests (*i.e.*, if a service provider receives a request, but does not fulfill the request, it shall "explain the basis for the denial"). Regulations § 999.314(d). However, the same section also provides that a service provider shall "inform the consumer that it should submit the request directly to the business on whose behalf the service provider processes the information and, when feasible, provide the consumer with contact information for that business." This sentence implies that the business, and not the service provider, is the entity that should receive and act on rights requests. Therefore, the proposed regulations seem



to allow a service provider to either evaluate and act on consumer requests or direct the consumer to the appropriate underlying business. Such a system is prone to causing confusion among consumers and businesses and may increase the likelihood of mistakes during the consumer rights request process.

As the entity that “determines the purposes and means of processing consumers’ personal information,” CCPA § 1798.140(c), the “business” should have sole responsibility for evaluating and acting on consumer rights requests. The business is best positioned to know what information it has about a given consumer and how such information is being used. Such information is critical for evaluating a consumer request and ensuring that the privacy interests of the CCPA and the other public interests and policy concerns are properly respected. A service provider that attempts to respond to a request with an incomplete picture of how the consumer’s information is used is also more likely to provide an incomplete and potentially incorrect response to the rights request (e.g., a service provider may not be aware that certain personal information is relevant to an ongoing investigation and therefore fail to apply the proper exceptions to a deletion request).

Clearly establishing the “business” as the single point of contact for CCPA requests will also help reduce consumer confusion. Under the current regulations, consumers may be confused about whether they have to submit CCPA requests to a business, its service providers, or all of these parties. Such an approach would also align the CCPA with the GDPR, which places the responsibility for responding to data subject requests with the “controller” (i.e., the entity that determines the purposes and means of processing personal data). GDPR, Art.12-22.

Revising the regulations to clarify the limited role of service providers in responding to consumer requests would be consistent with the CCPA’s transparency goals, more fully respect the variety of stakeholder and policy interests that may be impacted by CCPA requests, and promote the efficient fulfillment of consumer requests.

Message

From: Tobin, Timothy P. [REDACTED]
Sent: 12/6/2019 11:49:39 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Auto Alliance Comments on the Proposed California Consumer Privacy Act Regulations
Attachments: Alliance CCPA NPRM Comments 20191204_SB_2.pdf

To Whom it May Concern:

Please find attached comments on the CCPA by the Alliance of Automobile Manufacturers (the "Auto Alliance").

Regards,

Timothy Tobin

Partner

Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004

Tel: [REDACTED]
Direct: [REDACTED]
Fax: [REDACTED]
Email: [REDACTED]
Blog: www.hldataprotection.com
www.hoganlovells.com

Please consider the environment before printing this e-mail.

About Hogan Lovells

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

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



December 6, 2019

California Office of the Attorney General
ATTN: Privacy Regulations Coordinator
300 S. Spring Street, First Floor
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

RE: Comments of the Alliance of Automobile Manufacturers on the California Attorney General’s Proposed California Consumer Privacy Act Regulations

To Whom It May Concern:

The Alliance of Automobile Manufacturers (“Alliance”) welcomes the opportunity to provide these comments (“Comments”) to the Attorney General’s Office regarding the Proposed California Consumer Privacy Act Regulations.

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. 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.

Automakers have long recognized the potential privacy considerations raised by collecting data in association with connected vehicle technologies and services. And automakers have taken proactive steps to protect consumer privacy. In 2014, the Alliance, the Association of Global Automakers (a trade association representing U.S. operations of certain international vehicle manufacturers and original equipment suppliers), and their respective members issued the Privacy Principles for Vehicle Technologies and Services (“Principles”).¹ The Principles were groundbreaking. The Alliance’s members have all committed to meet or exceed the commitments contained in the Principles when offering innovative vehicle technologies and services.

The Alliance and its members appreciate the careful work that the Office of the Attorney General has undertaken in drafting the proposed regulations. In particular, the Alliance welcomes the following aspects of the proposed regulations:

- Clarifying that businesses need not provide consumers with specific pieces of personal information in response to access requests if the disclosure of the information creates a substantial, articulable, and unreasonable risk to the security of that personal information, the

¹ Consumer Privacy Protection Principles (2014) [hereinafter “Principles”], *available at* https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf.



- consumer's account with the business, or the security of the business's systems or networks. As reflected in the comments below, however, the Alliance does request that the Attorney General clarify that disclosure should not be required where there is a substantial, articulable, and unreasonable risk to the safety or security of consumers, and not just their personal information.
- Clarifying that businesses shall not disclose certain types of sensitive information in response to a consumer's request to know. The Alliance requests, though, that the Attorney General issue regulations permitting businesses to not disclose personal information in response to a request to know where such disclosure poses a significant risk to consumers, and not just to the information itself.
- Permitting businesses to offer granular options for sale opt-out and deletion requests, so long as the options to opt-out of all sales or delete all information are presented more prominently than any other option.
- Permitting businesses to provide aggregate household information in response to a request to know household information where the requestor does not have a password-protected account. The Alliance believes that requests to know for shared devices should be afforded the same treatment as they raise the same privacy concerns as households.

The remainder of this submission contains requests for additional modifications to the proposed regulations, including those referenced above. We present first those requests that are of particular relevance to the Alliance and its members and follow with requests of general relevance:

Requests and Comments of Particular Relevance to the Alliance and Its Members

- Permitting automakers to retain vehicle-related information for purposes of analyzing and addressing safety, quality, performance, efficiency, or security issues after receiving a request to delete;
- Permitting reasonable, beneficial data sharing among manufacturers, suppliers, and dealers given the close relationship the parties have in serving consumers;
- Permitting businesses to share personal information with providers of emergency response services even where sales opt-outs have been registered;
- Providing reasonable options for businesses to comply with notice at collection requirements in the context of devices that may be resold or used by multiple individuals when the business that collects information from the devices does not know of the sale or use of the device by multiple individuals;
- Permitting businesses to disclose only aggregated information related to shared devices unless all users submit verified requests; and
- Permitting businesses to not disclose information pursuant to a request to know if the disclosure exposes consumers or others to safety or security risks.

Requests and Comments of General Relevance

- Clarifying that with appropriate notice at the point of collection, a consumer's provision of personal information to a business involved in a clearly disclosed, jointly offered service constitutes an intentional disclosure under Cal. Civil Code §1798.140(t)(2)(A);



- Deferring action on the requirements and standards for user-enabled privacy controls pending the outcome of the proposed California Privacy Rights Act Initiative that would address this issue;
- Requiring explicit consent for new uses of personal information only if the change in practice is material;
- Clarifying that businesses may comply with notice at collection requirements when not collecting personal information from consumers by obtaining examples of consumer notices and a single attestation from data sources, rather than obtaining examples and attestations for each consumer;
- Permitting businesses to require authorized agents to use the same verification process that consumers would have to undergo if submitting requests on their own behalf;
- Removing from the proposed regulations the requirement that businesses receiving sales opt-out requests notify all third parties that received personal information via sales in the 90-day period prior to the opt-out that they may not further sell the information;
- Clarifying that businesses are permitted, but not required, to use signed declarations when verifying consumer requests;
- Permitting businesses to present in their privacy policies information about the sources, use purposes, and disclosures associated with all personal information collected by the business, rather than specifying by category, so long as the disclosure reasonably helps consumers understand processing activities;
- Clarifying that each right to know request (e.g., request to obtain access to specific pieces of personal information and request to learn about the categories of personal information collected about the particular consumer) counts toward the number of requests that a business must respond to within a 12-month period;
- Requiring businesses to disclose information about the sale of personal information related to minors only if businesses have actual knowledge that they collect such information;
- Permitting businesses to display the Do Not Sell My Personal Information link only on the main page of a website and in the privacy policy, rather than requiring the link on every page, which could lead consumers to believe that they must opt-out on every page they visit.
- Clarifying that businesses may, at their discretion, use fact-finding to verify a consumer request, where personal information is maintained in a format not associated with a named individual; and
- Permitting businesses to not disclose proprietary or trade secret information in response to a consumer's request to know.

The Alliance appreciates the Attorney General's consideration of these requests and the efforts the Attorney General is undertaking to develop the regulations. Please feel free to contact us if you have any questions or would like to discuss any aspect of these comments.

REQUESTS AND COMMENTS OF PARTICULAR RELEVANCE TO THE ALLIANCE AND ITS MEMBERS

ISSUE 1: Permit Automakers to Retain and Use Vehicle-Related Information Tied to VIN Only for Safety, Quality, Performance, Efficiency, or Security After Receiving a Request to Delete

Automakers often rely on Vehicle Identification Numbers (“VINs”) to link vehicle-related information for purposes of analyzing and addressing safety, quality, performance, efficiency, and security issues. To be able to track how vehicles perform over time for these purposes, including, for example, in different weather conditions and climates, automakers collect data on vehicles by VINs. This VIN-related, longitudinal information is essential to further improve the nation’s transportation and mobility services and infrastructure. Although the benefits of such data rely on the use of VINs, other identifiers typically are not necessary. The Alliance therefore requests that the Attorney General adopt one of the proposals below to enable automakers to retain vehicle data tied to VINs for purposes of analyzing and addressing vehicle safety, quality, performance, efficiency, or security issues.

PROPOSAL 1

Issue interpretive guidance clarifying that vehicle-related data stored in association with Vehicle Identification Numbers and no other identifiers (such as name, account number, postal address, email address, telephone number, or SIM card number) is not considered consumer personal information.

PROPOSAL 2

Issue interpretive guidance clarifying that information that cannot be linked to a particular consumer without the use of additional identifiers is “deidentified” so long as the business maintaining the information stores information that could be used to identify the information separately from the deidentified information and so long as the business complies with the requirements in Cal. Civ. Code § 1798.140(h).

PROPOSAL 3

§ 999.313 Responding to Requests to Know and Requests to Delete

(d)

...

(8) The collection and internal use of personal information for analysis related to safety, quality, performance, efficiency, or security by a business or service provider constitutes “solely internal uses that reasonably aligned with the expectations of the consumer based on the consumer’s relationship with the business” under Civil Code §1798.105(d)(7) and therefore shall not be subject to a request to delete, as long as this collection and use is disclosed to consumers.

ISSUE 2: Exempt Reasonable, Beneficial Data Sharing Between Suppliers, Dealers, and Manufacturers

The CCPA exempts from sale opt-out requirements the sharing of vehicle and ownership information for purposes of effectuating “a vehicle repair covered by a vehicle warranty or a recall” if the

information is not used for any other purpose. However, vehicle manufacturers, auto dealers, and suppliers routinely share information for reasonable, non-warranty, and non-recall purposes that benefit consumers. For example:

- Dealerships may rely on manufacturer data to evaluate past, non-warranty repairs. Franchisor-franchisee sharing arrangements generally, and especially in the vehicle sales context, are efficient and consistent with consumer expectations. The sharing of information allows consumers to receive consistent services from dealers by leveraging the relationships that the dealers have with the vehicle manufacturer.
- Suppliers and manufacturers may exchange vehicle-level data to assess safety, performance, and security-related issues.

Consumers may not recognize that by asking manufacturers, dealers, or suppliers to not sell their personal information, the sharing of information between these parties will be disrupted in ways that directly affect the consumers. When traveling, consumers may be surprised to learn that an out-of-town dealer is unable to obtain past service records. Or when consumers move, automakers may not be allowed to let consumers know of the local dealers that can now service their vehicles. Consumers may not recognize that a sales opt-out may prevent suppliers and manufacturers from analyzing vehicle-performance and efficiency issues.

The sharing of information between legally distinct, unaffiliated businesses that work closely together to provide transportation and mobility services promises great benefits to consumers, who may not even recognize that such sharing, which can be among entities that use a common brand, constitutes a sale.

The Alliance therefore requests that the Attorney General clarify that such data sharing practices are not subject to the sales opt-out.

PROPOSAL 1

The Attorney General's office could issue interpretive guidance clarifying that where sharing is consistent with reasonable, informed consumer expectations and benefits consumers with regard to motor vehicle safety, security, repair, performance, or efficiency, such sharing would not be considered a "sale."

PROPOSAL 2

Adopt the following regulation

§ 999.315 Requests to Opt-Out

...

(i) A request to opt-out does not apply when information is exchanged between parties whose commercial conduct is related to the degree that informed consumers would reasonably expect the parties to share information for the purposes of benefitting the consumer with regard to safety, security, repair, performance, or efficiency issues.

PROPOSAL 3

Adopt the following definition:

§ 999.301 Definitions

“Sell,” “selling,” “sale,” or “sold,” does not include a transfer of information between parties whose commercial conduct is related to the degree that informed consumers would reasonably expect the parties to share information for the purposes of benefitting the consumer with regard to safety, security, repair, performance, or efficiency issues.

ISSUE 3: Permit Businesses to Share Personal Information with Providers of Emergency Response Services Even Where Sales Opt-Outs May Apply

Many businesses, including automakers, provide emergency response services to consumers. In emergency situations, automakers may provide these services to consumers even if they have not subscribed to or have previously opted-out of the services. Some emergency and roadside assistance services may be provided by third-party, for-profit entities that retain and use personal information for their own purposes. For example, an emergency roadside assistance provider may be an independent mechanic that wishes to establish and maintain an independent relationship with the consumer. In some cases, an accident may automatically trigger a communication from a vehicle to an emergency provider. Even though this may be a direct disclosure from the vehicle to the provider and might not involve a transfer of personal information to the automaker and then the provider, the CCPA’s definition of sale includes “making available” personal information to another entity. Accordingly, when automakers share personal information with such emergency and roadside assistance providers or make it available to them through an automatic process from the vehicle, the disclosures may constitute “sales” under CCPA. If consumers have opted-out of sales, that could prevent automakers from disclosing personal information as necessary to support the delivery of emergency services.

The Alliance therefore requests that the Attorney General permits businesses, in response to a consumer’s request for emergency or roadside assistance services, or in response to automated crash or similar notifications, share personal information with providers of such emergency or roadside assistance services.

PROPOSAL

Provide interpretive guidance that an automaker may share personal information with emergency responders or roadside assistance providers or make it available from the vehicle in emergency situations regardless of whether the consumer associated with the personal information has requested that the automaker not sell the personal information.

ISSUE 4: Modify Notice at Collection Requirements to Support Reasonable Compliance by Businesses that Manufacture Devices Reasonably Subject to Resale or Use by Non-Owners

The CCPA requires businesses to provide consumers with notice, at or before data collection, of the categories of personal information to be collected and the purposes for which the information will be used. The draft regulations add a number of obligations to this requirement, including making the notice visible or accessible where consumers will see it before any personal information is collected; using formats that draw consumer attention, including on smaller screens; and making the notice accessible to consumers with disabilities.

These requirements may present challenges for resold devices, such as certain connected vehicles, that lack displays or have displays that cannot be remotely updated. Even with displays that can be remotely updated, an automaker, for example, may have no knowledge of a vehicle resale and therefore may not be able to provide notice to the new owner. If businesses have no knowledge that a device has been resold and the device has no interface via which to present a privacy notice, businesses may be unable to guarantee that subsequent owners receive notice at or before collection of information from the sold device.

The regulations should permit notice at collection options that support reasonable compliance by businesses that collect information from devices that may change owners without notice.

Similarly, devices such as vehicles that have multiple users may collect personal information from different users. The regulations should clarify that where initial notice is provided to a registered user or account holder, the notice is sufficient with respect to non-registered users that the account holder permits to use the vehicle, device, or service.

PROPOSAL

§ 999.305 Notice at Collection of Personal Information

...

(e) A business that collects personal information via a device that is reasonably expected to change owners should take reasonable steps to provide notice at collection to subsequent purchasers of that device. The business will be deemed to have taken reasonable steps if:

(1) Notice is provided to the new owner via email, device updates, or upon device reset or reactivation; or

(2) The business posts a privacy policy on its website, if reasonable notice cannot be provided by the methods above.

(f) Notice to the owner of a device or account-holder of a service at collection constitutes notice at collection as to other users of the device or service.

ISSUE 5: Permit Businesses to Disclose only Aggregated Information Related to Shared Devices Unless All Users Submit Verified Requests

The Attorney General's draft regulations include provisions designed to address the potential privacy issues associated with requests to access or delete household information. The draft regulations propose that where a consumer does not have a password-protected account with a business, businesses may respond to requests to know related to household information by providing aggregate information. Businesses may choose to honor requests to delete or obtain access to specific pieces of information when all household members jointly issue such requests, subject to verification.

The privacy risks posed by household information also apply in the context of shared devices. Requiring compliance with the access or deletion request of a single individual with respect to a shared device could harm the privacy interests of the other individuals who use the same device. For example, a co-owner of a vehicle could request access to precise geolocation information and therefore see the other co-owner's travel history, or could delete all personal information associated with a vehicle, which request the other co-owner of the vehicle would not have agreed to. The

Alliance thus requests the Attorney General adopt provisions extending the provisions for household information to information collected from shared devices.

PROPOSAL 1

§ 999.318. Requests to Access or Delete Household or Shared Device Information

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

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

PROPOSAL 2

§ 999.319. Requests to Access or Delete Shared Device Information

(a) A business may respond to a request to know personal information relating to a device intended for use by multiple users by providing aggregate information, subject to verification requirements set forth in Article 4.

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

ISSUE 6: Businesses Should Not Be Required to Disclose Information that Exposes Consumers or Others to Safety or Security Risks

The draft regulations clarify that businesses need not provide consumers with specific pieces of personal information in response to access requests if the disclosure of the information creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks. The Alliance welcomes these exceptions to the right to know, and the benefits to security which will result.

However, the right to know poses risks not only to the security of personal information, consumer accounts, and business systems or networks, but also to consumers themselves or other individuals (e.g., where the information disclosed may relate to more than one individual and may be misused by the recipient against another individual to whom the data also relates). For example, many vehicles are driven by more than one individual, including family members or friends. Automakers have no way of knowing whether or how frequently a non-owner drives a vehicle. The disclosure of the precise location history of a vehicle can create stalking or harassment risks, endangering individual or public safety. Specifically, if a business disclosed to the owner of a vehicle the precise location history of that vehicle on grounds that the information is reasonably linked to the owner by

virtue of ownership, that could enable an abusive owner to track and harm an estranged spouse, domestic partner, or others whose traveling patterns are revealed to the owner. In some cases, no level of verification could assure an automaker that an individual has not let another individual drive his or her vehicle.

The Alliance therefore requests that the Attorney General extend the exceptions to the right to know to include exceptions for individuals' safety or security. Such a change would be consistent with Cal. Civil Code § 1798.145(m), which states that "[t]he rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers."

PROPOSAL

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

...

(3) A business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, ~~or~~ the security of the business's systems or networks, **or the safety or security of the requesting consumer or other individuals.**

REQUESTS AND COMMENTS OF GENERAL RELEVANCE

ISSUE 7: With Notice, Allow the Sharing of Personal Information with Joint Offering Partners Even Where Sales Opt-Outs May Apply

Jointly offered goods or services create significant efficiencies and benefit consumers by enabling businesses to offer and provide consumers a product or service they might not otherwise be able to obtain. Jointly offered goods or services frequently require for recordkeeping, servicing and other reasons that both distinct businesses collect the personal information and process it for their own respective purposes in providing the joint offering. In other words, each entity is not necessarily a service provider to the other. However, for some jointly offered goods or services, consumers may provide their personal information to only one of the partners, though it is appropriate and expected that the receiving business would share the personal information with the other business.

Especially if consumers are informed at the outset of receiving a jointly offered good or service that their personal information will be shared with a joint offering partner, the activity should not be controversial. As long as there is effective notice and a consumer decides to move forward with entering into a relationship involving a jointly offered good or service, it is reasonable to consider the consumer to be intentionally disclosing their personal information to both partners.

For these reasons, we request that the California Attorney General clarify that with appropriate notice at the point of collection, a consumer's provision of personal information to a business involved in a clearly indicated jointly offered service equates to an intentional disclosure under Cal. Civil Code §1798.140(t)(2)(A).

PROPOSAL

§ 999.315. Requests to Opt-Out

...

- (i) In response to a request to opt-out, a business need not cease sharing information with a third party that receives personal information from the business in association with the provision of a jointly-offered service to the consumer, provided that the identity and participation of the joint offering partner was clearly disclosed to the consumer before the consumer elected to receive the jointly-offered service.

ISSUE 8: Remove User-Enabled Privacy Control Requirements or Make Them Consistent with the California Privacy Rights Act Initiative

The draft regulations would require businesses that collect personal information from consumers online to treat “user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism,” as a request to opt-out. The provision does not clarify what sort of settings or controls should be treated as valid opt-out signals, nor would it allow any period for development and implementation of a technical standard. The Alliance understands that enabling consumer-friendly preference mechanisms can enhance privacy protections. But for such mechanisms to be effective and understandable, there must be standards or a consensus regarding what signals are valid and how signals should be interpreted.

The lack of clarity here is particularly problematic for connected vehicles and other devices that collect information “online” but do not have standard interfaces. It is not clear what would constitute a user-based privacy signal in the connected vehicle ecosystem. Technologically savvy consumers could alter vehicle systems to trigger the transmission of snippets of code whenever data was collected, intending the code to signal an opt-out request. If manufacturers do not know that code is being transmitted or how to interpret the code, the code will not be respected as an opt-out signal. Moreover, requiring vehicles to respond to the random wireless transmission of code to vehicles raises significant cybersecurity concerns. For security reasons, vehicles may not be able to ingest and process any code transmitted to it.

The proposed regulation establishes an all-or-nothing approach to privacy signals that limits consumer choice—consumers may very well wish to restrict sales to some businesses but not others, or restrict sales to data brokers, while permitting third party tags to collect information on websites in order to receive more relevant ads or personalized content.

Moreover, the proposed regulations would mandate activities that would be optional under the California Privacy Rights Act initiative (“CPRA”) that is likely to be voted on and approved in the 2020 election. The CPRA would require businesses either to implement a do not sell signal or to post a “Do Not Sell My Personal Information” link or button and honor do not sell requests through that link or button. And the CPRA would instruct a Data Protection Authority to conduct a rulemaking to flesh out how the automated controls would work.

Given the likelihood of the CPRA taking effect, it is not reasonable for CCPA regulations to require compliance with a not yet elaborated “do not sell” controls framework that is likely to be replaced in a short period of time.

For all these reasons, the Alliance requests that the Attorney General remove from the final rule the requirement that businesses must comply with “user enabled privacy signals” and revisit this issues only if the CPRA Initiative that has been filed with the Attorney General is not approved by the voters in November of 2020.

PROPOSAL

§ 999.315. Requests to Opt-Out

...

~~(c) In response to a request to opt-out, a business need not cease sharing information with a third party that receives personal information from the business in association with the provision of a jointly offered service to the consumer, provided that the identity and participation of the joint offering partner was clearly disclosed to the consumer before the consumer elected to receive the jointly offered service.~~

...

(g) A consumer may use an authorized agent to submit a request to opt-out on the consumer’s behalf if the consumer provides the authorized agent written permission to do so. A business may deny a request from an authorized agent that does not submit proof that they have been authorized by the consumer to act on the consumer’s behalf. ~~User-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.~~

ISSUE 9: Explicit Consent Should Be Required Only for Uses of Previously Collected Information that Are Incompatible with Purposes Disclosed at Original Collection

The draft regulations require businesses to notify and obtain explicit consent from consumers before using personal information for purposes not disclosed in notices at collection. The Alliance and its members agree that businesses should be transparent in their data practices and process information in ways that respect the context in which the information was collected. That is why Alliance’s members have committed to obtain affirmative consent before using certain information in ways that are materially different than what was disclosed at the time of collection. However, the mere fact that a purpose was not disclosed at the point of collection does not mean that the purpose is inconsistent with or materially different from the purposes disclosed at collection.

For example, manufacturers may collect driver behavior information collected for a range of purposes, such as enabling consumers analyze their own driving behaviors. Consumers may expect that manufacturers will use such information to improve vehicle safety, security, and performance, even if every iteration of such purpose is not expressly disclosed in a notice at collection. Moreover, obtaining opt-in consent to any privacy policy change regarding a purpose, even if minor in scope, is burdensome. It also risks consumers not receive the benefit of a new or different purpose that is not such a significant change.

The Alliance therefore requests that the Attorney General follow FTC policy and require explicit consent for new data practices only if the new practices materially differ than those disclosed at the

point of collection.² A material difference would be one that is “likely to affect the consumer’s conduct or decision with regard to a product or service.”³ If a new data processing purpose would not be likely to change the conduct of reasonable consumers, businesses should not be required to obtain consent.

PROPOSAL 1

§ 999.305 Notice at Collection of Personal Information

(a) Purpose and General Principles

...

(3) A business shall not use a consumer’s personal information for any purpose **other than materially different from or incompatible with** those disclosed in the notice at collection. If the business intends to use a consumer’s personal information for a **materially new purpose or a purpose that is not compatible with the purposes was not** previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.

PROPOSAL 2

§ 999.305(a) Notice at Collection of Personal Information

(a) Purpose and General Principles

...

(3) A business shall use a consumer’s personal information for the purposes disclosed in the notice at collection. A business shall not use a consumer’s personal information for a purpose incompatible with the stated purpose at the time of collection without explicit consent.

ISSUE 10: Clarify that Signed Attestations Are Required Per Data Source, Not Per Consumer

The draft regulations include provisions that are designed to support businesses in ensuring that consumers receive notices at collection where the businesses did not collect personal information from the consumers. The regulations provide two options for businesses that do not collect personal information directly from consumers: (1) they can contact the consumer directly to provide notice and the opportunity to opt-out; or (2) they can contact the source of the information to confirm that the source provided adequate notice at collection to the consumer and obtain signed attestations from the source describing how notice was given and an example of the notice.

The draft regulations do not specify whether businesses must obtain signed attestations for each source or for each consumer. Requiring businesses to obtain and store signed attestations on a per consumer basis would lead to substantial data transfer and storage requirements with little benefit. If the attestations and example notices are identical, then a single, representative example would suffice, so long as businesses received confirmation initially from the source that the example was

² *Id.* at viii.

³ FTC, FTC Policy Statement on Deception 1 (1983), available at https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

accurate and representative of those provided to all consumers (or to all consumers in a given context). The Alliance therefore requests that the Attorney General clarify that attestations are required per source of information.

PROPOSAL

§ 999.305 Notice at Collection of Personal Information

...

(d)

...

(2) Contact the source of the personal information to:

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

b. Obtain signed attestations from the source describing how the source **gave gives** the notice at collection and including an example of the notice **or notices the source uses to provide such notice**. Attestations **from each source of information** shall be retained by the business for at least two years and made available to the consumer upon request.

Businesses need not obtain separate attestations for each consumer unless there are material differences in the notices provided to consumers.

ISSUE 11: Businesses Can Require Authorized Agents to Use the Same Verification Processes as Consumers

The CCPA allows consumers to authorize other individuals to opt-out of sales and to submit verified requests for access or deletion of personal information on their behalf. Businesses must take reasonable steps to verify requests. However, establishing unique procedures to verify authorized agents may prove burdensome on businesses and requestors. While it should not be easier for authorized agents to submit requests than it would be for consumers to issue requests on their own, it may not always be reasonable to require authorized agents to undergo processes that are more burdensome than those offered to consumers themselves. Though, in some cases requiring authorized agents to undergo additional verification procedures may be reasonable.

Authorized agents presumably have access to the same information that consumers would have to verify identities. Thus, a reasonable option for verifying requests submitted by authorized agents, at least in some circumstances, would be for businesses to require authorized agents to undergo the same verification as the consumers for whom they act. Authorized agents could “stand in the shoes of the consumer” and provide the same data points that would be requested of the consumer.

The Alliance therefore requests the Attorney General to clarify that businesses may require authorized agents to verify requests via the same processes provided to consumers.

PROPOSAL

§ 999.308 Privacy Policy

...

(5) Authorized Agent

a. Explain how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf, **which may include requiring that the authorized agent provide the same information to the business that the consumer would need to provide if the consumer were making the request on the consumer's own behalf.**

ISSUE 12: Remove Flow-Down Obligation for Opt-Out Requests

The CCPA grants consumers the right to opt-out of future sales of their personal information. Under the draft regulations, a business that receives an opt-out request is required not only to cease selling personal information, but also to notify all third parties to which the business sold the consumer's personal information in the 90 days prior to the consumer's opt-out request that the consumer has opted out, instructing the recipients to not further sell the information.

This look-back requirement goes beyond the requirements set forth in the CCPA. And it may not reflect consumer wishes. A consumer may have specific concerns with a certain business' practices but may have no issue with the practices of the businesses that receive personal information from the initial business. In fact, the consumer may want the receiving business to continue selling personal information due to the benefits received from that business and the associated data sharing which may differ from the consumer's concerns with the business to which the consumer made the sale opt-out request.

PROPOSAL

§ 999.315 Requests to Opt-Out

~~(f) A business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the consumer's request that the consumer has exercised their right to opt-out and instruct them not to further sell the information. The business shall notify the consumer when this has been completed.~~

ISSUE 13: Clarify That Signed Declarations Are Permitted but Not Required for "Reasonably High" Verification of Consumer Rights Requests

The draft regulations provide guidance on how businesses may verify the identity of a consumer before responding to a consumer's access or deletion request. The regulations state that verification to a "reasonably high degree of certainty *may include* matching three pieces of personal information provided by the consumer with personal information maintained by the business" together with a consumer's signed declaration of identity.⁴ The regulation then goes on to state that such declarations must be maintained as part of a business' record-keeping obligations.

⁴ § 999.325(c) (emphasis added).

Although the proposed regulatory language suggests that verification “may include” signed declarations, the final sentence of § 999.325(c) could be interpreted as requiring signed declarations from consumers. Although signed declarations may be warranted in some circumstances, some businesses may be able to verify the identity of a consumer to a reasonably high degree of certainty without such declarations—such as where consumers maintain secure, password-protected accounts.

The Alliance requests clarification that the signed declaration is an optional measure for verification, at the discretion of the business.

PROPOSAL

§ 999.325 Verification for Non-Accountholders

...

(c) A business’s compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. **If businesses elect to rely on signed declarations, Businesses they shall** maintain all signed declarations as part of their record-keeping obligations.

ISSUE 14: Eliminate the Requirement that Businesses Provide the Sources, Purposes, and Sharing Activity for Each Category of Information for Privacy Policy and Access Requests

The CCPA requires businesses to provide consumers in their online privacy policies and in response to access requests, information regarding the categories of personal information collected, categories of sources for the information, purposes for collecting or selling the information, and categories of third parties with whom the business shares the information. The draft regulations specify that in online privacy policies and in response to access requests, these descriptions of sources, purposes, and sharing should be provided for each category of personal information. This requirement would result in privacy policies that are lengthier and more granular than those required by the CCPA, which permits providing three descriptions, one for all sources, one for all purposes, and one for all third parties.

The regulatory requirements may therefore lead to notices that overwhelm consumers and are in tension with the proposed regulatory requirement that privacy policies be “presented in a way that is easy to read and understandable to the average consumer.”

For businesses that rely on the same sources, seek to achieve the same purposes, and engage in common disclosures for all categories of personal information processed, these granular privacy notice requirements will yield little consumer benefit and only serve to make privacy policies longer and less likely to be read by consumers than today. Accordingly, the requirement actually harms consumers. It would be simpler and more transparent for such businesses to provide information about how they process all personal information.

The Alliance therefore asks the Attorney General to modify the disclosure regulation, requiring businesses to provide meaningful information to consumers.

PROPOSAL

§ 999.305 Notice at Collection of Personal Information

...

(b)(2) ~~For each category of personal information, A list of the business or commercial purpose(s) for which it the personal information will be used in a manner reasonably designed to help consumers understand how the business will process personal information.~~

§ 999.308 Privacy Policy

...

(b)(1)(d)(1) ~~For each category of personal information collected, p~~Provide the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties with whom the business shares personal information. The notice shall be written in a manner that provides consumers a meaningful understanding of the categories listed **and the ways in which the business processes personal information.**

§ 999.313 Responding to Requests to Know and Requests to Delete

...

(c)(10) In responding to a verified request to know categories of personal information, the business shall ~~disclose provide for the each identified category of personal information it has collected about the consumer:~~

- a. The categories of sources from which the personal information was collected;
- b. The business or commercial purpose for which it collected the personal information;
- c. The categories of third parties to whom the business sold or disclosed the category of personal information for a business purpose; and
- d. The business or commercial purpose for which it sold or disclosed the category of personal information.

ISSUE 15: Clarify Limitations on Right to Know Requests

The CCPA provides that businesses shall not be required to provide personal information to a consumer more than twice in a 12-month period. Requests to know may take the form of a request for the “specific pieces of personal information” the business has collected about the consumer, or for the “categories of personal information, categories of sources, and/or categories of third parties.” It is unclear whether each type of request would count toward the two-request limit or whether both

types of request, together, count as one request. The Alliance therefore requests that the Attorney General clarify that any single instance of a right to know request counts toward the total number of such requests that a business must honor within any 12-month period.

PROPOSAL

§ 999.313 Responding to Requests to Know and Requests to Delete

...

(c)(11) A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner that provides consumers a meaningful understanding of the categories listed.

(12) A business shall not be required to respond to a consumer's right to know request more than twice in a 12-month period, regardless of whether such right to know requests are for "specific pieces" of personal information or for "categories" of personal information.

ISSUE 16: Require Businesses to Make Statements About Sales of Personal Information Related to Minors Only If Businesses Have Actual Knowledge that They Collect Such Information

The draft regulations apply an "actual knowledge" standard to requirements relating to affirmative authorizations for sale of personal information of children under the age of 16. This "actual knowledge" standard is consistent with existing federal law under the Children's Online Privacy Protection Act. The Alliance requests that this "actual knowledge" standard apply also to the requirements regarding disclosures in privacy notices about whether businesses business sell personal information related to minors. Businesses should not be required to make statements regarding the processing of such information if they do not have actual knowledge that they hold such information.

PROPOSAL

§ 999.308 Privacy Policy

(b)(1)(e)(3) If a business has actual knowledge that it collects or maintains the personal information of minors under 16 years of age, Sstate whether or not the business sells the personal information of minors under 16 years of age without affirmative authorization.

ISSUE 17: Clarify that Placement of "Do Not Sell My Info" Link Only on the Main Page of a Website Meets "Homepage" Requirement

The CCPA requires that a link titled "Do Not Sell My Personal Information" be provided on a business's Internet homepage. The CCPA further defines "homepage" to include "any internet web page where personal information is collected." Thus, the CCPA appears to require that the Do Not Sell button appear on every webpage that collects personal information. Given the breadth of the definition of personal information and typical automated data collection, this for most businesses means each and every webpage, rendering the concept of a homepage meaningless.

Given current business practices, consumers have become accustomed to looking to the footer of a website's main page to find the Terms of Use and Privacy Statement and other legal information, and similarly in the "Settings" link or menu on a mobile app. The Alliance therefore requests that the California Attorney General exercise discretion and allow for the placement of the Do Not Sell link on a website's main page, or on a mobile app's "Settings" or menu page, to satisfy the posting to "homepage" requirement. Placement on every page of a website could be distracting and could create the impression that consumers must opt-out each time the button appears.

PROPOSAL

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

...

(b)(1) A business shall post the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link on the website's **main page homepage** or the download or landing page of a mobile application.

§ 999.315 Requests to Opt-Out

(a) A business shall provide two or more designated methods for submitting requests to opt-out, including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," or "Do Not Sell My Info," on the **main page of the** business's website or **the Settings or menu of a** mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information.

ISSUE 18: Clarify Consumer Rights Request Verification Requirements When Personal Information Is Maintained Without Association with Named Persons

The draft regulations provide that if a business maintains personal information in a manner not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with that information. The regulations contemplate that this "may require the business to conduct a fact-based verification process." This provision is helpful in the automotive context, where manufacturers may retain information associated with a VIN but not a named individual. Vehicle manufacturers may be able to verify that a certain consumer is currently associated with a VIN. But they may not be able to determine whether that consumer is associated with all of the information associated with the VIN. Vehicles change owners and are operated by multiple consumers. So, a VIN may be associated with multiple consumers.

It is not clear from the draft regulations the degree to which manufacturers would be required to perform fact-finding to confirm the consumer request. As noted above, associating the consumer

with the personal information may be challenging. The Alliance therefore requests that the Attorney General clarify that businesses have reasonable discretion to conduct fact-finding.

PROPOSAL

§ 999.325 Verification for Non-Accountholders

...

(e)(2) If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the non-name identifying information. ~~This may require~~ **The business may, in its discretion, take reasonable steps** to conduct a fact-based verification process that considers the factors set forth in section 999.323(b)(3).

ISSUE 19: Exempt Proprietary Information and Trade Secrets from Mandatory Disclosure in Response to a Request to Know

Today's vehicles deploy a variety of sensors and other technologies that collect information relating to vehicle safety, performance, efficiency, and security. Automakers devote substantial resources to determine what combination of sensors, what frequency of data collection, and what combination of information will best address those issues.

Under the CCPA, consumers have the right to request that businesses disclose the specific pieces of personal information that businesses have collected. For automakers, and other businesses, disclosing all of the specific pieces of personal information, particularly if linkages between or uses of sensor data are revealed, would expose proprietary or trade secret information. The Alliance therefore requests that the Attorney General adopt one of the proposals below to prevent businesses from being forced to disclose their proprietary or trade-secret information.

PROPOSAL 1

Issue interpretive guidance clarifying that information that reveals proprietary information or information protected by trade secret or intellectual property rights does not constitute personal information subject to the CCPA.

PROPOSAL 2

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

...

(c) Responding to Requests to Know

...

(12) A business shall not be required to disclose information that would reveal proprietary information or trade secrets in response to a request to know.



Thank you for your consideration,



Jessica L. Simmons
Assistant General Counsel



Message

From: Steve Kirkham [REDACTED]
Sent: 12/6/2019 5:59:00 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Eric Levine [REDACTED]
Subject: Berbix Inc.'s Comments on the Proposed Regulations for CCPA
Attachments: berbix-ccpa-comments-dec2019.pdf

Hi there,

Please find our comments on the proposed regulations for CCPA in the attached PDF. Should you have any questions or prefer another format, please let us know.

Regards,
Steve Kirkham
Co-Founder, Berbix Inc.



2338 Market Street
San Francisco, CA 94114

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

Email: PrivacyRegulations@doj.ca.gov

December 5, 2019

Dear Mr. Becerra,

We're Steve Kirkham and Eric Levine, the co-founders of Berbix, an identity verification company headquartered in San Francisco, California (<https://www.berbix.com/>). Prior to founding Berbix, we led the proactive Trust & Safety efforts at Airbnb.

Berbix serves companies who need identity verification for a broad range of purposes (for example, data subject request verification, age verification, fraud reduction, or compliance with regulatory requirements). Our Software-as-a-Service product enables businesses to seamlessly collect and instantly validate photo IDs, driver licenses, and passports of their customers. Moreover, we offer a selfie match and liveness check feature which makes it possible to deterministically detect whether a person is who they say they are and whether they are in front of their device in real-time.

We are writing to submit comments regarding the Text of Proposed Regulations for the California Consumer Privacy Act that your office published on October 11, 2019. In particular, we'd like to offer some suggestions relating to (i) rules regarding verification (§§ 999.323 through 999.325), (ii) the role of authorized agents (§ 999.326 and § 999.315), and (iii) the enumerated methods for providing parental consent to the sale of a child's information (§ 999.330 (a)(2)). These suggestions revolve around the idea that your regulatory framework should leverage the existing government-issued identification document infrastructure for the purposes of verifying consumers' identity when they make data requests under CCPA, and are based on our experience fighting fraud and abuse at both Berbix and Airbnb.

We believe that, should your office follow our suggestions, the resulting regulatory framework would improve the ability of Californians to exercise their rights, while simultaneously limiting the ability of bad actors to fraudulently usurp Californians' rights. Moreover, the clarifications that we're suggesting would facilitate compliance with CCPA for businesses and for the third-party identity verification services that serve them. While our company, Berbix, could potentially benefit from some of our suggestions, it is our strong conviction that our own personal information, and that of all other California residents protected by CCPA, would be better safeguarded if you were to adopt our suggestions. Our comments follow, starting at page 3 of this letter.

We're available to provide further information to your office if we can make ourselves useful in any way, and are eagerly looking forward to the entry into force of CCPA on January 1st, 2020.

Best regards,

Steve Kirkham

Steve Kirkham
Co-Founder, Berbix Inc.

Eric Levine

Eric Levine
Co-Founder, Berbix Inc.

Berbix Inc.'s Comments on the Proposed Regulations for CCPA

(i) Rules regarding verification (§§ 999.323 through 999.325)

The Rules Regarding Verification in Article 4 of your Proposed Regulations should be amended to ensure that the requirements for identity verification effectively delineate the need to authenticate the consumer who is submitting a request from the need to tie that authenticated consumer with records held by the business. In addition, the Proposed Regulations should be amended to make it easier for businesses to rely on third-party identity verification services, who should be habilitated to perform an adequate level of identity verification, for example, by verifying a person's identity through the use of a government-issued identity document.

As they stand, §§ 999.323 through 999.325 do not effectively delineate the need to authenticate the consumer who is submitting a request from the need to tie that authenticated consumer with records held by the business. In the proposed regulations, these two distinct concerns appear to be at times merged together, so that business may be able to comply with your regulations merely by matching a few data points with information provided by an individual. While such a method may be adequate in cases where the business does not maintain information in a manner "associated with a named actual person" (§ 999.325 (e)(2)), it unnecessarily creates an important vector for fraud in all other cases.

Research has shown that when companies use weak identity verification mechanisms for verifying the identity of consumers submitting data access requests, it is extremely easy for even moderately skilled bad actors to exfiltrate data or cause it to be deleted.¹ In addition, bad actors can leverage data obtained in a first flight of fraudulent requests to be able to exfiltrate more data in subsequent requests to other businesses, as they may in the process have acquired more information to "match" against.² Moreover, with the prevalence of large-scale data breaches, the information that businesses may want to use for matching to an individual's identity might already be readily available to bad actors.

By properly distinguishing the task of verifying a consumer's identity with that of identifying the data that a business has about a consumer, and by reinforcing the role of third-party identity verification services, your regulatory framework could be improved to minimize fraud while simultaneously preventing businesses responding to Californians' requests from directly collecting sensitive information from them.

We suggest you make the following changes to the Proposed Regulations:

¹ See in a GDPR context, "GDPArrrr: Using Privacy Laws to Steal Identities", Black Hat Conference 2019, <https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf>

² See note 1.

- With respect to the procedures that can be used for verification, third-party identity verification services should only be subject to the restrictions that are relevant to them (§ 999.323 (c)). In particular, third party verification services should explicitly be authorized to request additional information from consumers for purposes of verification. However, such services would only be authorized to disclose to the business the set of information that the business would be able to collect if it wasn't using a third-party identity verification services (i.e. the information necessary to tie records to a given verifiable consumer request).
- Relying on a password-protected account for verification should explicitly be designated as insufficient for requests pertaining to sensitive data (§ 999.324 (a)). Indeed, consumers often reuse the same passwords and are often allowed by businesses to use simple passwords. Given how common data breaches are, it could be trivial for a third-party to guess a consumer's password and make CCPA requests on their behalf. Rather, requests pertaining to sensitive data should be subject to the higher requirements of § 999.325. While such a requirement may increase the burden of verification for consumers, it ensures that their information is adequately safeguarded, and that third-parties cannot improperly access their data or cause it to be deleted.
- Finally, the text of the Proposed Regulations should more granularly distinguish between the task of verifying the identity of a consumer, and the task of identifying the information that the business has which relates to a consumer (in particular at § 999.325). In addition, we strongly recommend that you remove the recommendation for the use of a signed declaration under penalty of perjury as an adequate modality for verification in cases where a higher bar is required in § 999.325 (c), as such a requirement is not only unlikely to deter bad actors, but could also be very easily circumvented by such bad actors willing to forge such a declaration, particularly when requests to know can be submitted over the Internet. Rather, you should encourage businesses to rely on the verification of a government-issued identification document, as such documents are effectively a "gold standard" method of identification, especially when matched with a live picture of the document holder.

The Text of the Proposed Regulations could be amended as follows:

§ 999.323. General Rules Regarding Verification

[...]

(c) A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may

request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, and for security or fraud-prevention purposes. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 999.317. If the business is using a third-party identity verification service, that third-party identity verification service may request additional information from the consumer for purposes of verification, but shall share with the business only the information necessary for the business to locate the information that the business has about the consumer.

[...]

§ 999.324. Verification for Password-Protected Accounts

(a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 999.323. The business shall also require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data. The use of a password-protected account shall not be sufficient for requests pertaining to sensitive or valuable personal information, which shall warrant a more stringent verification process complying with the requirements of section 999.325.

[...]

§ 999.325. Verification for Non-Accountholders or for Requests Pertaining to Sensitive or Valuable Personal Information

(a) If a consumer does not have or cannot access a password-protected account with the business, or if the consumer's request pertains to sensitive or valuable personal information, the business shall comply with subsections (b) through (g) of this section, in addition to section 999.323.

(b) A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data points extracted from a government-issued identification document provided by the consumer with data points maintained by the business, which the business has determined to be reliable for the purpose of verifying the consumer.

(c) A business's compliance with a request to know specific pieces of personal information

requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may include matching at least three pieces of personal information extracted from a government-issued identification document provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with the matching of a picture of the consumer's face taken at the moment of the submission of the consumer's request with the picture found on the consumer's government-issued identity document ~~a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. Businesses shall maintain all signed declarations as part of their record-keeping obligations.~~

(d) A business's compliance with a request to delete may require that the business verify the identity of the consumer to a reasonable degree or a reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion. For example, the deletion of family photographs and documents may require a reasonably high degree of certainty, while the deletion of browsing history may require a reasonable degree of certainty. A business shall act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with the regulations set forth in Article 4.

(e) Illustrative scenarios follow:

(1) If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide ~~evidence that matches the personal information maintained by the business, a copy of a government-issued identification document.~~ For example, if the business maintains the consumer's name ~~and credit card number~~, the business may require the consumer to ~~provide the credit card's security code and identifying a recent purchase made with the credit card to verify their identity to reasonable degree of certainty~~ compare the name of the consumer as it appears on the consumer's identity document with the name in records maintained by the business, and compare a picture of the consumer collected for verification purposes with the picture appearing on the consumer's government-issued identity document.

[...]

(ii) The role of authorized agents (§ 999.326 and § 999.315)

We suggest that your office changes § 999.326 (a)(2) to remove the ability for businesses to require that consumers using an authorized agent verify their own identity directly with the business in cases where a password-protected account is not a sufficient or available means of verifying a consumer's identity. We also suggest subjecting authorized agents to rigorous security and data privacy obligations (§ 999.326 (d)). Moreover, we suggest that your office explicitly clarifies that a permission obtained through electronic means shall be a satisfactory means for an authorized agent to obtain permission to act on a consumer's behalf (§ 999.326 (a)(1) and § 999.315).

The Proposed Regulations include the ability for businesses to force consumers using an authorized agent in their requests to know and requests to delete to verify their identity directly with the businesses whom they seek to exercise their rights with. This could effectively decrease consumers' ability to exercise their rights when a password-protected account is not an adequate or available means of verifying their identity with a business. In addition to the risks enumerated in our suggestions relating to §§ 999.323 through 999.325 ((i), above), this means that consumers may have to verify their identity with dozens, if not hundreds of different entities, with varying levels of privacy and security controls if they desire to control the way their information is handled.

Rather, in such cases, consumers should be able to verify their identity with an authorized agent, who would then be able to certify or otherwise attest to the business, electronically or in writing, that they have verified the consumer's identity in accordance with § 999.323. The authorized agent would be authorized to reveal to the business only the information that is strictly necessary for the business to satisfy the consumer's request.

Authorized agents should be a cornerstone of consumers' ability to exercise their rights under CCPA, thereby realizing the objective stated in your Initial Statement of Reasons of setting the ground for innovation and the development of new technology in this area. Authorized agents could be required to register with your office, and should be subjected to risk-appropriate requirements with respect to data protection and security measures that exceed the more general requirements of § 999.324 (d) (for example, the obtention of a SOC 2 report issued by an independent third-party auditor). Moreover, they should be strictly limited in the use they could make of consumers' information for any purpose other than verification or fraud prevention. Subject to such requirements, authorized agents could be an effective means through which you could ensure that Californians can effectively exert their rights under CCPA, while minimizing the risk of fraud committed by bad actors.

The Text of the Proposed Regulations could be amended as follows:

§ 999.326. Authorized Agent

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, the business may require that the consumer:

(1) Provide the authorized agent written or electronic permission to do so; and

(2) Verify their own identity directly with the business in cases where section 999.324 is applicable to the request submitted by the authorized agent on the consumer's behalf.

(b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4000 to 4465.

(c) A business may deny a request from an agent that does not submit proof that they have been authorized by the consumer to act on their behalf.

(d) Authorized agents shall implement and maintain a data protection program comprising risk-appropriate controls with respect to data privacy and security measures, and shall not use information collected from or about consumers while acting on consumers' behalf for any purpose other than verification or fraud prevention purposes.

§ 999.315. Requests to Opt-Out

[...]

(g) A consumer may use an authorized agent to submit a request to opt-out on the consumer's behalf if the consumer provides the authorized agent written **or electronic** permission to do so. A business may deny a request from an authorized agent that does not submit proof that they have been authorized by the consumer to act on the consumer's behalf. User-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.

[...]

(iii) The role of authorized agents with respect to requests to opt-out of the sale of information (§ 999.315)

§ 999.315. Requests to Opt-Out

[...]

(g) A consumer may use an authorized agent to submit a request to opt-out on the consumer's behalf if the consumer provides the authorized agent written **or electronic** permission to do so. A business may deny a request from an authorized agent that does not submit proof that they have been authorized by the consumer to act on the consumer's behalf. User-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.

(h) A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request. The business shall inform the requesting party that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent.

(iii) The enumerated methods for providing parental consent to the sale of a child's information (§ 999.330 (a)(2))

We suggest that you supplement the non-exhaustive list of methods for providing parental consent to the sale of a child's information (§ 999.330 (a)(2)) to include "Face Match to Verified Photo Identification", a method approved by the FTC in the context of COPPA.

The approach taken in the Proposed Regulations is to transpose the requirements elaborated by the FTC in the context of COPPA to the parental consent mechanism of CCPA. However, the enumeration of reasonably calculated methods in § 999.330 (a)(2) appears to be a direct copy of 16 CFR § 312.5, which doesn't reflect additional methods that the FTC has deemed sufficient to satisfy the COPPA parental consent requirements under the FTC's Rule Safe Harbor program (16 CFR § 312.5 (b)(3)).

In 2015, in an effort to reflect technological evolutions since the COPPA Rule was first drafted, the FTC approved an additional method for verifying parental consent, described by the FTC as "Face Match to Verified Photo Identification". That method is one by which a picture of the identification document of the parent is collected through a website or an app, along with a picture of the parent's face, the latter of which is scanned to ensure that the picture is one of a live person (and not a picture of a picture) and is matched to the face displayed on the photo identification using facial recognition technology.^{3,4} This method was deemed by the FTC to be superior to other methods approved in the COPPA Rule itself. Indeed, in its thorough review of the technology, the FTC noted:

The [Face Match to Verified Photo Identification] method is very similar to an existing [verifiable parental consent] method already in the Rule, which calls for verifying a parent's identity "by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete." The proposed method does not involve checking the government-issued identification against databases of such information, but, as noted above, does involve verification of the

³ "FTC Grants Approval for New COPPA Verifiable Parental Consent Method", November 19, 2015, <https://www.ftc.gov/news-events/press-releases/2015/11/ftc-grants-approval-new-coppa-verifiable-parental-consent-method>.

⁴ To the best of our knowledge, there is only one other method that was similarly approved by the FTC, Knowledge-Based Identification (<https://www.ftc.gov/news-events/press-releases/2013/12/ftc-grants-approval-new-coppa-verifiable-parental-consent-method>). However, this method was approved in 2013, and as noted in a 2019 report by the U.S. Government Accountability Office, "data stolen in recent breaches, such as the 2017 Equifax breach, could be used fraudulently to respond to knowledge-based verification questions. The risk that an attacker could obtain and use an individual's personal information to answer knowledge-based verification questions and impersonate that individual led the National Institute of Standards and Technology (NIST) to issue guidance in 2017 that effectively prohibits agencies from using knowledge-based verification for sensitive applications". See "Federal Agencies Need to Strengthen Online Identity Verification Processes", June 14, 2019, <https://www.gao.gov/products/GAO-19-288>.

identification document to ensure its authenticity. **The proposed method is more rigorous than the existing approved method in that it involves the use of facial recognition technology to check that the individual to whom the identification was issued is the same individual who is interacting with the system at that moment.** Both methods involve prompt deletion of the identification information collected from the parent.⁵ [our emphasis]

The addition of “Face Match to Verified Photo Identification” method to the enumeration in § 999.330 (a)(2) would reduce uncertainty for businesses that are evaluating how to comply with CCPA and encourage their reliance on the more robust means of verifying a parent’s identity that recent technological advances have enabled.

The Text of the Proposed Regulations could be amended as follows:

§ 999.330. Minors Under 13 Years of Age

[...]

(a) (2) Methods that are reasonably calculated to ensure that the person providing consent is the child’s parent or guardian include:

- a. Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;
- b. Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;
- c. Having a parent or guardian call a toll-free telephone number staffed by trained personnel;
- d. Having a parent or guardian connect to trained personnel via video-conference;
- e. Having a parent or guardian communicate in person with trained personnel; and

⁵ “Commission Letter Approving Application Filed by Jest8 Limited (Trading As Riyo) For Approval of A Proposed Verifiable Parental Consent Method Under the Children’s Online Privacy Protection Rule”, November 19, 2015, <https://www.ftc.gov/public-statements/2015/11/commission-letter-approving-application-filed-jest8-limited-trading-riyo>.

f. Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information, where the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.

g. Verifying a parent or guardian's identity by checking a form of government-issued identification and using facial recognition technology to check that the individual to whom the identification was issued is the same individual who is interacting with the business, where the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.

[...]



December 6, 2019

Via Electronic Mail

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

Re: Notice of Proposed Rulemaking – California Consumer Privacy Act

Dear Privacy Regulations Coordinator:

The Bank Policy Institute (BPI)¹ appreciates the opportunity to submit comments on the Attorney General's proposed regulations under the California Consumer Privacy Act.² BPI member banks are dedicated to protecting customer data, and they have adopted robust privacy and information security programs with administrative, technical, and physical safeguards designed to achieve that important goal. These programs are designed pursuant to and consistent with the requirements of state, federal and foreign laws, notably the federal Gramm-Leach-Bliley Act (GLBA)³ and its implementing regulations. Therefore, BPI member banks already adhere to notice and disclosure requirements, protect the security and confidentiality of customer information, protect against anticipated threats or hazards to the security or integrity of customer information, and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to customers.⁴ These programs are tailored to the size, complexity, activity, and overall risk profile of a bank, as contemplated under federal law.⁵

¹ The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost two million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

² Cal. Civ. Code § 1798.100 *et seq.*

³ 15 U.S.C. § 6801 *et seq.*

⁴ As noted by President Clinton in signing the GLBA into law, the GLBA requires banks to "clearly disclose their privacy policies to customers up front...consumers will have an absolute right to know if their financial institution intends to share or sell their personal financial data, either within the corporate family or with an unaffiliated third-party [and]...will have the right to "opt out" of such information sharing with unaffiliated third parties...[and] allows privacy protection to be included in regular bank examinations...[and] grants regulators full authority to issue privacy rules and to use the full range of their enforcement powers in case of violations." William J. Clinton, Statement on Signing the Gramm-Leach-Bliley Act, November 1999. Available at web.archive.org/web/20160322081604/http://www.presidency.ucsb.edu/ws/?pid=56922; accessed Nov. 20, 2019.

⁵ See, e.g., Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 30, app. B (2018).

I. Executive Summary

Given the CCPA's January 1, 2020 effective date and the separate, statutorily required, regulatory effort it is important that the Attorney General endeavor to harmonize any new requirements with the structure established by the CCPA itself. This harmonization is critical, both to allow businesses adequate time to test and implement strong compliance policies and processes and to help consumers understand their rights and responsibilities. Clarity and consistency are vital to achieving the CCPA's goal of putting consumers in control of their privacy online.

It is also crucial that the Attorney General recognize and align regulatory efforts with the long-standing and effective frameworks that banks have built over decades, under federal standards, to protect the privacy and security of consumer data. Banks already employ extensive programs in these areas, which differ from those utilized by other sectors of the economy. The regulations should take these programs into account and ensure that consumer protections are not unintentionally weakened by companies' CCPA compliance efforts.

In Part II of this letter, we propose amendments to the draft regulations to address such issues. In Part III, we describe two provisions of the regulations that, while not substantively problematic, would benefit from further clarification.

II. Proposed Amendments

- A. The effective date of the regulations should be at least six months after the final regulations are published, to account for the imposition of requirements that go beyond the statute, and the Attorney General should not undertake enforcement actions for conduct that occurs before January 1, 2021.**

As explained throughout these comments, the CCPA is a highly complex statute that requires businesses to invest significant time and resources in compliance. The proposed regulations, even if modified as recommended in this letter, will add additional implementation expectations to that effort, and it will take time for businesses to design, test, and implement compliant systems and processes. Many of these burdens are not contemplated by the CCPA itself, and so businesses have had less than two months to evaluate the implementation requirements of the proposed regulations, much less to invest substantial resources into compliance, given the uncertain nature of any final and binding rules. Thus, the Attorney General should provide a transitional implementation period to allow firms to establish and test compliance procedures that reflect the final regulations. Requiring businesses to compress this timeline unreasonably is likely to lead to mistakes and omissions that ultimately do not benefit consumers or the goals of the CCPA.

Section 11343.4(b)(2) of the California Government Code permits agencies to prescribe an effective date for regulations different from the default date unless the statute requires otherwise. The CCPA does not prescribe the effective date for the Attorney General's regulations, only for the CCPA itself. The Attorney General therefore has the authority to prescribe a later effective date for the regulations.

Even if the regulations are presumed to be enforceable on the same date as the statute, Section 1798.185(c) of the CCPA can reasonably be read to state that enforcement shall not begin until "six months after [1] the publication of the final regulations issued pursuant to this section or [2] July 1, 2020, whichever is sooner." That is, enforcement could be interpreted to be permitted either on January 1, 2021 or six months after the regulations are finalized, whichever is sooner. This reading is consistent with principles of fair notice and harmonizes with the legislature's clearly indicated intent to give businesses a reasonable amount of time (six months) to come into compliance with the Attorney General's regulations, which are not required to be finalized until July 1, 2020. Furthermore, it is common practice to allow such a period to give businesses a chance to interpret and implement regulations. Reading the statute to allow enforcement of the regulations on the very day they are made effective would be unjust.

The CCPA does not require the Attorney General to begin enforcement as soon as he is permitted to do so but instead leaves the commencement of enforcement efforts to the Attorney General's discretion. Thus, even if the Attorney General is statutorily empowered to begin enforcement of the final regulations on July 1, 2020, BPI would recommend that he refrain until January 1, 2021 in order to give businesses adequate time to develop compliance systems and processes, adequately test these procedures, and implement them. Doing so would better serve the interests of consumers by decreasing the risks of identity theft and security breaches that could result from hastily implemented compliance measures.

Finally, any "look back" requirements and enforcement activity should commence upon the implementation date of the CCPA regulations. Federal agencies have taken a similar approach with respect to data subject to "look back" periods in order to provide adequate time to institutions to effectively implement regulatory expectations.⁶

- B. The requirement in § 999.313(d)(1) that if a business cannot verify the identity of a requestor seeking deletion it shall instead treat the request as a request to opt out of sales does not comport with the text of the CCPA or a reasonable inference of consumer intent and should be removed.**

The CCPA treats the right to delete and the right to opt out of the sale of personal information as separate, placing them in distinct sections of the statute and subjecting them to distinct sets of exceptions. There does not seem to be any legal basis to convert a request to an unrequested, unrelated action because the requestor's identity could not be verified.

Additionally, without knowing who the consumer is, a business may not be able to fulfill the opt-out request or may have to opt out individuals who may not be the actual requestor, such as those who happen to share the same name. This would counter the intent of the statute to give consumers controls over their personal information, which is unreasonable and ill-advised.

If a request to delete cannot be verified, the only required action should be to inform the requestor of that fact; we therefore recommend that the attending opt-out expectations be removed. The business is separately required to provide the requisite notices and opportunities for the consumer to opt out of the sale of their information if they wish to do so.

- C. Section 999.323(c)'s statement that businesses shall "generally avoid" requesting additional information from the consumer for the purpose of verification is at odds with the need to ensure verification and should be removed.**

The CCPA's references to the verification of consumer requests serve as a protection of consumers' interests in the integrity and security of their personal information. It is not possible for businesses to determine with certainty at the outset what information and procedures will be necessary to verify a consumer's identity in all cases. This is particularly true because banks will be required to respond to requests from non-customers under the CCPA, and they often will not know at the outset what information they may have on such individuals that could be used for verification purposes. Discouraging businesses from asking for additional information when it is needed for reasonable verification efforts will only harm consumers and increase the likelihood of fraudulent requests. Despite efforts in the proposed regulations to decrease the value to fraudsters of submitting right-to-know requests, there is still a significant risk of disclosure of personal information to a bad actor or from the deletion of a consumer's

⁶ For example, in 2016, the Financial Crimes Enforcement Network chose not to require identification of beneficial owners on a "look back" basis prior to the May 11, 2018 implementation date of its Customer Due Diligence rule, as it felt it would be "unduly burdensome" due to the "significant changes to processes and systems that [covered institutions were] required to implement" under the rule. See 81 Fed. Reg. 29,404 (May 11, 2016).

personal information against their wishes. In order to reduce these risks, the Attorney General should encourage businesses to take all reasonable steps to verify a consumer's identity before responding to a request.

BPI members and other banks have rigorous procedures in place to comply with Know Your Customer (KYC) requirements⁷ that are well-suited to the verification required by the CCPA. It would better serve consumers' interests for banks to provide the full amount of protection these procedures offer, instead of watering them down for CCPA compliance purposes.

Furthermore, although the Attorney General's Statement of Reasons indicates that this provision is meant to "protect consumers by prohibiting businesses from using verification as an excuse to collect and use personal information for other means," the statute, as well as the proposed regulations, have established other safeguards to prevent such behavior. Section 1798.130(a)(7) of the CCPA requires businesses to "[u]se any personal information collected from the consumer in connection with the business' verification of the consumer's request solely for the purposes of verification." The second sentence of § 999.323(c) further requires that any additional information collected be used only for verification, security, or fraud-prevention purposes. Given these prohibitions, the potential harms to consumer privacy from weakened verification methods outweigh reduced risk of misuse by businesses that this regulatory language might accomplish. We therefore recommend that this language be removed from the final rule.

D. The requirement in § 999.325 that businesses provide two types of right-to-know requests with two different levels of authentication scrutiny would impose burdensome implementation requirements that go beyond the statute and do not benefit consumers.

Requiring multiple verification tiers for right to know requests, as the draft regulations contemplate, has no foundation in the statute and would not benefit consumers. Providing information even about the categories of personal information collected without adequate identity verification can pose security risks. A financial institution generally does not disclose whether a consumer has an account with it unless it is able to verify the consumer's identity. This is because bad actors can use information about the institution or other institutions with which a consumer has accounts to commit identity fraud. By providing individuals with information about data that has been collected on a consumer without verifying their identity to a high level of confidence, businesses run a significant risk of aiding identity thieves in their attempts to harm consumers.

If a business chooses to have multiple tiers of verification based on the sensitivity of the data and the level of risk, that should be permitted, but it should not be a requirement placed on all entities. The Initial Statement of Reasons does not specify why this differentiation is "reasonably necessary" to protect consumer privacy, nor does it address the concern that such an approach could actually result in identity theft. The regulations should instead encourage businesses to take all reasonably necessary steps—including use of existing KYC procedures, if they exist—to verify a consumer's identity before responding to a request. This aligns with the guidelines established by § 999.323(b)(3) of the draft regulations.

Relatedly, BPI requests that the Attorney General clarify that the requirement in §§ 999.308(b)(1)(c)-(b)(2)(c) and § 999.313(a) that a business describe the process used to verify consumer requests, including any information the consumer must provide, may be satisfied with a description at a high level of generality. Requiring more detailed descriptions of verification processes could aid bad actors in their efforts to exploit the system for fraudulent purposes. This is particularly true for banks, where information gathered about an individual's accounts with one institution is often used by identity thieves to attempt to gain access to accounts or to create new accounts at other institutions.

⁷ Although the term "KYC" is not used in regulations, it is generally used in industry and regulator parlance to refer to institutions' obligations to collect, analyze, and use information about their customers to comply with various anti-money laundering and sanctions requirements that require financial institutions to understand, to some extent, the nature and identities of the parties with whom or on whose behalf they are conducting financial transactions.

- E. Requiring publication of metrics regarding responses to consumer requests in a business's privacy policy, as § 999.317(g) would, will not benefit consumers, but could increase the risk of identity fraud. These metrics should instead be provided upon request to the AG.**

The metrics described by § 999.317(g) are intended to gauge a company's compliance with the CCPA. Since the statute is enforced by the Attorney General and not by the consumers for whom a privacy policy is drafted, it would be more appropriate for businesses to be required to provide them to the Attorney General upon request. Placing them in the privacy policy would only serve to increase the length and complexity of a document that is intended to be digestible by consumers, without providing them any useful information about how their personal information is collected or used. In addition, the posting of metrics provides additional information for fraudsters looking to attack companies with fraudulent requests. For example, businesses with metrics showing a high rate of fulfilling requests are likely to become victims of fraudulent requests, where fraudsters may avoid a business with metrics showing a high percentage of access request denials. Finally, such an approach is in line with Section 11346.3(a) of the California Administrative Procedure Act, which states that an agency must consider the impact on California businesses and avoid imposing "unnecessary or unreasonable regulations or reporting, recordkeeping, or compliance requirements."

- F. The requirement in § 999.313(d)(4) that a business must specify the manner in which it has deleted information is burdensome, confusing, and unnecessary, and it should be removed.**

In a large business, the process of responding to a request to delete personal information will be complicated, likely involving many systems and business units. Some data elements may be deleted outright, while others are deidentified, or otherwise modified to place them outside the scope of the CCPA's definition of personal information. Providing a detailed description of this process would be burdensome and, rather than providing "greater transparency about the business's practices in deleting personal information" as the Initial Statement of Reasons contemplates, would in fact create confusion for consumers. For example, consumers may not appreciate the differences between deletion, deidentification, and aggregation. Businesses should instead be permitted to simply inform a consumer that their personal information has been deleted, or to inform them of the reasons it has not been deleted, as provided by § 999.313(d)(6) of the proposed regulations.

- G. Section 999.305(d)'s requirement that a business obtain attestations of compliance from third-party collectors if the business does not directly collect information from a consumer is confusing and lacks statutory basis.**

Under § 999.305(d), a business is not required to provide initial notice if it is not directly collecting personal information from the consumer. However, this provision requires that businesses ensure that the party that provided (sourced) the data gave the consumer the initial notice mandated by the CCPA. It also requires that businesses retain a "signed attestation" by that party to confirm the third party's adherence with the initial-notice requirement.

This requirement is problematic because it places the burden on the business receiving data to confirm that all parties who are sourcing data are complying with their CCPA notice obligations. The requirement has no basis in the text of the CCPA. Third parties who provide data should be the ones maintaining any documentation of their compliance with their notice obligations, in line with the provisions set forth in Civil Code section 1798.115(d).

- H. The requirement in §§ 999.305(b)(2), 999.308(b)(1)d.2, and 999.313(c)(10) that information be presented category by category rather than in the aggregate—contrary to how the language of the CCPA is reasonably read—will result in consumer confusion and should be removed.**

Given the level of detail that the proposed regulations would require in these sections, consumers are likely to be overwhelmed by the quantity of information, without providing a more meaningful understanding of a business's

data practices. There are 11 CCPA categories of personal information, a proposed minimum of three source types, and seven third-party types, along with an uncertain number of uses or purposes of collection, all of which businesses would be required to describe both in a privacy notice and in customized responses to access requests. Under the draft regulations' approach of requiring this information to be described "category by category," which goes beyond a reasonable interpretation of the statute's requirements, this could require many additional pages to communicate the various permutations of these pieces of information. Even for a business of moderate complexity, for example, a notice could run to more than 20 pages. This would be overwhelming to consumers, and it is unclear if and how this information could be presented on a small screen, as the draft regulations require.

These provisions would impose a large administrative burden on businesses of all sizes, without meaningfully adding to consumers' understanding—and, in fact, quite possibly detracting from it. Therefore, we recommend that it be limited, as it is under the statute, to personal information that is sold.

I. Section 999.306(d)(2) appears to require that a business that begins selling personal information obtains opt-in consent from every consumer who the business has previously interacted with. This would be extremely burdensome and lacks statutory basis.

If a business that has not previously sold personal information decides to begin doing so—or if an aggressive interpretation of the CCPA's definition of "sale" is adopted that encompasses practices a business did not believe were included—§ 999.306(d)(1) prohibits it from selling information collected during the period when it did not post a notice of right to opt-out. This limitation is sufficient to provide the protection for consumers intended by the CCPA's right to opt out from sale. Consumers who interact with a business that does not sell their information have not thereby expressed any affirmative desire to opt out of the sale of their information, and it would be in tension with the statutory framework to treat them differently from other consumers.

Additionally, it may be very difficult or impossible for a business to implement this provision. Determining all consumers whose personal information may have been previously collected and contacting them to obtain consent may not be possible, depending on the information a business maintains. Instead, businesses should be prohibited from selling information that was collected without the proper notices in place, and they should be required to adhere to the practices disclosed at the time of collection for that data going forward (unless opt-in consent is obtained), but they should not be restricted from changing their practices and providing the same CCPA rights as any other business in relation to data collected in the future. BPI would recommend that businesses be required to give consumers a reasonable period of time to opt out after the requisite notices are provided, as is required, for example, by the GLBA.⁸

J. The 12-month lookback in the regulations and the statute should not be enforced in relation to conduct occurring before the effective date of the CCPA.

As of January 1, 2020, when the CCPA is effective, businesses will be required to make various disclosures about their practices for the past 12 months regarding collection, use, and sale of personal information. However, since the CCPA's definitions, particularly those of "sale" and "personal information" differ significantly from definitions in other statutes, some businesses may have difficulty ascertaining the precise set of data points they collected or transfers they engaged in that would fit these definitions. Accordingly, BPI would recommend that the Attorney General not bring enforcement actions based on disclosures of conduct occurring before the effective date of the CCPA, as long as businesses make reasonable efforts to give consumers an understanding of their practices.

⁸ See 16 CFR § 680.24.

K. Section 999.325(e)(2)'s instruction that businesses use a "fact-based verification process" for information not associated with a particular consumer should be removed.

For personal information that is not associated with a "named actual person," businesses are advised in § 999.325(e)(2) to conduct a "fact-based verification process" to allow a consumer to show that they are the only person associated with the personal information. This provision appears to require businesses to reidentify or link information that is not maintained in a manner that would be considered personal information, in contradiction of the CCPA.⁹ BPI requests that this provision be removed, or that the Attorney General clarify that the provision is a recommendation rather than a requirement and that it does not require re-linking of non-personal information. Additionally, if the provision is retained, BPI requests that the Attorney General clarify the meaning of the term "fact-based verification process."

III. Requests for Clarification

A. The regulations should clarify that consumers should not be able to skirt the rules of discovery during litigation by exercising rights under the CCPA.

The regulations should consider—and affirmatively prevent—the ability of a consumer to initiate a CCPA access or deletion request in lieu of discovery in a court matter. If not prevented, individuals would be able to circumvent established legal discovery rules under the false pretense of exercising a state-law privacy right. BPI requests that the Attorney General clarify that Section 1798.145(a)(4) of the CCPA, which states that the law shall not restrict a business's ability to "[e]xercise or defend legal claims" prevents this sort of avoidance of discovery rules.

B. The regulations should clarify that § 999.306(d)(2) does not restrict a business from changing its practices to begin selling personal information, if proper notice is given and opt-out mechanisms are provided.

Section 999.306(d)(2) requires that, for a business to be exempt from providing a notice of right to opt-out, it must "state in its privacy policy that it does not **and will not** sell personal information" (emphasis added). On its face, this would appear to restrict a business that does not sell information (and that therefore does not provide a notice of right to opt-out) from ever changing this practice. However, § 999.306(d)(1) plainly contemplates that the business only must refrain from selling information collected during the time period during which the notice of right to opt-out is not provided. BPI requests that the Attorney General clarify that § 999.306(d)(2) merely requires a business to state that it will not sell personal information collected during the time period during which the notice of right to opt-out is not provided.

The Bank Policy Institute appreciates the opportunity to submit comments concerning the Attorney General's draft regulations. If you have any questions, please contact the undersigned by phone at [REDACTED] or by email at [REDACTED].

Respectfully submitted,



Angelena Bradfield
Senior Vice President, AML/BSA, Sanctions & Privacy
Bank Policy Institute

⁹ See Cal. Civ. Code § 1798.100(e).

Message

From: Meghan Pensyl [REDACTED]
Sent: 12/6/2019 8:04:02 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Kate Goodloe [REDACTED]
Subject: BSA Comments on Proposed CCPA Regulations
Attachments: 2019.12.6 - BSA comments on CCPA AG Regulations - FINAL.pdf

To whom it may concern:

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

Many thanks.

Best,
Meghan





December 6, 2019

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

RE: Proposed Text of Regulations to Implement the California Consumer Privacy Act

Dear Attorney General Becerra:

BSA | The Software Alliance appreciates the opportunity to submit comments on proposed regulations to implement the California Consumer Privacy Act (“CCPA”).

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

BSA submits these comments to address the unique role of service providers, which create the products and services that other businesses rely on. Service providers have important obligations to safeguard the privacy of data they process and maintain. The CCPA recognizes this role, including by requiring service providers to act on behalf of businesses and at their direction. A broad reading of the draft regulations risks upsetting the business-service provider relationship set out in statute. We urge three revisions to the draft regulations to avoid that result:

- *First*, to ensure that service providers can meet the specific requests of their customers, the regulations should expressly state that a service provider may use personal information received from a business or consumer to serve another entity—*when a business or consumer directs it to do so*.
- *Second*, and for the same reason, the regulations should also expressly state that a service provider may combine information received from one or more businesses,

¹ BSA’s members include: Adobe, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informativa, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

when doing so is needed to provide and maintain the services and related services provided to those businesses.

- *Third, the regulations should clarify that a service provider should only respond to consumer requests sent to it by a business—to help avoid the privacy and security risks associated with requiring service providers to respond directly to consumers, with whom they generally lack a direct relationship.*

These changes will together help to ensure the business-service provider relationship established by the CCPA is not inadvertently altered by the draft regulations.

I. The Unique Role of Service Providers.

As enterprise software companies, BSA members develop and deliver the technology products and services on which other businesses rely. In this role, they generally act as service providers under the CCPA.² Service providers are critical in today's economy, as more companies across a range of industries become technology companies—and depend on service providers for the tools and services that fuel their growth. Software is the backbone of shipping and transportation logistics. It enables financial transactions all over the world. And it drives the growth of new technologies like artificial intelligence (“AI”), which have helped companies of all sizes enter new markets and compete on a global scale.

Businesses entrust some of their most sensitive data—including personal information—with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations. Indeed, many businesses depend on BSA members to help them better protect privacy. For example, our members offer cloud computing services that allow customers to compartmentalize datasets, which can prevent a breach in one location from impacting a full dataset. Other BSA members provide privacy-enhancing technologies that use, for example, data masking, which help companies to reduce the sensitivity of data they hold, and thereby reduce privacy and security threats.

II. The Difference Between “Businesses” and “Service Providers” Under the CCPA.

The CCPA recognizes the distinct role of service providers. While the statute focuses primarily on businesses, which “determine[] the purposes and means of the processing of consumers' personal information”³ it recognizes that businesses may engage service providers to

² Of course, when BSA members collect data for their own business purposes, they take on responsibility for complying with the provisions of the CCPA that apply to “businesses” that “determine[] the purposes and means of the processing of consumers' personal information.” For instance, a company that operates principally as a service provider will nonetheless be treated as a business when it collects data for the purposes of providing services directly to consumers. While these comments focus on issues relevant to service providers, we recognize there are a number of issues important to companies acting as “businesses” under the CCPA that are likewise important to BSA. Those include providing more clarity on how businesses can comply with requests to delete, including ensuring a reasonable timeline for deletion of personal information in backup systems, supporting use of security measures like multi-factor authentication in connection with user verification, and providing additional guidance on how businesses are to honor opt-out requests in connection with consumer browser plugins or privacy settings.

³ See Cal. Civil Code § 1798.140(d).

“process[] information on behalf of a business.”⁴ The CCPA requires service providers to enter into written contracts with businesses they serve, limiting how the service provider can retain, use, and disclose personal information provided to them by a business.⁵

The CCPA also assigns businesses and service providers different obligations, in line with their different roles in handling consumers’ data. Since businesses decide why and how to collect a consumer’s personal information, they must provide consumers certain rights, including the ability to opt-out of sales of their information. Businesses must therefore direct service providers to help implement certain rights, including the right to delete personal information.⁶ But service providers do not decide why a consumer’s information is collected or used. Rather, they process the personal information on behalf of a business, pursuant to their written contract.

Distinguishing between businesses and service providers is important from a privacy perspective, because adopting this type of role-based responsibility improves privacy protection. Indeed, the distinction is pervasive in the privacy ecosystem. For example, the EU’s General Data Protection Regulation (“GDPR”) applies to “controllers” that determine the means and purpose for which consumers’ data is collected (similar to businesses under the CCPA), and “processors” that process data on their behalf (similar to service providers under the CCPA). Voluntary frameworks that promote data privacy and cross-border transfers also reflect the distinct roles that different types of companies have in handling consumers’ data.⁷

III. The Draft Regulations Should be Clarified to Avoid Altering the Business-Service Provider Relationship Established in the CCPA.

The draft regulations should not be read to upset the business-service provider relationship created by the text of the CCPA. We encourage three revisions to avoid that result.

A. Service Providers’ Role in Processing Personal Information

Our first two recommendations focus on the portions of the draft regulations addressing how service providers process data provided to them by a business.

Text of Proposed Regulations. Section 999.314(c) states that a service provider “shall not use personal information received either from a person or entity it services or from a consumer’s direct interaction with the service provider for the purpose of providing services to another person or entity.” However, “[a] service provider may . . . combine personal information received from one or more entities . . . on behalf of such businesses, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.”

Negative Consequences of Reading Proposed Regulations Broadly. If this provision were read broadly, it would risk upsetting the business-service provider relationship created in the CCPA.

⁴ See Cal. Civil Code § 1798.140(v).

⁵ *Id.*

⁶ See Cal. Civil Code § 1798.105(d).

⁷ For example, privacy laws in Hong Kong, Malaysia, and Argentina distinguish between “data users” that control the collection or use of data and companies that only process data on behalf of others. In Mexico, the Philippines, and Switzerland, privacy laws adopt the “controller” and “processor” terminology. Likewise, the APEC Cross Border Privacy Rules, which the US Department of Commerce has strongly supported and promoted, apply only to controllers and are complemented by the APEC Privacy Recognition for Processors, which help companies that process data demonstrate adherence to privacy obligations and help controllers identify qualified and accountable processors.

Under the statute, if a business asks a service provider to use personal information to serve multiple businesses, or to combine that information with other data sets, the service provider is obligated to do so. The draft regulations should not be read so broadly to prevent that result.

If Section 999.314(c) were read to prevent these actions, it would have several negative consequences:

- *First*, it would risk placing new obligations on service providers that are inconsistent with their role under the CCPA. In particular, if the draft regulations were read to require a service provider to refuse to process data when a business specifically asks for the data to be provided to multiple businesses, it would effectively require the service provider to decide when it can and cannot process information. Yet the CCPA makes businesses—not service providers—responsible for those decisions.

By definition, a business “determines the purposes and means of the processing of consumers’ personal information.”⁸ Service providers have no such authority, which is fundamental to the distinction between businesses and service providers under the statute. Moreover, the CCPA prescribes specific contractual and other requirements that entities must observe if they wish to establish and maintain a business-service provider relationship.⁹ The draft regulations should not be read to upset this careful balance.

- *Second*, it would risk limiting the ability of businesses to combine information in ways that benefit consumers. Indeed, businesses may ask service providers to combine information with other data sets, or to serve multiple businesses, for a range of purposes that benefit consumers and support responsible innovation—without monetizing consumers’ data or using it for advertising. These include:
 - *Serving businesses that enter into a joint venture.* When two businesses want a service provider to act on their behalf, the CCPA allows the service provider to do so, as long as a written contract is in place. Similarly, a business may choose to engage two service providers, and direct them to share data on its behalf. The draft regulations should not be read to prohibit such arrangements.
 - *Providing and improving services.* Businesses may direct service providers to use personal information they disclose to the service provider to improve services offered to multiple businesses. For example, a service provider may use personal information provided by one business to improve an algorithm that powers a service provided to multiple businesses, even without combining the underlying data. Similarly, a business may direct a service provider to combine metadata that is personal information under the CCPA from its

⁸ See Cal. Civ. Code § 1798.140(c)(1).

⁹ See generally Cal. Civ. Code §§ 1798.140(v), (d) and (f) (defining “service provider,” “business purpose,” and “commercial purpose,” respectively). A broad reading of the draft regulations would limit the actions of service providers in new ways, not contained in the statutory text of CCPA. Even under the broadest grant of rulemaking authority in the CCPA, see Cal. Civ. Code § 1798.185(b), that broad reading of subdivision 999.314(c) would not “fill in the details” of the statutory scheme, See *Ford Dealers Ass’n v. Dep’t of Motor Vehicles*, 32 Cal. 3d 347, 362-63 (1982). The broad reading would also conflict with the CCPA’s consent requirements, which subjects certain actions to opt-out consent and others to opt-in consent. Reading subdivision 999.314(c) broadly to disallow these actions would also ignore the role of consent in the statutory scheme, and create a ban on processing to which no consent could be given.

- business and from other businesses to better provide a service, such as to prepare to handle peak traffic times across geographies.
- *Facilitating research.* Service providers can help entities conducting scientific research by combining multiple sets of data, at the direction of those entities and in line with privacy safeguards they have established. The resulting data could then be used to serve each of the participating entities.
 - *Providing benchmarking services to both consumers and businesses.* These services can provide context to a consumer or business seeking to understand how it fits into broader trends. For example, a consumer may want to opt-in to a program that allows her health care provider to use a service provider to combine her information with other data sets, to better understand potential health risk factors. While such a service would depend on the service provider's ability to combine several sets of personal information in order to identify those risk factors, it may limit the information shared with consumers to aggregated or de-identified information about how that consumer fits into these broader trends. Similarly, businesses may use benchmarking services to understand industry trends in hiring and human resources management, and to identify areas in which they may need to invest additional resources.
 - *Developing and testing AI systems.* AI systems are trained with large volumes of data. Their accuracy—and benefits—depend on access to large amounts of high-quality data, which service providers may process at the direction of businesses. For example, cities are optimizing medical emergency response processes using AI-based systems, enabling them to more strategically position personnel and reduce both response times and the overall number of emergency trips. The draft regulations should not prohibit service providers from using or combining information for such purposes, at the direction of a business.
 - *Supporting open data initiatives.* More broadly, there is increasing recognition among governments and companies of the benefits of sharing data—subject to appropriate privacy protections. For example, in January the United States enacted the OPEN Government Data Act, which makes non-sensitive government data more readily available so that they can be leveraged to improve the delivery of public services and enhance the development of AI.¹⁰ Companies have also supported voluntary information-sharing arrangements, including seeking to develop common terms so that companies that want to share data can more readily do so.¹¹

Proposed Revision to Regulations. To ensure the draft regulations are not read so broadly as to prohibit service providers from processing personal information at the direction of and on behalf of businesses—we suggest adding the italicized language to Section 999.314(c):

“A service provider shall not use personal information received either from a person or entity it services or from a consumer’s direct interaction with the service provider for

¹⁰ See Public Law No. 115-435, Title II (Jan. 14, 2019).

¹¹ See Microsoft, The Open Use of Data Agreement, available at <https://github.com/microsoft/Open-Use-of-Data-Agreement>; The Linux Foundation Projects, Community Data License Agreement, available at <https://cdla.io/>.

the purpose of providing services to another person or entity, *except at the direction and on behalf of the business providing the personal information*. A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity, or for purposes compatible with providing the services.”

B. Role of Service Providers in Responding to Consumer Requests

Our third recommendation addresses the role service providers play in responding to consumer requests under the CCPA.

Text of Proposed Regulations. Section 999.314(d) states: “If a service provider receives a request to know or a request to delete from a consumer regarding personal information that the service provider collects, maintains, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial. The service provider shall also inform the consumer that it should submit the request directly to the business on whose behalf the service provider processes the information and, when feasible, provide the consumer with contact information for that business.”

Negative Consequences of Proposed Regulations. This provision also risks upsetting the business-service provider relationship established in the CCPA. In particular, Section 999.314(d) could be read to require service providers to evaluate and respond to consumer requests to know or delete personal information—an obligation not placed on them by the CCPA.

Under the text of the CCPA, service providers merely play a supporting role in executing deletion requests on behalf of businesses.¹² Notably, the statute requires *businesses* to delete personal information pursuant to a verifiable consumer request and to “direct any service providers” to do the same.¹³ The statute thus anticipates that service providers act *at the direction of businesses*—and not at the direction of consumers, with whom they lack a direct relationship. The connection between right to know requests and service providers is even more attenuated; the text of the law does not refer explicitly to service providers in connection with the right to know.¹⁴ As a result, “neither the CCPA nor the regulations require service providers to comply with such requests.”¹⁵

This arrangement is for good reason. Requiring service providers to respond directly to consumer requests invites a host of security and privacy risks, which arise because service providers generally do not interact with consumers. In the ordinary course, a service provider may not maintain information about the consumers its business customers serve—and thus would not ordinarily review records containing their names, services provided, or other information needed to respond to a request. Service providers should not be encouraged to seek out that information, if they would not otherwise have access to it. For example, a service provider that works with multiple businesses may not be able to identify the business relevant to a consumer’s request without combing through personal information it provides on a host of businesses, to identify the relevant one. That result should be avoided, because it would invade consumers’ privacy, not protect it. Likewise, service providers may not have sufficient

¹² See Cal. Civ. Code §§ 1798.105(c), (d).

¹³ See Cal. Civ. Code § 1798.105(c).

¹⁴ See generally Cal. Civ. Code §§ 1798.100 and 1798.110.

¹⁵ *Initial Statement of Reasons*, at 22-23.

information to verify a consumer's request, and thus could create security risks in responding directly to a consumer without verifying her identity.

Instead, the CCPA recognizes that businesses should respond to consumer requests—since they have the most complete understanding of what data they control about a particular consumer. Section 999.314(d) should be revised to ensure it does not alter this process.

Proposed Revision. We suggest revising Section 999.314(d) to more clearly reflect the existing statutory scheme, by deleting the language in strikethrough below and adding the language in italics.

~~"If a service provider receives a request to know or a request to delete from a consumer regarding personal information that the service provider collects, maintains, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial. The service provider shall also~~ *then the service provider shall* inform the consumer that it should submit the request directly to the business ~~on whose behalf the service provider processes the information, and when feasible, provide the consumer with contact information for that business.~~ *with which the consumer interacted."*

* * *

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

Sincerely,



Kate Goodloe
Director, Policy
BSA | The Software Alliance

Message

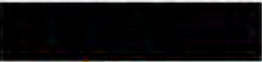
From: Moises Rosales [REDACTED]
Sent: 12/7/2019 12:31:27 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Anna Buck [REDACTED]
Subject: C.A.R.'s Comments on the Proposed CCPA Regulations
Attachments: C.A.R. - Comments on Proposed CCPA Regulations.pdf
Importance: High

To Whom It May Concern,

Attached please find C.A.R.'s comments on the proposed CCPA regulations.

Thank you.

MOISES ROSALES
ADMINISTRATIVE ASSISTANT
CALIFORNIA ASSOCIATION OF REALTORS®
1121 L STREET, SUITE 600
SACRAMENTO, CA 95814



Help your clients keep their homes & insurance coverage.
[Download the shareable materials today!](#)



CALIFORNIA ASSOCIATION OF REALTORS®

December 6, 2019

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

RE: California Consumer Privacy Act Proposed Regulations

Dear Attorney General Becerra:

Thank you for the opportunity to provide comments regarding the proposed California Consumer Privacy Act (CCPA) regulations. The California Association of REALTORS® (C.A.R.) seeks to be a valuable contributor in the development of these regulations so that the uniqueness of the real estate industry, and specifically the real estate transaction process, is considered. We also feel it is critical that the regulatory scheme consider some of the issues unique to our trade and we hope we can be of assistance to those working to craft the regulations associated with this landmark law.

Business practices for handling requests made pursuant to the CCPA

In the real estate industry, information held in the aggregate can nonetheless prove incredibly useful for both the principals and the professionals engaged in the homebuying and selling process. According to the proposed regulations, requests for deletion may be completed by deidentifying or aggregating the consumer's personal information ("PI"). It would be useful to our industry if more guidance was given on what steps should be taken to properly deidentify or aggregate information in order to properly comply with this part of the law.

Furthermore, another area of concern to the real estate industry is the fact that real estate transactions involve at a minimum two separate and unrelated households and the documents related to the transactions include PI of multiple consumers; at the least, documents will have PI of both the buyer and the seller, and in many cases may have PI of multiple consumers on the buyer and seller side respectively. It is feasible that a CCPA business by responding to one consumer's request could negatively impact another consumer's CCPA rights or require more burdensome compliance for the business. For example, in the real estate context a buyer might request disclosure from a REALTOR® that could require the disclosure of PI that also qualifies as the seller's PI. Similarly, a seller may request deletion of PI that also qualifies as a buyer's PI where the buyer wishes the REALTOR® business to continue to retain the PI. Additional guidance on how to properly process and respond to requests for information that involve multiple unrelated households and/or consumers would be helpful.



REALTOR® is a federally registered collective membership mark which identifies a real estate professional who is a Member of the NATIONAL ASSOCIATION OF REALTORS® and subscribes to its strict Code of Ethics.



Personal Information of Minors

Real estate transactions are likely to deal with the PI of families, which may very well include minors. Under the current law, if a business has actual knowledge that a minor's PI is collected, there needs to be an opt-in. Moreover, under CCPA as currently drafted, there is no scope for an implied opt-in, such as when two parents of minors provide their own PI to a REALTOR® in the course of a real estate transaction where the parents' PI also qualifies as the PI of the minors. Thus, when a business collects the parents' PI that would also qualify as their children's PI, like the family of two parents and their minor children suggested above, does the presence of minors subject all of the PI to opt-in requirements, both as household PI and as individual PI that relates to both adult and children? This would seem to pose an unintended but nevertheless unduly burdensome impact on business; therefore, we would request further guidance on how to handle this common scenario.

Anti-Discrimination

Under the CCPA, businesses may not discriminate against consumers for exercising their rights under the law. This is a laudable goal and in line with our State's long history of leading the way with regard to ensuring that all Californians are treated equally in the eyes of the law. However, there are circumstances under which the exercise of a CCPA right unavoidably will lead to a different level of service.

For example, one of the many benefits of listing a property with a licensed real estate agent or broker is that the property is listed on the Multiple Listing Service ("MLS") after a listing agreement is signed. If a consumer exercises his or right to opt out of any sharing of PI, the listing either cannot be completed or will be incomplete. Our industry currently gives consumers the right to do so irrespective of the CCPA, but we warn that this can restrict the ability of a listing agent to effectively market the seller's property and could mean a seller doesn't receive as high a sales price as if they had listed on the MLS. But under the CCPA, a consumer could complain that they were discriminated against for exercising their opt-out rights to not have their PI shared with the MLS, resulting in a lower sales price, despite the clear warnings that our members give as industry-standard. The regulations should be clarified so that not providing a service that cannot be offered due to the exercise of a CCPA right is not considered discriminatory.

Conclusion

C.A.R. thanks the Office of the Attorney General for their work on these regulations and looks forward to a collaborative relationship in building a regulatory framework that both protects consumer privacy and ensures that the real estate market continues to function in a healthy manner. If you or a member of your staff have any questions or comments, please do not hesitate to contact me at [REDACTED] or [REDACTED]

Sincerely,



Anna Buck
Legislative Advocate

Message

From: Andre Cotten [REDACTED]
Sent: 12/6/2019 8:51:06 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CA AG NPR concerning the CCPA: Consumer Bankers Association Comment
Attachments: California AG NPR concerning the CCPA - Consumer Bankers Comment .pdf

Hi—

Please find the Consumer Bankers Association's comment attached.

Best,

ANDRE' B. COTTEN, ESQ.

Assistant Vice President, Regulatory Counsel
Consumer Bankers Association
1225 Eye Street, NW, #550 | Washington, DC 20005
[REDACTED]

***CBA LIVE 2020**

San Diego, CA | March 23-25



December 6, 2019

VIA ELECTRONIC SUBMISSION

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

Re: Notice of Proposed Rulemaking Regarding the California Consumer Privacy Act

Dear Mr. Becerra:

The Consumer Bankers Association¹ (“CBA” or “the Association”) appreciates the opportunity to offer our views on the California Attorney General’s (“the Attorney General” or “the AG”) Notice of Proposed Rulemaking (the “Proposed Rule” or the “Draft Regulations”) concerning California’s regulatory approach to the California Consumer Privacy Act (the “Act” or “the CCPA”).

CBA appreciates the Attorney General’s efforts to provide guidance to businesses on how to comply with the CCPA and to clarify the Act’s requirements through proposed regulations. Most importantly, CBA’s member banks share the Attorney General’s goal of protecting the privacy of consumers. However, we have significant concerns about the proposed regulations as drafted by the Attorney General. Below, we have identified our most pressing issues and offered the Attorney General solutions to consider in the next phase of the rule writing process.

I. The Attorney General’s Right to Opt-Out of Sale Guidance is Insufficient to Address Practical Business Concerns.

CBA urges the Attorney General to provide more certainty about the right to opt-out of sales of personal information. From a review of the draft regulations, it seems a bank, or any covered entity, may present the choice to opt-out of certain sales, so long as a global option to opt-out of the sale of all personal information is more prominently presented than other choices. Note, this option assumes a global option is feasible. From a practical perspective, it is likely a business may possess varying data elements about a single consumer through different relationships with the consumer, which may not be linked.

Moreover, the proposed regulations require a bank, or covered entity, which collects personal information from consumers online to “treat user-enabled privacy controls, such as browser plugin or privacy setting or another mechanism, which communicates or signal the consumer’s choice to opt-out of

¹ The Consumer Bankers Association is the only national trade association focused exclusively on retail banking. Established in 1919, the Association is now a leading voice in the banking industry and Washington, representing members who employ nearly two million Americans, extend roughly \$3 trillion in consumer loans, and provide \$270 billion in small business loans.

the sale as a valid request” to opt-out of sale of personal information “for that browser or device, or, if known, for that consumer.” This raises a number of operational complexities and issues since neither the statute nor the proposed regulations condition this opt-out method being a well-established or widely used standard to communicate requests to opt out of sale of personal information.

II. Provide Covered Entities with a Safe Harbor When Verifying Consumer Requests.

The CCPA establishes a series of rights which are contingent upon the receipt and authentication of a “verifiable consumer request.” In order to comply with a consumer’s request to exercise his or her rights under the CCPA, the “business shall promptly take steps to determine whether the request is a verifiable consumer request.”

CBA appreciates the Attorney General for providing helpful guidance related to verification requests. Generally, the proposed regulations direct banks to use a more rigorous verification process when dealing with more sensitive information. The proposed regulations also take it a step further by directing banks not to release sensitive information without being highly certain about the identity of the individual requesting the information. The proposed regulations also provide prescriptive steps of what to do in cases where an identity cannot be verified.

As the Attorney General is aware, banks collect personal information as part of routine transactions to facilitate consumer requests. Even with the proposed rules, furnishing personal information to customers purporting to exercise their rights under the CCPA, in response to a verifiable consumer request, may result in unintended risk and harm to the consumer, including misuse of personal information to perpetuate fraud and identity theft. As a potential solution, the Attorney General should establish a safe harbor from liability to assure banks, and other covered entities, that rejecting a suspicious right of access request in good faith will not later result in a violation.

Moreover, CBA implores the Attorney General to look to the implementation issues encountered by the General Data Protection Regulation (GDPR) in its next stage of rule writing. According to a study published by Blackhat USA 2019 (“the Study”)², the Study demonstrates how legal ambiguity surrounding the “right of access” process may be used by social engineers to facilitate fraud. The Study’s experimental findings also demonstrate many organizations fail to adequately verify the originating identity of right of access requests. As a result, social engineers can abuse right of access requests as a scalable attack mechanism for acquiring deeply sensitive information about individuals.

The Attorney General’s proposed regulations do not seem to consider the prevalence and petulance of social engineers. Without a safe harbor from liability, banks may be hesitant to reject the legitimacy of consumer requests for fear of potential enforcement actions. Thus, the Attorney General’s oversight would allow more potential gateways for social engineers to exploit legal and policy loopholes.

As the CCPA is set to apply to various industries, CBA also encourages the Attorney General to better consider a business’ size and complexity, the nature and scope of its business activities, and the sensitivity of any personal information at issue. In alternative, the Attorney General may consider

² <https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf>

utilizing principles such as those found in existing authentication guidance issued by the Federal Financial Institutions Examination Council.

III. The CCPA as Proposed is Potentially Harmful for Consumers' Information.

Building on the previous discussion, CBA encourages the Attorney General to finalize a rule which does not put consumers at any additional risk of fraud or identity theft. The proposed regulations impose new disclosure obligations beyond those enumerated in the statute.

In particular, the proposed disclosures require banks, and other covered entities, to specify a potentially concerning level of detail about certain privacy practices. For example, the draft would require a business to address the following new disclosures:

- Describe the process the bank will use to verify the consumer request, including any information the consumer must provide;
- Explain how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf; and
- For each category of personal information collected, provide the categories of sources from which the information was collected, the business or commercial purposes(s) for which the information was collected, and the categories of third parties with whom the business shares personal information.

As previously mentioned, banks are constantly having to safeguard and mitigate against potential and real fraud. The CCPA as proposed seems to be another apparent path for fraudsters to attempt to infiltrate the banking system and harm real consumers.

IV. The CCPA Should Protect the Intellectual Property Rights of Covered Entities.

As the proposed rules are currently written, CBA believes the CCPA may infringe on the intellectual property rights of our member banks. Pursuant to § 1798.185(a)(3), the CCPA grants the Attorney General 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."

Furthermore, we urge the Attorney General to include a rule to establish an exception from the CCPA for intellectual property or for data which, if disclosed, would have an adverse effect on the rights or freedoms of others. The CCPA should not apply to information which is protected intellectual property of a bank, or any other covered entity, including information subject to copyright, patent, service mark and/or trade secret protections. A bank also should be required to disclose any information which is subject to intellectual property protections, including any formula, pattern, compilation, program, device, method, technique or process developed to process or analyze personal information, or any information derived from such process or analysis.

The Attorney General should consider duplicating the EU's GDPR approach to intellectual property. The GDPR places reasonable limitations on its enumerated consumer privacy rights. It provides both an intellectual property exclusion and the avoidance of infringement on the rights of others. CBA believes its

member banks, and other covered entities, deserve the same protections if a bank is presented with a scenario where its attempt to comply with a consumer's request may put it in the position of violating the rights of others or placing it in jeopardy with its competitors.

V. The Definition of "Sell" is too Broad and Unnecessarily Burdensome.

The CCPA includes definition for "sell" as follows:

"(t)(1) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration. (2) For purposes of this title, a business does not sell personal information when: (A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party. (B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.

(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met: (i) The business has provided notice that information being used or shared in its terms and conditions consistent with § 1798.135. (ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose. (D) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with § 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with § 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with § 17200) of Part 2 of Division 7 of the Business and Professions Code)."

CBA urges the Attorney General to provide more clarification about the covered activities in its definition of "sell." The definition as written is too general and too open-ended. There are a myriad of activities which would possibly fall within the CCPA's current definition of sale, which see beyond the scope of the law's actual public policy concerns. For example, cookies embedded on a bank's website could currently be construed to be covered under the current definition of "sell." As an additional practical complexity posed by the CCPA, it is also unclear how a bank's interactions with the Google

search engine or via an ad placed on Facebook would be treated under the current definition. There is also a lack of clarity about what constitutes valuable consideration under the CCPA.

Note, banks, and other covered financial institutions, are also unsure about the scope of the CCPA's Gramm-Leach-Bliley exception. The Attorney General should draft rules to provided banks, and other covered entities, with the clarity needed to comply with this comprehensive privacy law.

VI. Transfers of Personal Information to Service Providers is Not a Sale.

Banks, and other financial institutions, transfer personal information to service providers to maximize the consumer experience by providing products and services. These transfers are not sales as contemplated in the CCPA, and the final regulations should clarify this distinction for service providers. Section 999.314 proposes a covered entity which otherwise meets the definition of a service provider is a service provider even if it collects personal information directly from consumers at the request of a business.

Note, the proposed rules also state a service provider which also meets the definition of a business must comply with the CCPA for any personal information it collects or sells outside of its role as a service provider. CBA supports this proposed clarification regarding service providers, and we urge the Attorney General to consider further clarifications. A final rule with additional clarity is essential to ensure banks, and other financial institutions, can transfer personal information to a service provider to benefit the bank's customers without the transfer being deemed a sale of personal information pursuant to the CCPA.

VII. Provide More Clarity Concerning the "Right to Cure."

Section 1798.155(b) states, in part, a "[bank] shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance." To begin, the Attorney General's regulations did not propose any rules to codify this provision of the CCPA. CBA urges the Attorney General to establish specific criteria for what is necessary in order for a bank, or other covered entity, to successfully "cure" a violation.

The Attorney General should provide more detailed guidance. For example, there may be a circumstance where a cure cannot unwind the effects of a violation, guidance is needed as to other means in which the bank, other covered entity, could cure, or mitigate against, the violation through implementation of enhanced business practices.

VIII. The "Lookback" Period Should Begin January 1, 2020.

As the proposed rules are currently written, the CCPA appears to apply retroactively by requiring businesses to provide information subject to a consumer's request covering the time period prior to the Act's effective date and prior to the publication of implementing regulations. CBA believes rulemaking should clarify the 12-month lookback period provided for in § 1798.130 applies from the effective date of

the CCPA, which is January 1, 2020. This change would preclude its application to activities occurring prior to the effective date.

IX. Establish an Effective Date for Final Rules to Allow Covered Entities Adequate Time to Comply.

The Attorney General should exercise its discretionary authority to set an effective date of 18 months after the final rules are issued. CBA believes this extension is essential so banks, and other covered entities, can properly comply. Banks will need sufficient time to review and implement direction from the Attorney General's final regulations, which may require changes to implementation plans which were based in good faith on the statutory language, prior to regulations being adopted.

For example, the final regulations will require banks, and other covered entities, to change their verification processes due to the CCPA's prescriptive requirements, e.g. "double" authentication for deletion, declaration signed under penalty of perjury, etc. These potential changes and clarifications will require development work, testing and validation, and employee training. Truncating these necessary steps into a potentially short time frame, e.g. 1 month, may create the undue operation risk of either not properly verifying a valid request or disclosing information to the incorrect person. These types of risks are anti-consumer and preventable.

Currently, the CCPA's deadline for the Attorney General's rulemaking is July 1, 2020, six months after the law's January 1 effective date. Pursuant to the CCPA, the Attorney General could technically begin enforcement of the CCPA on July 1, 2020, which is the same day the final rules could be published. This would be an unreasonable request for covered entities. CBA supports the goal of consumer privacy protection, however, the CCPA is complex and in part, unclear. Banks, and other covered entities, will need sufficient time to come into full compliance to ensure they implement the full privacy protections as intended by the legislature to ultimately benefit consumers.

X. Establish an Enforcement Date of No Earlier than July 1, 2020.

CBA urges the Attorney General to preclude any enforcement action based on conduct or omission occurring on or after the enforcement date. The CCPA provides in §1798.185(c), the "Attorney General shall not bring an enforcement action under this title until six months after the publication of the final issued pursuant to this section or July 1, 2020, whichever is sooner." For example, if the enforcement date is July 1, 2020, because it is earlier than the six-month anniversary of final regulations, the AG should clarify any enforcement will be based only on conduct or omissions occurring July 1, 2020 or later and not conduct or omissions occurring on or after the CCPA effective date, January 1, 2020.

CBA appreciates the opportunity to comment on the Notice of Proposed Rulemaking, and we plan to continue to engage the California Office of the Attorney General as the rulemaking process continues and to ensure our member banks have the necessary guidance to comply with the tenants of the final rule. Please feel free to contact André Cotten for further discussion regarding our comments at

██████████ or ██████████.

Sincerely,

A handwritten signature in cursive script, appearing to read "Andre B. Cotte".

Assistant Vice President, Regulatory Counsel
Consumer Bankers Association

Message

From: Von Borstel, Megan (Perkins Coie) [REDACTED]
Sent: 12/7/2019 12:42:24 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Shelton Leipzig, Dominique (Perkins Coie) [REDACTED]
Subject: California Chamber Comments Regarding AG's Proposed CCPA Regulations
Attachments: California Chamber of Commerce Comments Regarding Attorney General's Proposed CCPA Regulations December 6 2019.pdf

Office of the Attorney General: Privacy Unit,

On behalf of the California Chamber of Commerce, we wish to thank the Office of the Attorney General for the opportunity to make comments to the Attorney General's draft regulations for the CCPA. Attached are the California Chamber's comments, titled "California Chamber of Commerce Comments Regarding Attorney General's Proposed CCPA Regulations December 6, 2019." Please do not hesitate to contact me with any questions.

Thank you,

Dominique Shelton Leipzig | Perkins Coie LLP
PARTNER PRIVACY & SECURITY
CO-CHAIR AD TECH PRIVACY & DATA MANAGEMENT
1888 Century Park East Suite 1700
Los Angeles, CA 90067-1721
[REDACTED]

Megan Von Borstel | Perkins Coie LLP
ASSOCIATE | she/her/hers
131 S. Dearborn Street Suite 1700
Chicago, IL 60603-5559
[REDACTED]

NOTICE: This communication may contain privileged or other confidential information. If you have received it in error, please advise the sender by reply email and immediately delete the message and any attachments without copying or disclosing the contents. Thank you.



California Chamber of Commerce Comments Regarding Attorney General’s Proposed CCPA Regulations December 6, 2019

JENNIFER BARRERA

EXECUTIVE VICE PRESIDENT



DOMINIQUE SHELTON LEIPZIG

PARTNER



MEGAN VON BORSTEL

ASSOCIATE



Executive Summary

The California Chamber of Commerce (“CalChamber”) submits the comments herein to the California Attorney General’s (“AG”) office regarding the AG’s proposed regulations for the California Consumer Privacy Act (“CCPA”).

Each comment is presented separately in three parts: (a) the header which identifies the proposed regulation; (b) issue headers that synthesize the issue or concern with the proposed regulation; and (c) subparts that identify (i) the proposed regulation, (ii) problem with proposed regulation, and (iii) recommended change(s) in the language to solve or mitigate CalChamber’s related concern(s). Specific language is proposed in Exhibit “A” in a redlined version of the proposed regulations.

As indicated in Exhibit A, we request that the enforcement date of the regulations be delayed until January 1, 2021 to allow time for companies to update their practices to comply. Companies have already spent millions to update their practices for the CCPA itself. It would be burdensome, costly, and in some instances, impossible to change administrative and technical processes for regulations that are not yet final.

As individual groups are raising a variety of discrete issues with the proposed regulations, this is not a collectively exhaustive list; rather, this report is intended to reflect key issues for the CalChamber at large.

JENNIFER BARRERA

EXECUTIVE VICE PRESIDENT



DOMINIQUE SHELTON LEIPZIG

PARTNER



MEGAN VON BORSTEL

ASSOCIATE



Biographies



JENNIFER BARRERA | EXECUTIVE VICE PRESIDENT | CAL CHAMBER

<https://advocacy.calchamber.com/bios/jennifer-barrera>

Jennifer Barrera oversees the development and implementation of policy and strategy as executive vice president and represents the California Chamber of Commerce on legal reform issues.

She led CalChamber advocacy on labor and employment and taxation from September 2010 through the end of 2017. As senior policy advocate in 2017, Barrera worked with the executive vice president in developing policy strategy. She was named senior vice president, policy, for 2018 and promoted to executive vice president as of January 1, 2019.

In addition, she advises the business compliance activities of the CalChamber on interpreting changes in employment law.

From May 2003 until joining the CalChamber staff, she worked at a statewide law firm that specializes in labor/employment defense, now Carothers, DiSane & Freudenberger, LLP. She represented employers in both state and federal court on a variety of issues, including wage and hour disputes, discrimination, harassment, retaliation, breach of contract, and wrongful termination.

She also advised both small and large businesses on compliance issues, presented seminars on various employment-related topics, and regularly authored articles in human resources publications.

Barrera earned a B.A. in English from California State University, Bakersfield, and a J.D. with high honors from California Western School of Law.



DOMINIQUE SHELTON LEIPZIG | PARTNER | LOS ANGELES, CA

www.perkinscoie.com/DSheltonLeipzig/

Privacy and cybersecurity attorney Dominique Shelton co-chairs the firm's Ad Tech Privacy & Data Management group. She provides strategic privacy and cyber-preparedness compliance counseling, and defends, counsels and represents companies on privacy, global data security compliance, data breaches and investigations with an eye towards helping clients avoid litigation. Dominique frequently conducts trainings for senior leadership, corporate boards and audit committees regarding risk identification and mitigation in the areas of privacy and cyber.

She leads companies in legal assessments of privacy, data security, cyber preparedness and compliance with such regulations as the California Consumer Protection Act (CCPA), California Confidentiality of Medical Information Act (CMIA), the Video Privacy Protection Act (VPPA), the Children's Online Privacy Protection Act (COPPA) and the NIST Cybersecurity Framework.

Dominique has significant experience leading investigations related to data and forensic breaches. She has steered investigations for a range of companies, including for national retailers, financial institutions, health and wellness enterprises, media companies and others.

Dominique also advises companies on global privacy and data security, particularly on EU General Data Protection Regulation (GDPR). Her background includes advising on European, Asian and South American privacy and security compliance projects for U.S.-based and overseas companies. In addition, she counsels on strategies for related legal compliance and vendor management in cross-border transfers.

Dominique is the author of two books titled *Implementing the CCPA- a Global Guide for Business* (Sept. 2019, IAPP); and *Transform* (Mar. 2019)



MEGAN VON BORSTEL | ASSOCIATE | CHICAGO, IL

www.perkinscoie.com/megan-von-borstel

Megan Von Borstel has experience with privacy counseling and data breach response. She counsels clients on compliance efforts with state, federal, and international privacy laws and regulations, including the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). Megan is also familiar with the Stored Communications Act, the Biometric Information Protection Act, and various other state and federal statutes.

Megan earned her J.D. at Washington University School of Law, where she served as editor-in-chief for the *Washington University Jurisprudence Review*, received the Judge Amandus Brackman Moot Court Award, and volunteered at the law school's appellate and children's rights clinics. Megan also served as a judicial extern for the Honorable Shirley Padmore Mensah, U.S. Magistrate Judge for the U.S. District Court of Eastern Missouri.

TABLE OF CONTENTS

	Page
I. SECTION 999.315 REQUESTS TO OPT-OUT–CHAMBER PROPOSED CHANGES.....	1
A. ISSUE: BUSINESSES NEED THE OPTION NOT TO TREAT BROWSER PLUG-INS OR SETTINGS AS OPT-OUT REQUESTS, AND INSTEAD HAVE THE CHOICE TO PROVIDE AN OPT-OUT BUTTON.	1
1. Proposed Regulation: 999.315(c); 999.315(g).....	1
2. Problem with Proposed Regulation:	1
3. Recommended Change:	1
B. ISSUE: PROPOSED REGULATIONS GIVE BROWSERS SIGNIFICANT DISCRETION TO EXERCISE AGAINST BUSINESSES THAT BROWSERS MAY BE IN COMPETITION WITH AND WHOSE “SALES” THEY ARE BLOCKING.	1
1. Proposed Regulation: §999.315(a); 999.315(c).....	1
2. Problem with Proposed Regulation:	1
3. Recommended Change:	2
C. ISSUE: PROPOSED REGULATION’S REQUIREMENT TO SHARE OPT-OUT REQUESTS WITH THIRD PARTIES EXCEEDS STATUTORY REQUIREMENTS.....	2
1. Proposed Regulation: §999.315(f).....	2
2. Problem with Proposed Regulation:	2
3. Recommended Change:	3
D. ISSUE: VERIFICATION OR AUTHENTICATION OF CONSUMERS SUBMITTING OPT-OUT REQUESTS SHOULD NOT BE PREVENTED OR LIMITED.....	3
1. Proposed Regulation: §999.315(h)	3
2. Problem with Proposed Regulation:	3
3. Recommended Change:	3
E. ISSUE: RESPONSE TO REQUEST TO OPT-OUT ONLY SHOULD APPLY TO BUSINESS THAT SELL PERSONAL INFORMATION AND MORE TIME TO RESPOND IS NECESSARY.....	3
1. Proposed Regulation: §§999.315(d); 999.315(e).....	3
2. Problem with Proposed Regulation:	3
3. Recommended Change:	3

TABLE OF CONTENTS

(continued)

	Page
II. SECTION 999.307 NOTICE OF FINANCIAL INCENTIVE–CHAMBER PROPOSED CHANGES	4
A. ISSUE: DATA DOES NOT HAVE INDEPENDENT VALUE	4
1. Proposed Regulation: §999.307; 999.337	4
2. Problem with Proposed Regulation:	4
3. Recommended Change:	4
B. ISSUE: REGULATION CREATES ONEROUS DISCLOSURE REQUIREMENTS.....	4
1. Proposed Regulation: §999.307(a); 999.307(a)(3); 999.307(b)(2); 999.307(b)(5)	4
2. Problem with Proposed Regulation:	4
3. Recommended Change:	4
III. SECTION 999.313 RESPONDING TO REQUESTS TO KNOW AND REQUESTS TO DELETE–CHAMBER PROPOSED CHANGES	5
A. ISSUE: UNVERIFIABLE REQUESTS TO DELETE SHOULD NOT BE REQUIRED TO BE TREATED AS OPT-OUTS BECAUSE IT CHANGES THE CONSUMER’S INTENT, INCREASES COSTS, AND EXACERBATES DIFFICULTIES WITH DELETING DATA FROM ARCHIVES OR BACKUPS.....	5
1. Proposed Regulation: §999.313(d)	5
2. Problem with Proposed Regulation:	5
3. Recommended Change:	6
B. ISSUE: ENSURE BUSINESSES HAVE ENOUGH TIME AND FLEXIBILITY TO RESPOND TO REQUESTS UNDER STATUTORY TIMEFRAME.....	7
1. Proposed Regulation: §999.313(a); 999.313(b).....	7
2. Problem with Proposed Regulation:	7
3. Recommended Change:	7
C. ISSUE: PROPOSED REGULATION REQUIREMENTS HEIGHTEN BURDENS ON BUSINESS AND EXCEED STATUTORY LANGUAGE.....	7
1. Proposed Regulation: §999.313	7
2. Problem with Proposed Regulation:	7
3. Recommended Change:	8

TABLE OF CONTENTS

(continued)

	Page
D. ISSUE: REGULATION SHOULD CLARIFY THAT A BUSINESS’S OBLIGATION TO COMPLY WITH A CONSUMER REQUEST IS LIMITED TO ITS ABILITY TO IDENTIFY RESPONSIVE MATERIALS USING COMMERCIALY REASONABLE EFFORTS.	8
1. Proposed Regulation: §999.313(c); 999.313(d).....	8
2. Problem with Proposed Regulation:	8
3. Recommended Change:	9
E. ISSUE: REGULATION SHOULD CONSIDER HOW RESPONDING TO REQUESTS COULD JEOPARDIZE OTHER CUSTOMERS’ SECURITY AS WELL.....	9
1. Proposed Regulation: §999.313(c)(3); <i>see also</i> 999.313(d); 999.323.....	9
2. Problem with Proposed Regulation:	9
3. Recommended Change:	9
F. ISSUE: REGULATION DOES NOT ADDRESS REQUESTS SEEKING PORTABILITY OF INFORMATION WHERE DISCLOSURE OF CONSUMER’S PERSONAL INFORMATION IS NECESSARY TO SUPPORT PORTABILITY.....	9
1. Proposed Regulation: §999.313(c)(4).....	9
2. Problem with Proposed Regulation:	9
3. Recommended Change:	9
G. ISSUE: NOTIFYING CONSUMER OF REASON FOR REQUEST DENIAL MAY INTERFERE WITH LAW ENFORCEMENT INVESTIGATION, HINDER BUSINESS OPERATIONS, AND IS CONTRARY TO THE PURPOSE OF AN EXEMPTION.....	10
1. Proposed Regulation: §999.313(c)(5).....	10
2. Problem with Proposed Regulation:	10
3. Recommended Change:	10
H. ISSUE: INDIVIDUALIZED RESPONSES TO CATEGORIES OF SOURCES OR THIRD PARTIES IS TOO BURDENSOME FOR BUSINESSES.....	10
1. Proposed Regulation: §999.313(c)(9)-(10).....	10
2. Problem with Proposed Regulation:	10
3. Recommended Change:	11

TABLE OF CONTENTS

(continued)

	Page
IV. SECTION 999.314 SERVICE PROVIDERS–CHAMBER PROPOSED CHANGES.....	11
A. ISSUE: PROPOSED REGULATIONS’ LIMITATIONS ON SERVICE PROVIDERS’ PERMISSIBLE USES OF DATA CONTRADICTS THE STATUTORY DEFINITION OF “BUSINESS PURPOSE” AND “SERVICE PROVIDER.”	11
1. Proposed Regulation: §999.314(c).....	11
2. Problems with Proposed Regulation:.....	11
3. Recommended Change:	12
B. ISSUE: PROPOSED REGULATION CREATES ADDITIONAL BURDENS FOR BUSINESS THAT EXCEED STATUTORY LANGUAGE.	12
1. Proposed Regulation: §999.314(d)	12
2. Problem with Proposed Regulation:	12
3. Recommended Change:	13
V. SECTION 999.301 DEFINITIONS–CHAMBER PROPOSED CHANGES.....	13
A. ISSUE: DEFINITION OF RIGHT TO KNOW CONFLICTS WITH REQUIREMENTS FOR HOW TO RESPOND TO RIGHT TO KNOW.	13
1. Proposed Regulation: §§999.301(n); 999.313(c)(10)	13
2. Problem with Proposed Regulation:	13
3. Recommended Change:	13
B. ISSUE: DEFINITION OF RIGHT TO KNOW CREATES INFEASIBLE REQUIREMENTS FOR RESPONDING TO INDIVIDUAL CONSUMER REQUESTS.	13
1. Proposed Regulation: §999.301(n).	13
2. Problem with Proposed Regulation:	13
3. Recommended Change:	13
C. THE SCOPE OF THE DEFINITION OF “PRICE OR SERVICE DIFFERENCE” COULD PREVENT BUSINESS WITH SERVICE PROVIDERS.	14
1. Proposed Regulation: §999.301(l)	14
2. Problem with Proposed Regulation:	14
3. Recommended Change:	14

TABLE OF CONTENTS

(continued)

	Page
D. ISSUE: DEFINITION OF “AFFIRMATIVE AUTHORIZATION” REQUIREMENT FOR TWO-STEP PROCESS TO OPT-IN IS OVERLY BURDENSOME FOR CONSUMERS AND BUSINESS.	14
1. Proposed Regulation: §999.301(a).....	14
2. Problem with Proposed Regulation:	14
3. Recommended Change:	14
E. ISSUE: PROPOSED REGULATIONS NEED TO PROVIDE CLARIFICATION REGARDING DEFINITION OF DIRECT NOTICE TO CONSUMERS.....	14
1. Proposed Regulation: §999.301; <i>see also</i> §§999.305(a)(3); 999.305(d)(1); 999.306(d)(2).....	14
2. Problem with Proposed Regulation:	14
3. Recommended Change:	14
VI. SECTION 999.300 TITLE AND SCOPE—CHAMBER PROPOSED CHANGES	15
A. ISSUE: THE REGULATIONS SHOULD CLARIFY THE CCPA’S JURISDICTIONAL SCOPE AND EFFECTIVE DATE.	15
1. Proposed Regulation: §999.300	15
2. Problem with Proposed Regulation:	15
3. Recommended Change:	15
VII. SECTION 999.305 NOTICE AT COLLECTION OF PERSONAL INFORMATION—CHAMBER PROPOSED CHANGES	15
A. ISSUE: PROPOSED REGULATION REQUIREMENTS FOR EACH CATEGORY OF PERSONAL INFORMATION EXCEED STATUTORY REQUIREMENTS.....	15
1. Proposed Regulation: §999.305; 999.305(d)(2)(b).....	15
2. Problem with Proposed Regulation:	15
3. Recommended Change:	16
B. ISSUE: PROPOSED REGULATION’S REQUIREMENT FOR EXPLICIT CONSENT EXCEEDS STATUTORY REQUIREMENTS.....	16
1. Proposed Regulation: §999.305(a)(3).....	16
2. Problem with Proposed Regulation:	16
3. Recommended Change:	16

TABLE OF CONTENTS

(continued)

	Page
C. ISSUE: NOTICE AT COLLECTION IS IMPRACTICAL UNDER CERTAIN CIRCUMSTANCES AND EXCEEDS THE STATUTORY PURPOSE.....	16
1. Proposed Regulation: §999.305(a)(2); 999.305(c)	16
2. Problem with Proposed Regulation:	16
3. Recommended Change:	17
D. ISSUE: ACCESSIBILITY FOR CONSUMERS WITH DISABILITIES SHOULD BE CLARIFIED TO BE WHEN REQUIRED BY THE AMERICANS WITH DISABILITIES ACT OF 1990.....	17
1. Proposed Regulation: §999.305(a)(2)(d); <i>see also</i> §§999.306(a)(2)(d); 999.307(a)(2)(d); 999.308(a)(2)(d).....	17
2. Problem with Proposed Regulation:	17
3. Recommended Change:	17
E. ISSUE: REGULATION DOES NOT ACCOUNT FOR SCENARIO WHERE BUSINESS RECEIVES PERSONAL INFORMATION ABOUT A CONSUMER FROM ANOTHER BUSINESS AND THEN CREATES ITS OWN DIRECT RELATIONSHIP WITH THE CONSUMER.	17
1. Proposed Regulation: §999.305	17
2. Problem with Proposed Regulation:	17
3. Recommend Change:	17
VIII. SECTION 999.306 NOTICE OF RIGHT TO OPT-OUT OF SALE OF PERSONAL INFORMATION—CHAMBER PROPOSED CHANGES.....	18
A. ISSUE: PROPOSED REGULATION EXCEEDS STATUTORY LANGUAGE, LIMITING BUSINESS ABILITY TO OPERATE, AND CREATES UNTENABLE COMPLIANCE OBLIGATIONS.....	18
1. Proposed Regulation: §999.306; 999.306(a)(1).....	18
2. Problem with Proposed Regulation:	18
3. Recommended Change:	18
B. ISSUE: REGULATION IMPROPERLY FORCES BUSINESS TO MAKE FUTURE REPRESENTATIONS TO CUSTOMERS.....	18
1. Proposed Regulation: §§999.306(d)(1); 999.306(d)(2)	18
2. Problem with Proposed Regulation:	18
3. Recommended Change	18

TABLE OF CONTENTS

(continued)

	Page
C. ISSUE: REGULATION COMPLICATES OPT-OUT NOTICE AND CREATES UNNECESSARY BURDEN FOR BUSINESS	18
1. Proposed Regulation: §999.306(d)	18
2. Problem with Proposed Regulation:	18
3. Recommended Change:	19
IX. SECTION 999.312 METHODS FOR SUBMITTING REQUESTS TO KNOW AND REQUESTS TO DELETE–CHAMBER PROPOSED CHANGES	19
A. ISSUE: MANDATING A THIRD METHOD FOR SUBMITTING REQUESTS IS UNNECESSARY, POSES SECURITY RISKS, AND CREATES CONFUSION.	19
1. Proposed Regulation: §999.312	19
2. Problem with Proposed Regulation:	19
3. Recommended Change:	20
B. ISSUE: REGULATIONS REQUIRE SAME RESPONSE REQUIREMENTS REGARDLESS OF WHAT METHOD WAS USED TO SUBMIT THE REQUEST.	20
1. Proposed Regulation: §999.312(e); 999.313(f)	20
2. Problem with Proposed Regulation:	20
3. Recommended Change:	21
C. ISSUE: MANDATING A TWO-STEP PROCESS DISEMPOWERS THE CONSUMER.	21
1. Proposed Regulation: §999.312(d)	21
2. Problem with Proposed Regulation:	21
3. Recommended Change:	21
X. SECTION 999.317 TRAINING; RECORD-KEEPING–CHAMBER PROPOSED CHANGES	21
A. ISSUE: RECORD-KEEPING REQUIREMENT DOES NOT ALIGN WITH PURPOSES OF CCPA.	21
1. Proposed Regulation: §999.317(g)	21
2. Problem with Proposed Regulation:	21
3. Recommended Change:	21
XI. SECTION 999.316 REQUESTS TO OPT-IN AFTER OPTING OUT OF THE SALE OF PERSONAL INFORMATION–CHAMBER PROPOSED CHANGES	22

TABLE OF CONTENTS

(continued)

	Page
A. ISSUE: REGULATION’S TWO-STEP PROCESS CREATES UNNECESSARY FRICTION AND CONSUMER CONFUSION.	22
1. Proposed Regulation: §999.316(a).....	22
2. Problem with Proposed Regulation:	22
3. Recommended Change:	22
XII. SECTION 999.325 VERIFICATION FOR NON-ACCOUNTHOLDERS–CHAMBER PROPOSED CHANGES	22
A. ISSUE: SIGNED DECLARATION OF PERJURY REQUIREMENT IS UNNECESSARY.	22
1. Proposed Regulation: §999.325(c).....	22
2. Problem with Proposed Regulation:	22
3. Recommended Change:	23
B. ISSUE: REQUIREMENT THAT BUSINESSES PROVIDE TWO TIERS OF AUTHENTICATION FOR RIGHT TO KNOW REQUESTS IS OVERLY BURDENSOME AND NOT COMMON PRACTICE.	23
1. Proposed Regulation: §999.325	23
2. Problem with Proposed Regulation:	23
3. Recommended Change:	23
C. ISSUE: TYPES AND THRESHOLD OF PERSONAL INFORMATION FOR VERIFIABLE REQUEST MAY LEAVE CONSUMERS VULNERABLE TO FRAUDULENT REQUESTS.....	23
1. Proposed Regulation: §999.325(c); 999.325(e); <i>see also</i> 999.323	23
2. Problem with Proposed Regulation:	23
3. Recommended Change:	23
XIII. SECTION 999.308 PRIVACY POLICY–CHAMBER PROPOSED CHANGES	24
A. ISSUE: REQUIREMENT THAT BUSINESS PUBLICLY DESCRIBE VERIFICATION PROCESS SHOULD BE ELIMINATED OR SATISFIED BY GENERAL DESCRIPTIONS TO MITIGATE SECURITY RISKS.....	24
1. Proposed Regulation: §999.308(b)(1); <i>see also</i> 999.313(a)	24
2. Problem with Proposed Regulation:	24
3. Recommended Change:	24

TABLE OF CONTENTS

(continued)

	Page
B. ISSUE: REGULATIONS SHOULD PROVIDE CLARIFICATION REGARDING THE REQUISITE LEVEL OF DETAIL TO DESIGNATE AN AUTHORIZED AGENT TO MAKE CONSUMER REQUESTS.....	24
1. Proposed Regulation: §999.308(b)(5)(a);	24
2. Problem with Proposed Regulation:	24
3. Recommended Change:	24
XIV. SECTION 999.318 REQUESTS TO ACCESS OR DELETE HOUSEHOLD INFORMATION—CHAMBER PROPOSED CHANGES	25
A. ISSUE: PROPOSED REGULATION DOES NOT ADDRESS CONCERN THAT HOUSEHOLD INFORMATION COULD BE DISCLOSED INCORRECTLY	25
1. Proposed Regulation: §999.318(b)	25
2. Problem with Proposed Regulation:	25
3. Recommended Change:	25
XV. SECTION 999.323 GENERAL RULES REGARDING VERIFICATION—CHAMBER PROPOSED CHANGES	25
A. ISSUE: INCREASED COMPLEXITY FOR VERIFICATION OF CONSUMERS.	25
1. Proposed Regulation: §999.323; 999.323(d)	25
2. Problem with Proposed Regulation:	25
3. Recommended Change:	25
B. ISSUE: REQUIREMENT TO GENERALLY AVOID REQUESTING ADDITIONAL CONSUMER INFORMATION FOR VERIFICATION IS COUNTERINTUITIVE TO NEED TO ENSURE VERIFICATION AND PROTECT CONSUMER SECURITY.....	26
1. Proposed Regulation: §999.323(c).....	26
2. Problem with Proposed Regulation:	26
3. Recommended Change:	26
XVI. SECTION 999.326 AUTHORIZED AGENT—CHAMBER PROPOSED CHANGES.....	26
A. ISSUE: BUSINESSES NEED MORE GUIDANCE REGARDING VERIFICATION OF AUTHORIZED AGENTS.....	26
1. Proposed Regulation: §999.326	26
2. Problem with Proposed Regulation:	26

TABLE OF CONTENTS

(continued)

	Page
3. Recommended Change:	26
XVII. SECTION 999.336 DISCRIMINATORY PRACTICES–CHAMBER PROPOSED CHANGES	26
A. ISSUE: AMBIGUITY IN PROPOSED REGULATION RELATED TO “FINANCIAL INCENTIVE” CREATES CONFUSION CONCERNING HOW LOYALTY PROGRAMS WILL OPERATE UNDER THE CCPA.	26
1. Proposed Regulation: §999.336	26
2. Problem with Proposed Regulation:	26
3. Recommended Changes:	27
XVIII. SECTION 999.337 CALCULATING THE VALUE OF CONSUMER DATA– CHAMBER PROPOSED CHANGES	27
A. ISSUE: PROPOSED REGULATIONS ARE INCONSISTENT WITH STATUTORY LANGUAGE.....	27
1. Proposed Regulation: §999.337	27
2. Problem with Proposed Regulation:	27
3. Recommend Change:	27
XIX. SECTION 999.330 MINORS UNDER 13 YEARS OF AGE–CHAMBER PROPOSED CHANGES	27
A. ISSUE: REGULATIONS SHOULD ALLOW FOR ANY METHOD PERMITTED BY COPPA FOR DISCLOSURE.	27
1. Proposed Regulation: §999.330(a).....	27
2. Problem with Proposed Regulation:	27
3. Recommended Change:	27
XX. SECTION 999.331 MINORS 13 TO 16 YEARS OF AGE–CHAMBER PROPOSED CHANGES	28
A. ISSUE: BUSINESSES THAT DO NOT PLAN TO SELL PERSONAL INFORMATION OF 13 TO 16 YEARS OLD SHOULD NOT NEED TO HAVE AN OPT-IN MECHANISM.	28
1. Proposed Regulation: §999.331(a).....	28
2. Problem with Proposed Regulation:	28
3. Recommended Change:	28

I. SECTION 999.315 REQUESTS TO OPT-OUT-CHAMBER PROPOSED CHANGES

A. ISSUE: BUSINESSES NEED THE OPTION NOT TO TREAT BROWSER PLUG-INS OR SETTINGS AS OPT-OUT REQUESTS, AND INSTEAD HAVE THE CHOICE TO PROVIDE AN OPT-OUT BUTTON.

1. Proposed Regulation: 999.315(c); 999.315(g)
2. Problem with Proposed Regulation:
 - a. CalChamber proposes that the AG's Office defer the browser enabled signal issue until after the California Privacy Rights Act of 2020 (CPRA) is voted on in November 2020 if it qualifies. As the CPRA at section 1798.185 provides for rule making at subsection 20-21, it would represent cost savings to industry and regulators to undergo this process once rather than twice in two years.
 - b. Existing browser signals are not "opt-out of sale" signals. There is also no industry-accepted technical standard regarding opt-out via a browser mechanism. Further, there is no guarantee that a browser installed opt-out reflects actual consumer choice versus a technical default.
 - c. The proposed regulations do not provide sufficient clarity as to what criteria must be present with respect to mechanisms developed in the future that may be effectuating a consumer choice.
 - d. These types of technology were designed in other contexts and are not aligned with the CCPA's complex and extremely broad definitions of "sale" and "personal information." The CCPA emphasizes consumer choice. It specifically defines a mechanism, the "Do Not Sell" button, that businesses must make available to consumers on their Web sites to exercise their choices. It is not consistent with the statute to create this additional mechanism, nor is it clear that consumers, who use plug-ins, intend to opt-out of CCPA sales. Currently, browser-based opt-out technology is not sufficiently interoperable and developed to ensure that all parties that receive such a signal can operationalize it.
 - e. A business should not be required to treat these settings as an official CCPA opt-out request. A business should be able to accept the browser-enabled method or provide the 'Opt-Out Button' and related processes set forth herein as an alternative.
3. Recommended Change:
 - a. Revise Section 999.315(c): "If a business collects personal information from consumers online, the business ~~shall~~ may treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer, provided that the consumer undertakes an affirmative action to opt-out of the sale of their information. Default opt-outs shall not constitute an affirmative step to opt-out."

B. ISSUE: PROPOSED REGULATIONS GIVE BROWSERS SIGNIFICANT DISCRETION TO EXERCISE AGAINST BUSINESSES THAT BROWSERS MAY BE IN COMPETITION WITH AND WHOSE "SALES" THEY ARE BLOCKING.

1. Proposed Regulation: §999.315(a); 999.315(c)
2. Problem with Proposed Regulation:
 - a. Regulations describe permitting a browser plugin or privacy setting to communicate a consumer opt-out of the sale of their personal information. Codifying browser-based signals would give significant power to browsers, who could unilaterally turn on "Do Not Sell" or even do it selectively for certain companies. In the event a browser-based

program will be established, to avoid the potential for self-serving implementation by browsers/devices, the law should empower the AG/Agency (whichever is in charge) to establish a uniform mechanism that browsers/devices would be required to implement so there is a level playing field for businesses and clarity for consumers.

3. Recommended Change:

- a. Revise section 999.315(a): “A business shall provide two or more designated methods for submitting requests to opt-out, including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information,” or “Do Not Sell My Info,” on the business’s website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information. The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should: (i) ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business; (ii) ensure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer, and does not require that the consumer provide additional information beyond what is necessary; (iii) clearly represent a consumer’s intent and be free of defaults constraining or presupposing such intent; and (iv) ensure that the opt-out preference signal does not conflict with other commonly-used privacy settings or tools that consumers may employ.”

C. ISSUE: PROPOSED REGULATION’S REQUIREMENT TO SHARE OPT-OUT REQUESTS WITH THIRD PARTIES EXCEEDS STATUTORY REQUIREMENTS.

1. Proposed Regulation: §999.315(f)

2. Problem with Proposed Regulation:

- a. Under section 999.315(f), a business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business’s receipt of the request and notify the consumer when this has been completed. Under the CCPA, there is no requirement for the sharing of a consumer requests outside of a service provider relationship in the context of deletion. 1798.105(c). The provision would likely result in a burdensome obligation to monitor and track the performance of a third party’s compliance, with no additional benefit to the consumer. A requirement to share opt-out requests with third parties is outside the scope of the CCPA. Also, this would be impossible for a business to do if the browser controls opt-out from sale and the option remains part of the regulatory framework.
- b. The CCPA does not address how a business that collects data from another business can provide the required consumer disclosure at the point of collection. The draft regulations allow either (1) contacting the consumer directly or (2) contact the source of the personal information to confirm notice was provided and obtain a signed attestation with an example of the notice from the source. The draft regulations go beyond a signed attestation or contractual assurances to require a description and example of the notice at collection and require the business to provide a copy of the attestation to the consumer upon request. The obligation presumes that a data user has proximity to the original collector. The AG’s statement of reasons suggests that this additional information would provide additional consumer protections by providing internal checks. However, the requirement would result in a burdensome and expensive process and require an organization to manage the CCPA compliance obligations of first-party collection, despite these obligations already required by law.
- c. A consumer exercising its right to know will also receive a description of the categories of business in which its personal information is sold. This list should be a roadmap for the consumer to exercise its rights with each individual business. A consumer may not

want each business to be opted-out of the sale of its personal information and this provision would make it mandatory.

3. Recommended Change:
 - a. Strike section 999.315(f).
 - b. If this provision remains, there should be alternative options such as allowing the purchaser to deidentify or aggregate the data or continue selling the personal information for purposes exempt under CCPA.

D. ISSUE: VERIFICATION OR AUTHENTICATION OF CONSUMERS SUBMITTING OPT-OUT REQUESTS SHOULD NOT BE PREVENTED OR LIMITED.

1. Proposed Regulation: §999.315(h)
2. Problem with Proposed Regulation:
 - a. The restriction on verifying opt-out requests may be appropriate for advertising or marketing uses, but the CCPA opt-out rights extend to data sales that are actually fraud prevention or identity authentication services that are vital to protect consumers. It puts consumers at risk to limit the ability to “verify” or authenticate such requests because that will allow criminals to opt their planned victims out of data services designed to protect those consumers. For further discussion of this issue, see “GDPArrrr: Using Privacy Laws to Steal Identities,” a study done under the GDPR, warning of identity theft issues for unverified requests for data. <https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf>.
 - b. Not requiring verification means that the wrong consumer could be opted-out.
3. Recommended Change:
 - a. Revise section 999.315(h): “A request to opt-out need not be a verifiable consumer request. If a business, however, cannot verify the identity of a person making a request concerning personal information sold for purposes other than advertising or marketing, has a good faith, reasonable, and documented belief that a request to opt out is fraudulent, the business may deny the request. ~~The business and~~ shall inform the requestor that their identity cannot be verified. ~~requesting party it will not comply with the request and shall provide an explanation of why it believes the request is fraudulent.~~”

E. ISSUE: RESPONSE TO REQUEST TO OPT-OUT ONLY SHOULD APPLY TO BUSINESS THAT SELL PERSONAL INFORMATION AND MORE TIME TO RESPOND IS NECESSARY.

1. Proposed Regulation: §§999.315(d); 999.315(e)
2. Problem with Proposed Regulation:
 - a. Businesses need clarity that this section does not apply if the business does not sell information.
3. Recommended Change:
 - a. Revise section 999.315(d): “In responding to a request to opt-out, a business that sells personal information may present the consumer with the choice to opt-out of sales of certain categories of personal information as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices.”
 - b. Revise section 999.315(e) from 15 to 30 days to act upon a request.

II. SECTION 999.307 NOTICE OF FINANCIAL INCENTIVE—CHAMBER PROPOSED CHANGES

A. ISSUE: DATA DOES NOT HAVE INDEPENDENT VALUE.

1. Proposed Regulation: §999.307; 999.337
2. Problem with Proposed Regulation:
 - a. Data does not have independent, objective value: It is more accurate to think of data as a raw material like flour, where the thing that creates the value in a pastry is the expertise and work of the baker. The perceived value of data is subjective and always in flux.
 - b. Data enables ads-based services to provide the core of the service itself, which is personalized content. The reason certain businesses can offer their services for free isn't that they're being compensated with people's data. It is that they make money by selling ads: these businesses sell advertisers the opportunity to present their messages to people. And advertisers pay the businesses based on objective metrics such as the number of people who see their ads or the number of people who click on their ads.
 - c. However, the free, ad-supported model is also used by newspapers, blogs, professional associations, and services that people find really useful (like online surveys, EventBrite, trip planning apps).
3. Recommended Change:
 - a. Remove any requirements for providing an estimate of the value of consumer data in Section 999.307(b)(5): “[a]n explanation of why the financial incentive or price or service difference is permitted under the CCPA, ~~including: a good faith estimate of the value of the consumer’s data that forms the basis for offering the financial incentive or price or service difference, and a description of the method the business used to calculate the value of the consumer’s data.~~”
 - b. Also strike Section 999.337, which describes the methods in calculating the value of consumer data.

B. ISSUE: REGULATION CREATES ONEROUS DISCLOSURE REQUIREMENTS.

1. Proposed Regulation: §999.307(a); 999.307(a)(3); 999.307(b)(2); 999.307(b)(5)
2. Problem with Proposed Regulation:
 - a. Regulation’s disclosure requirements are onerous.
 - b. Requirement to disclose the value and the methodology goes beyond the statutory language of the CCPA.
3. Recommended Change:
 - a. Reduce the information required to be disclosed.
 - b. Is Section 999.307 intended to only apply (1) where consumers receive a financial incentive or price or service difference in connection with exercise of their rights of access, deletion and opt-out of sale under CCPA or (2) to any financial incentive or price or service difference offered by businesses in connection with simply the collection of personal information? If (1), recommend clarifying regulation Section 999.307 to make clearer that making a financial incentive or offering differing services or prices simply by collecting personal data is not within scope of requiring notice of financial incentive.

when “the archived or backup system is next accessed or used” considering multiple users and departments.

- d. If a consumer submits a CCPA request using the wrong method, a business must either treat it as being correctly submitted and respond or inform the consumer how they can properly submit request, thereby increasing mailing costs. The requirement to confirm receipt of request within 10 days also increases mailing costs.
 - e. Under Sections 999.313(d)(1) and 999.313(d)(6)(a), if a business cannot identify identity for purposes of deletion, how can it effectuate an opt-out? This may be feasible for online identifiers—where you can simply opt out on an identifier basis, rather than delete. But in the non-identifier context this would not be feasible. In addition, this entire requirement runs counter to the verification requirements in the regulations.
 - f. A request to know, under Section 999.301(n), includes any or all of a number of elements. However, in responding to a request to know under Section 999.313(c)(10) the regulations call for all four types of data categories to be displayed.
 - g. Section 999.313(d)(3) permits a business to delay deleting consumer data stored on a back-up or archived system, but only until the archived or backup system is “next accessed or used.” This is vague and ambiguous and ignores the reality of how businesses keep data. If a business accesses a backup system for security or integrity-verification purposes, for example, does that count as accessing consumer data that might be stored in another database on the backup system such that the consumer data then has to be retrieved and deleted even if no longer accessed or used?
 - h. Unless and until a company can extract personal information of restored data on a back-up drive on a per individual basis, the company should be allowed to develop systems and safeguards to ensure that any such personal information is not restored into active systems where it could be accessed or used in any manner.
 - i. Compliance in the context of these technical limitations would necessarily require the destruction of data critical to the fundamental purpose of the backup system, i.e. business continuity. This is especially concerning in a time of climatological change in California where increased threats of fire, cyclones, and earthquakes are already testing and compromising business operations and systems integrity. The need for increased vigilance and protection for backup systems, data, and controls should be recognized or at least, evaluated in this context.
 - j. Unverifiable requests pose additional security risks. For further discussion, see “GDPArrrr: Using Privacy Laws to Steal Identities,” a study done under the GDPR, warning of identity theft issues for unverified requests for data. <https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf>.
3. Recommended Change:
- a. Priority recommendation would be to strike this provision entirely noting there are separate requests for separate reasons.
 - b. An alternative recommendation would be instead to focus on a process for making an unverifiable request to delete become a verified request to delete.
 - c. Revise Section 999.313(d)(3): “If a business stores any personal information on archived or backup systems, it may delay compliance with the consumer’s request to delete, with respect to data stored on the archived or backup system, until the data on the archived or backup system is next accessed or used.”
 - d. Change “and” to “or, as requested by the consumer” in Section 999.313(c)(10).

B. ISSUE: ENSURE BUSINESSES HAVE ENOUGH TIME AND FLEXIBILITY TO RESPOND TO REQUESTS UNDER STATUTORY TIMEFRAME.

1. Proposed Regulation: §999.313(a); 999.313(b)
2. Problem with Proposed Regulation:
 - a. The 45-day period for responding to consumer requests should begin to run once the request has been verified (§ 999.313(b)). The proposed regulations recognize businesses' responsibility to verify requests properly, a task that may take days or weeks to complete and is reliant upon a consumer's collaboration in providing accurate information in a timely manner. After a request is verified, a company must then find the information that it holds on a consumer—information which may be kept in separate databases—and convert it into a form which can be delivered to the consumer. If receipt of the request initiates the 45-day period, businesses will be incentivized to rush through one of these processes, which does not serve the consumer.
 - b. The proposal specifically states that the 45-day time limit applies, “regardless of time required to verify the request.” This could lead to a situation where a business is out of compliance because a consumer has failed to respond to a verification request. It should be revised to delete the time a consumer takes to respond.
3. Recommended Change:
 - a. It is likely that in the months after the CCPA takes effect, businesses will receive a flood of consumer requests. The AG should incentivize businesses to handle these requests responsibly and efficiently.
 - b. Revise Section 999.313(a): “Upon receiving a request to know or a request to delete, a business shall confirm receipt of the request, through either mail, email, or another notification method, within 10 days and provide information about how the business will process the request. The information provided shall describe the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request.”
 - c. Revise Section 999.313(b): “Businesses shall respond to complete requests to know and requests to delete within 45 days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request unless the request is incomplete, or, unless the request is incomplete, or the consumer fails to provide information necessary to verify the request. If necessary, businesses may take up to an additional 45 days to respond to the consumer's request, for a maximum total of 90 days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.”
 - d. Businesses should have option for confirmation of request using the same method as the request was submitted, unless the consumer clearly indicates an alternative means of communication in the initial request.

C. ISSUE: PROPOSED REGULATION REQUIREMENTS HEIGHTEN BURDENS ON BUSINESS AND EXCEED STATUTORY LANGUAGE.

1. Proposed Regulation: §999.313
2. Problem with Proposed Regulation:
 - a. Section 999.313(a)-(c) creates substantial additional burdens on top of already-burdensome “right to know” requirements included in CCPA and GDPR, by requiring companies to produce a second set of responses in addition to the specific pieces of information retained about the customer—namely, customized metadata regarding the

information collected for each customer, categorized in a complicated manner outlined by the statute.

- b. Clarify that businesses do not need to provide categories of personal information if already providing specific information; remove requirements to provide information about each category of personal information; confirm that language used in statute is sufficiently meaningful for consumers; permit generic disclosures in the privacy notice in cases where response is accurate for most or substantially all consumers.
 - c. The draft regulations suggest that businesses must provide the categories of sources of information, uses of information, categories of third parties to which information is disclosed or sold, and the purposes of such disclosures or sales for each category of personal information that it collects. These requirements require disclosures beyond what the statute requires, as the statute does not require such disclosure for each category of information.
3. Recommended Change:
- a. Align language with statute.
 - b. A revision to Section 999.313(c)(9) expanding the circumstances in which a company could rely on a generic articulation of categories in the Privacy Notice, as opposed to a customer-specific feed. For example, the regulation could be broadened to clarify that we may refer to our privacy policy when our response would be the same for “substantially all” or “most” consumers.
 - c. A revision to Section 999.313(c)(10) that would not require the additional pieces of information listed there (categories of sources, business purpose, categories of parties to whom disclosed/sold and why) to be broken out for *each category of information collected*.
 - d. A revision to Section 999.313(c)(11) clarifying that use of the language specifically enumerated in either the statute or the regulation “provides consumers a meaningful understanding of the categories listed.”
 - e. A revision to Section 999.313(c) to add new Section 999.312(c)(12) that would clarify that a company need not *additionally* fulfill a request to provide *categories* of information collected if it is *also* providing specific pieces of information. (Perhaps this could be time-bound to make it more palatable?).
 - f. A revision to Section 999.313(c) to add new Section 999.312(c)(13) that would clarify a business shall identify the personal information responsive to a request to know by conducting a commercially reasonable search of its records.

D. ISSUE: REGULATION SHOULD CLARIFY THAT A BUSINESS’S OBLIGATION TO COMPLY WITH A CONSUMER REQUEST IS LIMITED TO ITS ABILITY TO IDENTIFY RESPONSIVE MATERIALS USING COMMERCIALY REASONABLE EFFORTS.

- 1. Proposed Regulation: §999.313(c); 999.313(d)
- 2. Problem with Proposed Regulation:
 - a. Regulation should address the level of diligence a business must use when complying with consumer requests to know or delete. The regulation does not address whether a business that engages in a good-faith, commercially reasonable and diligent search of its records, could be found non-compliant in the event it fails to identify a record containing personal information pertaining to a request. Without a specified standard, a business could spare no expense to comply, engaging an army of people to scour every record that the business holds manually for potential matches. Such a process would not be commercially reasonable or worthwhile to California consumers, as it would force

businesses to raise prices to cover the costs of searching. Analogous frameworks in which large volumes of information are requested from businesses with widespread records provide standards. For example, both the California and Federal Rules of Civil Procedure allow parties to consider the burden and expense associated with discovery requests.

3. Recommended Change:

- a. Add language, consistent with the statute (1798.145), to new subsections 999.313(c)(13) and 999.313(d)(8): “A business shall identify the personal information responsive to a request by conducting a commercially reasonable search of its records for documents that are responsive, considering the sensitivity of the personal information the business holds and the expense of compliance. A business does not violate the CCPA when, it conducts a commercially reasonable search of its records in good faith but fails to identify a responsive record.”

E. ISSUE: REGULATION SHOULD CONSIDER HOW RESPONDING TO REQUESTS COULD JEOPARDIZE OTHER CUSTOMERS’ SECURITY AS WELL.

1. Proposed Regulation: §999.313(c)(3); *see also* 999.313(d), 999.323

2. Problem with Proposed Regulation:

- a. Regulation should reference security risks to personal information of other consumers as well. Businesses are concerned that the CCPA’s requirement to provide certain specific pieces of personal information to consumers will create a risk of identity theft by malefactors. The prohibition on disclosing sensitive personal data elements to consumers represents good security practice. Additionally, the balancing tests laid out in the proposed regulations are helpful clarifications that businesses must weigh the benefit to the consumer of receiving specific pieces of personal information with the risk of facilitating improper disclosure of such information.
- b. We welcome the fact that de-identification of personal information serves as an acceptable method of deletion. This provisions similarly strikes the proper balance between consumers’ rights and the interests of businesses and the public in analyzing data that presents little risk to consumer privacy.

3. Recommended Change:

- a. Revise Section 999.313(c)(3) language to: “substantial, articulable, and unreasonable risk to the security of that personal information, the consumer’s or another consumer’s account with the business, or the security of the business’s systems or networks.”

F. ISSUE: REGULATION DOES NOT ADDRESS REQUESTS SEEKING PORTABILITY OF INFORMATION WHERE DISCLOSURE OF CONSUMER’S PERSONAL INFORMATION IS NECESSARY TO SUPPORT PORTABILITY.

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

2. Problem with Proposed Regulation:

- a. The language does not address requests seeking portability of information where such identifiers enumerated in Section 999.313(c)(4) are necessary to support portability.

3. Recommended Change:

- a. Revise Section 999.313(c)(4): “A business shall not at any time disclose a consumer’s Social Security number, driver’s license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers. This

subsection does not apply to requests seeking portability of information where such identifiers enumerated in Section 999.313(c)(4) are necessary to support portability.

G. ISSUE: NOTIFYING CONSUMER OF REASON FOR REQUEST DENIAL MAY INTERFERE WITH LAW ENFORCEMENT INVESTIGATION, HINDER BUSINESS OPERATIONS, AND IS CONTRARY TO THE PURPOSE OF AN EXEMPTION.

1. Proposed Regulation: §999.313(c)(5)
2. Problem with Proposed Regulation:
 - a. Section 999.313(c)(5) requires that if an access request is denied because of federal or state law, or because of an exception to the CCPA, the consumer must be notified of the reason why. Under certain circumstances, this could interfere with an active law enforcement investigation, or it could result in the disclosure of information that may interfere with a business's operations or the rights of others.
 - b. Under Section 999.313(c)(5), if a business denies a consumer's verified request to know specific pieces of personal information because of an exemption to the CCPA, the business must inform the requestor of the basis for the denial. This section would require a business to inform a consumer that it holds data subject to an exemption under the CCPA and undermines the purpose of an exemption from the obligations under the law. By providing data exemptions under the CCPA, the provision could require new tracking mechanisms to understand if an organization has exempted data about a consumer that could be included in disclosures.
3. Recommended Change:
 - a. Limit the disclosure regarding request denial.
 - b. Modify language so that if a company includes the CCPA exemptions in their privacy policy, they can just point consumers to those exemptions on their privacy policy and note that they are not responding because of an exemption listed in the privacy policy per the CCPA.
 - c. Revise Section 999.313(c)(5): "If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception pursuant to the CCPA, the business shall inform the requestor and explain the basis for its denial, provided however that a business shall be deemed to be in compliance with the requirement if bases for denial are set forth in its privacy policy and the business refers the consumer to its privacy policy. If the request is denied only in part, the business shall disclose the other information sought by the consumer."

H. ISSUE: INDIVIDUALIZED RESPONSES TO CATEGORIES OF SOURCES OR THIRD PARTIES IS TOO BURDENSOME FOR BUSINESSES.

1. Proposed Regulation: §999.313(c)(9)-(10)
2. Problem with Proposed Regulation:
 - a. Sections 999.313(c)(9)-(10) require a business to provide an "individualized response" as to categories of personal information, sources, and third parties to whom data is sold, rather than reporting the business's general business practices and categories. This will require businesses to provide for each category of information applicable to a consumer: (a) The categories of sources from which the personal information was collected; (b) The business or commercial purpose for which it collected the personal information; (c) The categories of third parties to whom the business sold or disclosed the category of personal information for a business purpose; and (d) The business or commercial purpose for which it sold or disclosed the category of personal information. Companies do not track

personal information elements in this manner and this requirement will burden companies significantly to comply with new requirements that at best will provide consumers with marginal incremental general information about their personal information and its use.

3. Recommended Change:
 - a. Remove language in Sections 999.313(c)(9)-(10) that require detailed disclosures for each category of personal information.
 - b. Remove the requirement that disclosures include reference to all elements of Section 999.313(c)(10), as the CCPA via sections 1798.100; 1798.110; and 1798.115, permit consumers to request to know about different types of practices in differing level of detail.

IV. SECTION 999.314 SERVICE PROVIDERS—CHAMBER PROPOSED CHANGES

A. ISSUE: PROPOSED REGULATIONS' LIMITATIONS ON SERVICE PROVIDERS' PERMISSIBLE USES OF DATA CONTRADICTS THE STATUTORY DEFINITION OF "BUSINESS PURPOSE" AND "SERVICE PROVIDER."

1. Proposed Regulation: §999.314(c)
2. Problems with Proposed Regulation:
 - a. Because the service provider's business purposes may include using personal information for the benefit of one business in a way that might also benefit other businesses, the CCPA statute is best interpreted to permit the service provider to use the personal information that it receives for business purposes that might provide a benefit to other of its business partners, as long as such use is permitted under the written agreement between the business and the service provider and otherwise consistent with the CCPA. In many circumstances, this information would be considered aggregate insights or information that is not personally identifiable, but here, as in other sections, the overly broad definition of personal information threatens an ordinary business practice that presents little risk to consumers.
 - b. Section 999.314(c) would severely limit the ability of service providers to improve and build services that can be used to process personal information. In many cases, service providers that process personal information may make improvements to their services in connection with the personal information in a way that does not identify, target, or otherwise impact any consumer or household—for example, an improvement in handling technical aspects of data. The language would restrict this kind of improvement as it could be interpreted to not allow improvements to be used for any other customer, thus limiting service innovation or improvement by service providers. Service providers that have permission from an entity to use provided information to improve their services should be able to do so as long as the improvement and use does not result in the disclosure of that information to a third party. The text of the statute explicitly permits disclosures to "service providers" for a broad list of enumerated "business purposes" defined under the statute. Importantly, the statute defines "business purpose" to include both a business's *or a service provider's* operational purposes or other notified purposes. The statutory text also permits a service provider to use the personal information it receives from one business for such business purposes of both that business and the service provider where the use is authorized as part of the contracted-for "services" provided to the business or as otherwise permitted by the Act.
 - c. The plain text of the section appears to prohibit service providers from using the personal information they receive from one entity to provide services to another person or entity, unless such services are necessary for detecting security incidents or preventing fraud or other illegal activity. The draft regulations improperly focus solely on the business purpose of the business and ignore the fact that the statutory definition of "business purpose" also includes the use of personal information for the "service provider's operational purposes or other notified purposes."

- d. The activities included in the list of business purposes (such as “performing services on behalf of the business or service provider, including providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider”) require the combination and use of personal information received from and for the benefit of multiple businesses.
 - e. As such, focusing solely on the business purposes of the business, as the proposed regulations do, would both render the bolded language surplusage, contrary to well-established canons of statutory interpretation, as well as potentially render impermissible a number of the activities explicitly included on the list of permissible business purposes.
 - f. Combining the data with other personal information to further the purposes of the services being provided should be permitted, especially when the services are to further deidentify or aggregate the personal information. Combining personal information from multiple businesses as a service provider for each business for purposes of aggregating the data should not be considered a “sale.”
 - g. The language in Section 999.314(c) is written very broadly and could be interpreted to not allow certain internal operations for the service provider that might require the combining of data, including improving the quality of the service providers services that it provides for businesses generally. To that end, the text should be modified as indicated.
3. Recommended Change:
- a. Modify language:
 - “(c) A service provider shall not use personal information received either from a person or entity it services or from a consumer’s direct interaction with the service provider, without the agreement of such person, entity, or consumer, for the purpose of providing services that result in the sale of a consumer’s personal information to a third party to another person or entity. A service provider may, however, combine personal information received from one or more entities to which it is a service provider, ~~on behalf of such businesses in order to provide the services specified in a contract with a business, or~~ to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.”
 - b. Revise use limitations to (1) permit service providers to use personal information for the benefit of all customers with the permission of the person, entity, or consumer from whom the service provider received the personal information; or (2) reduce the limitation to apply only to providing services that result in the disclosure of a consumer’s personal information to a third party.

B. ISSUE: PROPOSED REGULATION CREATES ADDITIONAL BURDENS FOR BUSINESS THAT EXCEED STATUTORY LANGUAGE.

- 1. Proposed Regulation: §999.314(d)
- 2. Problem with Proposed Regulation:
 - a. This is difficult to manage since many businesses act as a service provider, while also collecting additional personal information for their own business purposes (as is noted above in Section 999.314(c)). If a business receives a “request to know” from a consumer, the business should be able to focus only on the personal information collected by that business and not the personal information it is maintaining for a different business when acting as a service provider. In addition, many service provider relationships are confidential and proprietary to the business engaging the service provider. Disclosing the name of the business engaging the service provider could violate those restrictions while also sharing competitive information publicly.

- b. Section 999.314(d) requires that a service provider that receives but “does not comply” with a consumer’s request to know or delete must inform the consumer of the reason for the denial, explain that the consumer should submit the request directly to the business, and, when feasible, provide the contact information for the business. This requirement creates new obligations for service providers beyond the statutory text because service providers do not have an obligation to comply with such deletion requests.
- 3. Recommended Change:
 - a. Revise Section 999.314(d): “If a service provider receives a request to know or a request to delete from a consumer regarding personal information that the service provider collects, maintains, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial. ~~If a service provider receives a request to know or a request to delete from a consumer regarding personal information that the service provider collects, maintains, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial.~~”

V. SECTION 999.301 DEFINITIONS—CHAMBER PROPOSED CHANGES

A. ISSUE: DEFINITION OF RIGHT TO KNOW CONFLICTS WITH REQUIREMENTS FOR HOW TO RESPOND TO RIGHT TO KNOW.

- 1. Proposed Regulation: §§999.301(n); 999.313(c)(10)
- 2. Problem with Proposed Regulation:
 - a. The definition of right to know under Section 999.301(n) says a consumer has a right to “any or all” of the following categories of personal information. However, Section 999.313(c)(10), instructing businesses how to respond to requests to know, uses the conjunctive “and”—not “and/or”—for the categories of information a business must disclose in response to a consumer request. Thus, under Section 999.313, a business is required to disclose all enumerated categories, even if consumer only makes a limited request.
- 3. Recommended Change:
 - a. Correct the wording in Section 999.313(c)(10) to say “and/or as requested by the consumer.”

B. ISSUE: DEFINITION OF RIGHT TO KNOW CREATES INFEASIBLE REQUIREMENTS FOR RESPONDING TO INDIVIDUAL CONSUMER REQUESTS.

- 1. Proposed Regulation: §999.301(n).
- 2. Problem with Proposed Regulation:
 - a. This definition is perceived as the most concerning. It lumps one request into different categories, sources, and a variety of different requests. It would be preferred if each subsection (1) through (6) were separately defined. Subsections (2) through (6) should be addressed through a notice so it is standardized across the board for all consumers. It is not feasible or scalable to provide the customized set of categories to each individual consumer.
- 3. Recommended Change:
 - a. The “Request to know” should be linked only to subsection (1).

- C. THE SCOPE OF THE DEFINITION OF “PRICE OR SERVICE DIFFERENCE” COULD PREVENT BUSINESS WITH SERVICE PROVIDERS.
1. Proposed Regulation: §999.301(1)
 2. Problem with Proposed Regulation:
 - a. Regarding the definition of “Price or service difference,” there is a concern that if a broker or provider (as a business partner) opts-out of the sale of personal information, this could unknowingly to the business partners) serve to prevent their continued business with a business.
 3. Recommended Change:
 - a. Revise Section 999.301(1) to include language that “If an individual working for a broker or provider as a business partner opts-out of the sale of personal information this will not prevent the continued relationship with a business.”
- D. ISSUE: DEFINITION OF “AFFIRMATIVE AUTHORIZATION” REQUIREMENT FOR TWO-STEP PROCESS TO OPT-IN IS OVERLY BURDENSOME FOR CONSUMERS AND BUSINESS.
1. Proposed Regulation: §999.301(a)
 2. Problem with Proposed Regulation:
 - a. For consumers 13 years and older, Section 999.301(a) mandates a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in. Mandating a two-step process can be cumbersome and disruptive for consumers and overly prescriptive for businesses. It can prevent businesses from developing innovative consent flows based on extensive UX/UI research.
 3. Recommended Change:
 - a. Strike the language in section 999.301(a) mandating a two-step process.
- E. ISSUE: PROPOSED REGULATIONS NEED TO PROVIDE CLARIFICATION REGARDING DEFINITION OF DIRECT NOTICE TO CONSUMERS.
1. Proposed Regulation: §999.301; *see also* §§999.305(a)(3), 999.305(d)(1), 999.306(d)(2)
 2. Problem with Proposed Regulation:
 - a. There is a lack of clarity as to direct notification under the regulations. Providing a definition of “directly notify” would provide certainty as well as coordination across all the rules that require some sort of direct notice to consumers.
 3. Recommended Change:
 - a. Add a new subsection 999.301(g): “Directly Notify” means contacting the consumer directly with the required information, provided, however, that a business will have been deemed to directly notify a consumer of changes to its policies and practices if the notification is published and made available on its website for a sufficient period of time or other standard method of providing privacy policies and notices to consumers.”

VI. SECTION 999.300 TITLE AND SCOPE—CHAMBER PROPOSED CHANGES

A. ISSUE: THE REGULATIONS SHOULD CLARIFY THE CCPA’S JURISDICTIONAL SCOPE AND EFFECTIVE DATE.

1. Proposed Regulation: §999.300
2. Problem with Proposed Regulation:
 - a. The CCPA’s broad definition of business suggests that a non-U.S. business that incidentally collects the personal information of a single California resident should comply with all of its requirements. This could sweep in a large number of entities over whom California would not normally have jurisdiction.
 - b. The effective date of enforcement should be delayed until January 1, 2021 to allow companies time to comply with the regulations.
 - c. The regulations should clarify and make specific the Health Insurance Portability and Accountability Act (HIPPA) and Confidentiality of Medical Information Act (CMIA) exemption language in Section 1798.145(c)(1)(B) of the CCPA.
3. Recommended Change:
 - a. The regulations should clarify that a business whose operations are outside of California and who only collect a *de minimus* amount of personal information from California residents—such as bbc.co.uk or lajornada.com.mx—are not required to comply with CCPA. Alternatively, the regulations might state that businesses that operate outside of California and do not target their services to California residents are not covered.
 - b. Revise section 999.300 to include the following: “The title shall not apply to a provider of health care governed by CMIA or HIPAA, to the extent the provider or covered entity collects personal information in connection with the provision or sale of health care-related products or services, and to the extent that the provider or covered entity maintains that personal information in a way that meets HIPAA Security Rule requirements.”

VII. SECTION 999.305 NOTICE AT COLLECTION OF PERSONAL INFORMATION—CHAMBER PROPOSED CHANGES

A. ISSUE: PROPOSED REGULATION REQUIREMENTS FOR EACH CATEGORY OF PERSONAL INFORMATION EXCEED STATUTORY REQUIREMENTS.

1. Proposed Regulation: §999.305; 999.305(d)(2)(b)
2. Problem with Proposed Regulation:
 - a. Section 999.305 mandates that the notice at collection includes requirements that go beyond the statute, which only requires that businesses describe the categories of personal information collected and the purpose for which such information is used for employee data.
 - b. The proposed regulations do not seem to distinguish between the notice to employees and the notice to customers. Each notice would address different types of data. Also, the proposed regulation’s notice requirement to include a link to the business’s privacy policy creates confusion whether a business needs two privacy policies, one for employee data and one for customer data.

3. Recommended Change:
 - a. We first recommend deletion of Section 999.305(d)(2)(b). In the alternative, the regulations should clarify that a business that receives personal information from an indirect source may comply with its CCPA obligations through contractual provisions that require other businesses to provide the requisite notice to consumers. The requirements to contact the source and obtain signed attestations are confusing and duplicative.
 - b. The AG should provide a different set of regulations to apply to the employee notice separate from the customer notice.

B. ISSUE: PROPOSED REGULATION’S REQUIREMENT FOR EXPLICIT CONSENT EXCEEDS STATUTORY REQUIREMENTS.

1. Proposed Regulation: §999.305(a)(3)
2. Problem with Proposed Regulation:
 - a. Section 999.305(a)(3) requires businesses to obtain explicit consent from consumers to use personal information for a purpose not disclosed at the time of collection. Explicit consent is such a high bar that is likely to make it either infeasible to use previously collected information for a purpose not previously disclosed or incentivize broad disclosures that may cut against data minimization principles.
 - b. This new purpose limitation requiring obtaining explicit consent from the consumer to use personal information for a new purpose also exceeds the scope of the CCPA’s statutory language, which only requires notice of new purposes. *See* 1798.100(b).
 - c. There should be a way of expanding usage and ability to sell personal information without having to directly notify consumers and obtain explicit consent (e.g. data uses within the same category of business or which align with the consumer’s expectations when the data was collected).
3. Recommended Change:
 - a. Revise Section 999.305(a)(3) to permit businesses to use personal information for a purpose not disclosed at the time of collection upon notice to the consumer. The change would be consistent with Section 178.100(b), which requires only notice consistent with the Section, not explicit consent as contemplated by the regulations.
 - b. Revise Section 999.305(a)(3): “A business shall not use a consumer’s personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer’s personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall notify the consumer of this new use ~~and obtain explicit consent from the consumer to use it for this new purpose.~~”

C. ISSUE: NOTICE AT COLLECTION IS IMPRACTICAL UNDER CERTAIN CIRCUMSTANCES AND EXCEEDS THE STATUTORY PURPOSE.

1. Proposed Regulation: §999.305(a)(2); 999.305(c)
2. Problem with Proposed Regulation:
 - a. Section 999.305(a)(2)(e) requires businesses to provide notice of collection of personal information before any information is collected. This approach is not practical for online environments, where information such as IP addresses is collected automatically.

- b. Also need clarity whether, under section 999.305(c), cookie data collection requires a pop-up for the Notice at Collection.
 - 3. Recommended Change:
 - a. Revise Section 999.305(a)(2) to require notice at or before the time of collection, rather than before collection. The change would be consistent with Section 1798.100(b), which requires notice at or before the point of collection.
- D. ISSUE: ACCESSIBILITY FOR CONSUMERS WITH DISABILITIES SHOULD BE CLARIFIED TO BE WHEN REQUIRED BY THE AMERICANS WITH DISABILITIES ACT OF 1990.
- 1. Proposed Regulation: §999.305(a)(2)(d); *see also* §§999.306(a)(2)(d); 999.307(a)(2)(d); 999.308(a)(2)(d)
 - 2. Problem with Proposed Regulation:
 - a. The ambiguity created by this proposal is that the Americans with Disabilities Act of 1990 (ADA) currently does not apply to marketing-only websites. Does this proposed regulation extend the breadth of the ADA to marketing-only websites that do not offer sales/service such that *all* websites operated by entities within the scope of the CCPA have to also be ADA compliant?
 - 3. Recommended Change:
 - a. Revise Sections 999.305(a)(2)(d); 999.306(a)(2)(d); 999.307(a)(2)(d); 999.308(a)(2)(d): “Be accessible to consumers with disabilities when required by the Americans with Disabilities Act of 1990, Pub. L. No. 101-336, 104 Stat. 328 (1990). ~~At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.”~~
- E. ISSUE: REGULATION DOES NOT ACCOUNT FOR SCENARIO WHERE BUSINESS RECEIVES PERSONAL INFORMATION ABOUT A CONSUMER FROM ANOTHER BUSINESS AND THEN CREATES ITS OWN DIRECT RELATIONSHIP WITH THE CONSUMER.
- 1. Proposed Regulation: §999.305
 - 2. Problem with Proposed Regulation:
 - a. The regulations cover how a business that collects information *directly* from consumers provides notice and how a business that *does not collect information directly from consumers* is to comply with the notice requirement. The regulations do not provide clarity as to the middle ground between those two scenarios— i.e. a business that receives information about a consumer from another business and then creates its own direct relationship with the consumer. In that scenario, it is impossible to provide notice before the initial “collection” of information from the other business, but it is possible to provide notice before the business begins to collect information *directly* from the consumer as part of the consumer’s direct, intentional, interaction with the business.
 - b. We suggest that the regulations be revised to provide clarity that a business that receives consumer information from another business may comply with the notice requirement by providing a notice at or before additional information is collected *directly* from the consumer.
 - 3. Recommend Change:
 - a. If feasible, providing notice within a reasonable time frame upon receiving the information, and *no later than at the time of directly collecting additional information from the consumer.*

VIII. SECTION 999.306 NOTICE OF RIGHT TO OPT-OUT OF SALE OF PERSONAL INFORMATION—CHAMBER PROPOSED CHANGES

A. ISSUE: PROPOSED REGULATION EXCEEDS STATUTORY LANGUAGE, LIMITING BUSINESS ABILITY TO OPERATE, AND CREATES UNTENABLE COMPLIANCE OBLIGATIONS.

1. Proposed Regulation: §999.306; 999.306(a)(1)
2. Problem with Proposed Regulation:
 - a. The CCPA does not govern a business’s future potential to sell personal information, but instead governs the practices of businesses that sell personal information at the time of processing the personal information. The proposed regulation references not only businesses that actually sell personal information, but also businesses that may in the future, exceeding the current statutory language.
 - b. This requirement means that if a business did not sell personal information, and then did not have a “Do Not Sell” button, if it then chooses to sell and has a button, then personal information collected about consumers during the time the button was not shown will automatically be subject to the opt-out. Accordingly, businesses will then have the option to request that consumers authorize the sale pursuant to Section 1798.135. First, this is counter to the text of the CCPA, which allows for new uses of data pursuant to notice (whereas explicit consent is required under the draft regulations, and we have already pointed out that this is in contravention to the statute). In addition, there is lack of clarity as to when businesses will be able to seek authorization from these consumers who will have been “deemed” to have opted-out.
3. Recommended Change:
 - a. Remove “future sell” language from Section 999.306(a)(1).

B. ISSUE: REGULATION IMPROPERLY FORCES BUSINESS TO MAKE FUTURE REPRESENTATIONS TO CUSTOMERS.

1. Proposed Regulation: §§999.306(d)(1); 999.306(d)(2)
2. Problem with Proposed Regulation:
 - a. The proposed rules also state that businesses are exempt from providing a notice of right to opt-out if does not sell “and will not” sell personal information and if it states in its privacy policy that it does not and “will not” sell not personal information. Mandating that businesses make future representations like this unnecessarily restricts businesses from evolving their business models and roadmaps. And in the event that a business in good faith makes a representation that it will not sell information and at a later time decides to sell personal information with adequate notice to consumers, the business now risks that it has made an unfair and deceptive claim to consumers by previously representing that it will not sell personal information.
3. Recommended Change
 - a. Remove “will not” sell language from Sections 999.306(d)(1) and 999.306(d)(2).

C. ISSUE: REGULATION COMPLICATES OPT-OUT NOTICE AND CREATES UNNECESSARY BURDEN FOR BUSINESS

1. Proposed Regulation: §999.306(d)
2. Problem with Proposed Regulation:

- a. First, the proposed rule conflates general personal information collection (not selling) with the right to opt-out of the selling of personal information. A business that does not post an opt-out notice because it does not sell personal information shouldn't be deemed to have received an opt-out because there is nothing from which the consumer can opt-out (the business doesn't sell information).
 - b. Second, the CCPA explicitly references that a business shall be prohibited from selling a consumer's information after receiving "direction from a consumer not to sell the consumer's personal information" 1708.120(d). The draft regulation has replaced this "direction" requirement, which requires an explicit action through the opt-out button, with a "default" opt-out.
 - c. Third, pursuant to the draft regulations, businesses are required to keep a record of the opt-outs they receive. For businesses who don't sell personal information but to whom consumers can be deemed to have submitted the default opt-out mentioned above, this creates an unnecessary compliance burden.
 - d. Also, if a business receives "default" opt-outs at a time where it didn't sell information but decides to sell information within 12 months, the business will be preemptively prohibited from selling information for 12 months even though the business has not received explicit "direction from a consumer not to sell the consumer's personal information," as required by the CCPA.
 - e. Section 999.306(d)(2) may not be operable for businesses.
3. Recommended Change:
- a. Allow businesses to instead publish a change in policy for a sufficient period of time to give consumers the right to opt out.
 - b. Revise Section 999.306(d)(2): ~~"It states in its privacy policy that that it does not and will not sell personal information. A consumer whose personal information is collected while a notice of right to opt-out notice is not posted shall be deemed to have validly submitted a request to opt-out."~~

IX. SECTION 999.312 METHODS FOR SUBMITTING REQUESTS TO KNOW AND REQUESTS TO DELETE—CHAMBER PROPOSED CHANGES

A. ISSUE: MANDATING A THIRD METHOD FOR SUBMITTING REQUESTS IS UNNECESSARY, POSES SECURITY RISKS, AND CREATES CONFUSION.

- 1. Proposed Regulation: §999.312
- 2. Problem with Proposed Regulation:
 - a. The proposed regulations in Sections 999.312(a) and (b) require that businesses provide two or more designated methods for submitting requests to know and requests to delete. However, Section 999.312(c) increases the burden on certain businesses beyond the statutory requirements from a minimum of two to a minimum of three methods to submit a request.
 - b. The requirement in Section 999.312(c) that submissions be accepted at physical locations is not contemplated by statute, is not considered sound security practice, and imposes disproportionate obligations on brick and mortar stores. Using paper forms increases risks to security and privacy because they can be misplaced or mishandled even if a company has certain protocols in place, especially given the high turnover of employees in retail.
 - c. For companies with multiple physical locations, providing a toll-free number along with an online portal provide effective and consumer friendly methods for consumers to

submit requests. Mandating a *third* method for certain businesses with physical locations creates confusion and uncertainty depending on how the term “primarily interacts” is construed. We suggest that businesses who elect to provide *both* a toll-free number and online portal are providing consumers with ample opportunity to submit requests and therefore should not be required to provide another option that is unlikely to provide any additional consumer benefit.

- d. This section needs to be revised to allow for businesses that interact with consumers online only to not have the toll-free number requirement, but rather an email requirement per AB 1564.
3. Recommended Change:
- a. Modify the language in Section 999.312(c)(2) so that a business operating a website, but primarily interacting with customers in person, shall offer two—not three—methods: a toll-free telephone number, and an interactive webform, or a form that can be submitted in person.
 - b. Modify the language so that a business providing both a toll-free number and online portal for customers to submit requests would be sufficient.
 - Add new subsection 999.312(c)(3): “Example 3: If the business operates a website and interacts with customers in person at a retail location, but primarily collects data online (such as a travel company website), the business can offer two methods to submit requests to know—a toll-free telephone number and an interactive webform accessible through the business’s website. In this case, a form that can be submitted in person at the retail location is not necessary.”
 - c. Modify the language so that businesses that interact with consumers online only to not have the toll-free number requirement, but rather only an email requirement per AB 1564.
 - Delete existing subsection 999.312(f) and add new 312(f) to include: “A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.”

B. ISSUE: REGULATIONS REQUIRE SAME RESPONSE REQUIREMENTS REGARDLESS OF WHAT METHOD WAS USED TO SUBMIT THE REQUEST.

1. Proposed Regulation: §999.312(e); 999.313(f)
2. Problem with Proposed Regulation:
 - a. It is unclear how this section interacts with Section 999.313, which requires a business to confirm receipt of a request within 10 days of the date received and to respond within 45 days (regardless of how long verification takes).
 - b. Potentially broadens training requirements for personnel who handle consumer requests, since personnel may have to be trained to forward requests internally.
 - c. CCPA only requires that a business designate two or more methods for such requests to be submitted and this proposed language defeats the purpose of a business designating a method if consumers can still submit requests not using a designated method of submission (i.e. to be able to staff with trained personnel and meet statutory deadlines).
 - d. This timeline is challenging. Additional time akin to 45 days would be reasonable in light of the steps a business will need to take to coordinate. Especially where vendors are

involved in supporting the process, things like monthly data feeds could be affected. Also, the 15 versus 90 days as noted in Section 999.312(f) below are not congruent.

3. Recommended Change:
 - a. Strike existing section 999.312(f).

C. ISSUE: MANDATING A TWO-STEP PROCESS DISEMPOWERS THE CONSUMER.

1. Proposed Regulation: §999.312(d)
2. Problem with Proposed Regulation:
 - a. Mandating a two-step process actually disempowers the consumer as many companies may operate a “self-serve” type process where consumers can make their choices as to information to be deleted. Requiring this two-step process could frustrate consumers. Companies should have the flexibility on process flow; in some cases it may make sense to have a two-step process, in other cases it may not.
3. Recommended Change:
 - a. Modify section 999.312(d): “A business ~~shall~~ may use a two-step process for online requests to delete where the consumer must first, clearly submit the request to delete and then second, separately confirm that they want their personal information deleted.”

X. SECTION 999.317 TRAINING; RECORD-KEEPING–CHAMBER PROPOSED CHANGES

A. ISSUE: RECORD-KEEPING REQUIREMENT DOES NOT ALIGN WITH PURPOSES OF CCPA.

1. Proposed Regulation: §999.317(g)
2. Problem with Proposed Regulation:
 - a. The CCPA does not impose the record-keeping requirements mentioned in this section.
 - b. It imposes an additional burden on businesses, does not appear tied to consumer benefits or rights, and it requires the collection of more personal information, thereby contravening the spirit of the CCPA. Imposing additional record-keeping and disclosure requirements on businesses that handle the personal information of four million or more consumers appears arbitrary. The CCPA already requires that businesses provide multiple disclosures to consumers, and this information is unlikely to give them a more meaningful understanding of their privacy protections.
 - c. Also, it is very unclear what would constitute a request that is “complied with” or “denied.” If a consumer could not be verified, how would that be characterized? What if the request was subject to a statutory exception? The lack of specificity will make this extremely challenging.
 - d. The release of metrics in the business’s privacy policy does not benefit consumers nor do the regulations provide any guidance relating to the calculation of the four million or more consumers.
3. Recommended Change:
 - a. The record-keeping requirements in section 999.317(g) should be struck.
 - b. Alternatively, if the effective date of the regulation is after January 1, 2020, revise the regulation to require recordkeeping information only after the date the regulations become effective. This requirement does not appear to be reflected in the statute, and it’s

unreasonable to require companies to begin collecting this information on January 1, 2020 if the regulations have not been finalized.

- c. Also, as an alternative to including the information in the privacy policy, these metrics should instead be provided to the AG upon request.
- d. If section 999.317(g) is kept, revise “median” to “average” because median is a difficult number to calculate.

XI. SECTION 999.316 REQUESTS TO OPT-IN AFTER OPTING OUT OF THE SALE OF PERSONAL INFORMATION—CHAMBER PROPOSED CHANGES

A. ISSUE: REGULATION’S TWO-STEP PROCESS CREATES UNNECESSARY FRICTION AND CONSUMER CONFUSION.

- 1. Proposed Regulation: §999.316(a)
- 2. Problem with Proposed Regulation:
 - a. This requirement is not consistent with other laws or with consumer expectations. It would require businesses to build new systems and to make users jump through unnecessary hurdles in order to express a preference. It appears to nudge consumers toward a course of action, rather than empowering them to make their own decisions in a straightforward manner.

Relatedly, it is burdensome and confusing to require this two-step, opt-in consent in situations in which a business may use personal information for additional purposes that are related to those that were disclosed to the consumer (§999.305(a)(3)). The CCPA deliberately adopts an opt-out regime rather than one that is opt-in, making this proposal inconsistent with the law. Furthermore, data protection principles typically do not require additional consent for the use of data that is consistent with the context in which the consumer receives the service.

The GDPR’s Article 6(4) allows further processing of personal data for compatible purposes, provided the controller puts safeguards in place. The proposed regulations would go beyond this requirement.

- b. Requires a two-step process: consumer requests to opt-in and then confirms opt-in. Businesses should be given flexibility concerning how consumers should use an opt-in process.
- 3. Recommended Change:
 - a. Strike the reference to a “two-step” process in section 999.316(a).

XII. SECTION 999.325 VERIFICATION FOR NON-ACCOUNTHOLDERS—CHAMBER PROPOSED CHANGES

A. ISSUE: SIGNED DECLARATION OF PERJURY REQUIREMENT IS UNNECESSARY.

- 1. Proposed Regulation: §999.325(c)
- 2. Problem with Proposed Regulation:
 - a. The language could be interpreted to require “a signed declaration under penalty of perjury” but there could be separate methods of verifying identity that are more reliable than a signed declaration in a business’s particular environment (e.g., blockchain or otherwise).

3. Recommended Change:
 - a. We recommend deleting Section 999.325(c).
 - b. In the event this request is not accepted, the language should be clarified to provide that a business may choose to execute or maintain “a signed declaration under penalty of perjury” or any other higher standard in order to verify requests.
 - c. In the alternative, revise Section 999.325(c): “A business’s compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury and/or any other information that the business determines in necessary to confirm that the requestor is the consumer whose personal information is the subject of the request. Businesses shall maintain all signed declarations as part of their record-keeping obligations.”

- B. ISSUE: REQUIREMENT THAT BUSINESSES PROVIDE TWO TIERS OF AUTHENTICATION FOR RIGHT TO KNOW REQUESTS IS OVERLY BURDENSOME AND NOT COMMON PRACTICE.
 1. Proposed Regulation: §999.325
 2. Problem with Proposed Regulation:
 - a. The requirement that businesses provide two tiers of authentication for right to know requests, depending on whether the request is for categories of specific pieces of personal information, would impose additional burdensome implementation requirements beyond the statute. This is not common practice for third party verification service providers.
 3. Recommended Change:
 - a. Strike section 999.325(c).

- C. ISSUE: TYPES AND THRESHOLD OF PERSONAL INFORMATION FOR VERIFIABLE REQUEST MAY LEAVE CONSUMERS VULNERABLE TO FRAUDULENT REQUESTS.
 1. Proposed Regulation: §999.325(c); 999.325(e); *see also* 999.323
 2. Problem with Proposed Regulation:
 - a. Concerns about feasibility and sufficiency. Name, SSN, DOB are commonly available. If those are provided to a business to request to know specific information (account numbers, for instance), and those data points match what the business has on a consumer, they could be providing the consumer’s account number to a fraudster who bought that identifying data on the web. A fraudster is not going to be deterred by a signed declaration under penalty of perjury.
 - b. Under Section 999.325(c), the requirement that businesses shall “generally avoid” requesting additional information from a consumer for the purposes of verification is at odds with the need to ensure verification.
 3. Recommended Change:
 - a. Strike section 999.325(c).

XIII. SECTION 999.308 PRIVACY POLICY—CHAMBER PROPOSED CHANGES

A. ISSUE: REQUIREMENT THAT BUSINESS PUBLICLY DESCRIBE VERIFICATION PROCESS SHOULD BE ELIMINATED OR SATISFIED BY GENERAL DESCRIPTIONS TO MITIGATE SECURITY RISKS.

1. Proposed Regulation: §999.308(b)(1); *see also* 999.313(a)
2. Problem with Proposed Regulation:
 - a. By requiring a business to publicly communicate how it will verify a consumer request, it could make it easier for an individual to impersonate another in an attempt to illegally collect consumer data. It would be best for each business to design a verification process that is communicated to an individual upon inquiry, and not posted for the public. This section is further made ambiguous by the proposed Section 999.313(a) which says that a business will confirm receipt of a request within 10 days and also provide information on the business's verification process. This latter situation seems the appropriate time/method to disclose such information—not the former and certainly not both on the website and within the private communication.
 - b. The requirement that a business describe the process used to verify consumer requests, including any information the consumer must provide, may be satisfied with a description at a high level of generality in order to mitigate security risks.
3. Recommended Change:
 - a. Strike section 999.308(b)(1)(c).
 - b. For consistency with Section 1798.130(a)(5)(C)(i) of the statute, revise regulation section 999.308(b)(1)(d)(2) to: "For each category of personal information collected, provide the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties ~~with to~~ whom the business ~~shares~~ sells personal information. The notice shall be written in a manner that provides consumers a meaningful understanding of the categories listed."

B. ISSUE: REGULATIONS SHOULD PROVIDE CLARIFICATION REGARDING THE REQUISITE LEVEL OF DETAIL TO DESIGNATE AN AUTHORIZED AGENT TO MAKE CONSUMER REQUESTS.

1. Proposed Regulation: §999.308(b)(5)(a);
2. Problem with Proposed Regulation:
 - a. The AG should clarify the level of detail required under Section 999.308(b)(5)(a) to explain how a consumer can designate an authorized agent for making requests.
3. Recommended Change:
 - a. Revise Section 999.308(b)(5)(a): "Explain generally how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf."

XIV. SECTION 999.318 REQUESTS TO ACCESS OR DELETE HOUSEHOLD INFORMATION—CHAMBER PROPOSED CHANGES

A. ISSUE: PROPOSED REGULATION DOES NOT ADDRESS CONCERN THAT HOUSEHOLD INFORMATION COULD BE DISCLOSED INCORRECTLY.

1. Proposed Regulation: §999.318(b)
2. Problem with Proposed Regulation:
 - a. Section 999.318(b) does not eliminate the risk that household information could be disclosed incorrectly because a business has no way of knowing whether the members of the household who have verified their identity are in fact all of the members of the household (i.e. if there's one member who's not there, a business might not know.)
 - b. The current definition of "household" in Section 999.318 is problematic and might cause businesses to provide data to members of households that might not have a right to see that data or delete that data. Businesses need further clarity regarding the security issue of providing data to household members that may not have a right to see or delete the data of other household members.
3. Recommended Change:
 - a. Revise Section 999.318(b): "If all consumers of the household jointly request access to specific pieces of information for the household or the deletion of household personal information, and the business can individually verify all the members of the household subject to verification requirements set forth in Article 4, then the business shall comply with the request. This obligation exists for businesses only if (i) all users have verified their identity, and (ii) they can verify that these are all of the members of the household."

XV. SECTION 999.323 GENERAL RULES REGARDING VERIFICATION—CHAMBER PROPOSED CHANGES

A. ISSUE: INCREASED COMPLEXITY FOR VERIFICATION OF CONSUMERS.

1. Proposed Regulation: §999.323; 999.323(d)
2. Problem with Proposed Regulation:
 - a. Proposed regulations create a complicated process for verifying consumers: two data point match for categories, but three data point match and a signed declaration under penalty of perjury are required for specific pieces. If there is not enough information to verify for one purpose, a company must proactively determine whether there is enough to verify for another type of request, even if the consumer did not request it.
 - b. On the one hand, the amended statute says that businesses should use a verification process that makes sense given the sensitivity, etc. of the data at issue. On the other hand, the proposed regulations set forth a formulaic statement for verification (two data points versus three data points). Those two provisions need to be reconciled.
 - c. Section 999.323(d) is vague. What are "reasonable security measures to detect fraudulent identity-verification activity"—this entire process will involve matching what consumers are willing to provide with incomplete data kept in business databases? How are businesses to determine reasonable security measures without more guidance from the AG?
3. Recommended Change:
 - a. Strike Section 999.323(d).

- a. The illustrative examples in Section 999.336(c) are ambiguous. This ambiguity and the confusing term “financial incentive” all point to the serious concerns about how loyalty programs will operate under the CCPA and whether loyalty programs should even be considered “financial incentive” in the first place, especially if a consumer will be inherently treated differently if their data is deleted from a loyalty program (won’t receive the same personalized discounts, points/reward removed, etc.)
- 3. Recommended Changes:
 - a. Remove 999.336(c)(2) illustrative Example 2.

XVIII. SECTION 999.337 CALCULATING THE VALUE OF CONSUMER DATA—CHAMBER PROPOSED CHANGES

A. ISSUE: PROPOSED REGULATIONS ARE INCONSISTENT WITH STATUTORY LANGUAGE.

- 1. Proposed Regulation: §999.337
- 2. Problem with Proposed Regulation:
 - a. Section 999.337 permits a business to offer a price or service difference if “reasonably related to the value of the consumer’s data.” The amended statute, as defined in CCPA Section 1798.125, allows financial incentives if “reasonably related to the value provided to the business by the consumer’s data.” These are inconsistent guidelines.
- 3. Recommend Change:
 - a. Strike Section 999.337.
 - b. In the alternative, align language with CCPA Section 1798.125 such that this regulation section reads “reasonably related to the value provided to the business by the consumer’s data.”

XIX. SECTION 999.330 MINORS UNDER 13 YEARS OF AGE—CHAMBER PROPOSED CHANGES

A. ISSUE: REGULATIONS SHOULD ALLOW FOR ANY METHOD PERMITTED BY COPPA FOR DISCLOSURE.

- 1. Proposed Regulation: §999.330(a)
- 2. Problem with Proposed Regulation:
 - a. The regulations should allow for any method permitted by COPPA for disclosure. This will allow for any new methods approved by the FTC to be also permitted under CCPA.
- 3. Recommended Change:
 - a. Revise Section 999.330(a) to simply be a reference to the methods approved by the FTC for disclosure.
 - b. Revise Section 999.330(a) to add Section 999.330(a)(2)(g): “Any other method of disclosure permitted by the Children’s Online Privacy Protection Act.”

XX. SECTION 999.331 MINORS 13 TO 16 YEARS OF AGE—CHAMBER PROPOSED CHANGES

- A. ISSUE: BUSINESSES THAT DO NOT PLAN TO SELL PERSONAL INFORMATION OF 13 TO 16 YEARS OLD SHOULD NOT NEED TO HAVE AN OPT-IN MECHANISM.
1. Proposed Regulation: §999.331(a)
 2. Problem with Proposed Regulation:
 - a. If a company does not plan to sell this personal information, they need not have an opt-in mechanism.
 3. Recommended Change:
 - a. Revise Section 999.331(a): “A business that has actual knowledge that it collects or maintains the personal information of minors at least 13 and less than 16 years of age, and wishes to sell such personal information, shall establish, document, and comply with a reasonable process for allowing such minors to opt-in to the sale of their personal information, pursuant to section 999.316.

EXHIBIT A

**TITLE 11. LAW
DIVISION 1. ATTORNEY GENERAL**

**CHAPTER 20. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS
PROPOSED TEXT OF REGULATIONS**

Article 1. General Provisions

§ 999.300. Title and Scope

- (a) This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as “these regulations.” These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have.
- (b) A violation of these regulations shall constitute a violation of the CCPA, and be subject to the remedies provided for therein.
- (c) A business whose operations are outside of California and that only collects a de minimus amount of personal information from California residents – such as a business with a domain .co.uk or .com.mx – are not required to comply with CCPA.
- (d) Businesses that operate outside of California and do not target their services to California residents are not covered.
- (e) The title shall not apply to a provider of health care governed by CMIA or HIPAA, to the extent the provider or covered entity collects personal information in connection with the provision or sale of health care-related products or services, and to the extent that the provider or covered entity maintains that personal information in a way that meets HIPAA Security Rule requirements.
- (b)(f) These regulations shall be operative on the effective date of January 1, 2021.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100-1798.199, Civil Code.

§ 999.301. Definitions

In addition to the definitions set forth in Civil Code section 1798.140, for purposes of these regulations:

- (a) “Affirmative authorization” means an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a child under 13, it means that the parent or guardian has provided consent to the sale of the child’s personal information in accordance with the methods set forth in section 999.330. For consumers 13 years and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

- (b) "Attorney General" means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General.
- (c) "Authorized agent" means a natural person or a business entity registered with the Secretary of State that a consumer has authorized to act on their behalf subject to the requirements set forth in section 999.326.
- (d) "Categories of sources" means types of entities from which a business collects personal information about consumers, including but not limited to the consumer directly, government entities from which public records are obtained, and consumer data resellers.
- (e) "Categories of third parties" means types of entities that do not collect personal information directly from consumers, including but not limited to advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers.
- ~~(f)~~ (i) "CCPA" means the California Consumer Privacy Act of 2018, Civil Code sections 1798.100 *et seq.*
- ~~(g)~~ (g) "Directly notify" means contacting the consumer directly with the required information, provided, however, that a business will have been deemed to directly notify a consumer of changes to its policies and practices if the notification is published and made available on its website for a sufficient period of time or other standard method of providing privacy policies and notices to consumers.
- ~~(h)~~ (h) "Financial incentive" means a program, benefit, or other offering, including payments to consumers as compensation, for the disclosure, deletion, or sale of personal information.
- ~~(i)~~ (i) "Household" means a person or group of people occupying a single dwelling.
- ~~(j)~~ (j) "Notice at collection" means the notice given by a business to a consumer at or before the time a business collects personal information from the consumer as required by Civil Code section 1798.100(b) and specified in these regulations.
- ~~(k)~~ (k) "Notice of right to opt-out" means the notice given by a business informing consumers of their right to opt-out of the sale of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations.
- ~~(l)~~ (l) "Notice of financial incentive" means the notice given by a business explaining each financial incentive or price or service difference subject to Civil Code section 1798.125(b) as required by that section and specified in these regulations.
- ~~(m)~~ (m) "Price or service difference" means (1) any difference in the price or rate charged for any goods or services to any consumer, including through the use of discounts, financial payments, or other benefits or penalties; or (2) any difference in the level or quality of any goods or services offered to any consumer, including denial of goods or services to the consumer. If an individual working for a broker or provider as a business partner opts out.

of the sale of personal information this will not prevent the continued relationship with a business.

~~(n)~~ “Privacy policy” means the policy referred to in Civil Code section 1798.130(a)(5), and means the statement that a business shall make available to consumers describing the business’s practices, both online and offline, regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their own personal information.

~~(o)~~ “Request to know” means a consumer request that a business disclose personal information that it has about the consumer pursuant to Civil Code sections 1798.100, 1798.110, or 1798.115. It includes a request for any or all of the following:

- (1) Specific pieces of personal information that a business has about the consumer;
- (2) Categories of personal information it has collected about the consumer;
- (3) Categories of sources from which the personal information is collected;
- (4) Categories of personal information that the business sold or disclosed for a business purpose about the consumer;
- (5) Categories of third parties to whom the personal information was sold or disclosed for a business purpose; and
- (6) The business or commercial purpose for collecting or selling personal information.

~~(p)~~ “Request to delete” means a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105.

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

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

~~(s)~~ “Third-party identity verification service” means a security process offered by an independent third party who verifies the identity of the consumer making a request to the business. Third-party verification services are subject to the requirements set forth in Article 4 regarding requests to know and requests to delete.

~~(t)~~ “Typical consumer” means a natural person residing in the United States.

~~(u)~~ “URL” stands for Uniform Resource Locator and refers to the web address of a

specific website.

(+)(v) “Verify” means to determine that the consumer making a request to know or request to delete is the consumer about whom the business has collected information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100-1798.199, Civil Code.

Article 2. Notices to Consumers

§ 999.305. Notice at Collection of Personal Information

(a) Purpose and General Principles

- (1) The purpose of the notice at collection is to inform consumers at or before the time of collection of a consumer’s personal information of the categories of personal information to be collected from them and the purposes for which the categories of personal information will be used.
- (2) The notice at collection shall be designed and presented to the consumer in a way that is easy to read and understandable to an average consumer. The notice shall:
 - a. Use plain, straightforward language and avoid technical or legal jargon.
 - b. Use a format that draws the consumer’s attention to the notice and makes the notice readable, including on smaller screens, if applicable.
 - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.
 - d. Be accessible to consumers with disabilities when required by the Americans with Disabilities Act of 1990, Pub. L. No. 101-336, 104 Stat. 328 (1990). At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.
 - e. Be visible or accessible where consumers will see it before any personal information is collected. For example, when a business collects consumers’ personal information online, it may conspicuously post a link to the notice on the business’s website homepage or the mobile application’s download page, or on all webpages where personal information is collected. When a business collects consumers’ personal information offline, it may, for example, include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to the web address where the notice can be found.
- (3) A business shall not use a consumer’s personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer’s personal information for a purpose that was not previously disclosed to

the consumer in the notice at collection, the business shall directly notify the consumer of this new use ~~and obtain explicit consent from the consumer to use it for this new purpose.~~

- (4) A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection.
 - (5) If a business does not give the notice at collection to the consumer at or before the collection of their personal information, the business shall not collect personal information from the consumer.
- (b) A business shall include the following in its notice at collection:
- (1) A list of the categories of personal information about consumers to be collected. Each category of personal information shall be written in a manner that provides consumers a meaningful understanding of the information being collected.
 - (2) For each category of personal information, the business or commercial purpose(s) for which it will be used.
 - (3) If the business sells personal information, the link titled “Do Not Sell My Personal Information” or “Do Not Sell My Info” required by section 999.315(a), or in the case of offline notices, the web address for the webpage to which it links.
 - (4) A link to the business’s privacy policy, or in the case of offline notices, the web address of the business’s privacy policy.
- (c) If a business collects personal information from a consumer online, the notice at collection may be given to the consumer by providing a link to the section of the business’s privacy policy that contains the information required in subsection (b).
- (d) A business that does not collect information directly from consumers does not need to provide a notice at collection to the consumer, but before it can sell a consumer’s personal information, it shall do either of the following:
- (1) ~~Contact~~ Directly notify the consumer ~~directly~~ to provide notice that the business sells personal information about the consumer and provide the consumer with a notice of right to opt-out in accordance with section 999.306; or
 - (2) Contact the source of the personal information to:
 - a. Confirm that the source provided a notice at collection to the consumer in accordance with subsections (a) and (b), ~~and~~
 - b. ~~Obtain signed attestations from the source describing how the source gave the notice at collection and including an example of the notice. Attestations shall be retained by the business for at least two years and made available to the consumer~~

Commented [SLD(1): We suggest deletion. In the alternative, the regulations should clarify that a business that receives personal information from an indirect source may comply with its CCPA obligations through contractual provisions that require other businesses to provide the requisite notice to consumers. The requirements to contact the source and obtain signed attestations are confusing and duplicative.

~~upon request.~~

Note: Authority: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.115, and 1798.185, Civil Code.

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

(a) Purpose and General Principles

- (1) The purpose of the notice of right to opt-out of sale of personal information is to inform consumers of their right to direct a business that sells ~~(or may in the future sell)~~ their personal information to stop selling their personal information, and to refrain from doing so in the future.
- (2) The notice of right to opt-out shall be designed and presented to the consumer in a way that is easy to read and understandable to an average consumer. The notice shall:
 - a. Use plain, straightforward language and avoid technical or legal jargon.
 - b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.
 - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.
 - d. Be accessible to consumers with disabilities. ~~when required by the Americans with Disabilities Act of 1990, Pub. L. No. 101-336, 104 Stat. 328 (1990). At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.~~

(b) A business that sells the personal information of a consumer shall provide a notice of right to opt-out to the consumer as follows:

- (1) A business shall post the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link on the website homepage or the download or landing page of a mobile application. The notice shall include the information specified in subsection (c) or link to the section of the business's privacy policy that contains the same information.
- (2) A business that substantially interacts with consumers offline shall also provide notice to the consumer by an offline method that facilitates consumer awareness of their right to opt-out. Such methods include, but are not limited to, printing the notice on paper forms that collect personal information, providing the consumer with a paper version of the notice, and posting signage directing consumers to a website where the notice can be found.
- (3) A business that does not operate a website shall establish, document, and comply with

another method by which it informs consumers of their right to direct a business that sells their personal information to stop selling their personal information. That method shall comply with the requirements set forth in subsection (a)(2).

- (c) A business shall include the following in its notice of right to opt-out:
- (1) A description of the consumer's right to opt-out of the sale of their personal information by the business;
 - (2) The webform by which the consumer can submit their request to opt-out online, as required by Section 999.315(a), or if the business does not operate a website, the offline method by which the consumer can submit their request to opt-out;
 - (3) Instructions for any other method by which the consumer may submit their request to opt-out;
 - (4) Any proof required when a consumer uses an authorized agent to exercise their right to opt-out, or in the case of a printed form containing the notice, a webpage, online location, or URL, where consumers can find information about authorized agents; and
 - (5) A link or the URL to the business's privacy policy, or in the case of a printed form containing the notice, the URL of the webpage where consumers can access the privacy policy.
- (d) A business is exempt from providing a notice of right to opt-out if:
- (1) It does not, ~~and will not~~, sell personal information collected during the time period during which the notice of right to opt-out is not posted; and
 - (2) It states in its privacy policy that that it does not ~~and will not~~ sell personal information. ~~A consumer whose personal information is collected while a notice of right to opt-out notice is not posted shall be deemed to have validly submitted a request to opt-out.~~
- (e) Opt-Out Button or Logo
- (1) The following opt-out button or logo may be used in addition to posting the notice of right to opt-out, but not in lieu of any posting of the notice. [BUTTON OR LOGO TO BE ADDED IN A MODIFIED VERSION OF THE REGULATIONS AND MADE AVAILABLE FOR PUBLIC COMMENT.]
 - (2) This opt-out button or logo shall link to a webpage or online location containing the information specified in section 999.306(c), or to the section of the business's privacy policy that contains the same information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

§ 999.307. Notice of Financial Incentive

(a) Purpose and General Principles

- (1) The purpose of the notice of financial incentive is to explain to the consumer each financial incentive or price or service difference a business may offer in exchange for the retention or sale of a consumer's personal information so that the consumer may make an informed decision on whether to participate. A financial incentive or price or service difference offered in connection with only collecting personal data but unrelated to a consumer's exercise of rights under CCPA does not require a notice of financial incentive.
- (2) The notice of financial incentive shall be designed and presented to the consumer in a way that is easy to read and understandable to an average consumer. The notice shall:
 - a. Use plain, straightforward language and avoid technical or legal jargon.
 - b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.
 - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.
 - d. Be accessible to consumers with disabilities when required by the Americans with Disabilities Act of 1990, Pub. L. No. 101-336, 104 Stat. 328 (1990). ~~At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.~~
 - e. Be available online or other physical location where consumers will see it before opting into the financial incentive or price or service difference.
- (3) If the business offers the financial incentive or price of service difference online, the notice may be given by providing a link to the section of a business's privacy policy that contains the information required in subsection (b).

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

- (1) A succinct summary of the financial incentive or price or service difference offered;
- (2) A description of the material terms of the financial incentive or price of service difference, ~~including the categories of personal information that are implicated by the financial incentive or price or service difference;~~
- (3) How the consumer can opt-in to the financial incentive or price or service difference;
- (4) Notification of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and
- ~~(5) An explanation of why the financial incentive or price or service difference is permitted under the CCPA.~~

- a. ~~A good faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and~~
- b. ~~A description of the method the business used to calculate the value of the consumer's data.~~

Formatted: Indent: Hanging: 0.31", Right: 0.71", Tab stops: 0.77", Left + Not at 1.08"

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.130, Civil Code.

§ 999.308. Privacy Policy

(a) Purpose and General Principles

- (1) The purpose of the privacy policy is to provide the consumer with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information. The privacy policy shall not contain specific pieces of personal information about individual consumers and need not be personalized for each consumer.
- (2) The privacy policy shall be designed and presented in a way that is easy to read and understandable to ~~an average typical~~ consumer. The notice shall:
 - a. Use plain, straightforward language and avoid technical or legal jargon.
 - b. Use a format that makes the policy readable, including on smaller screens, if applicable.
 - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.
 - d. Be accessible to consumers with disabilities when required by the Americans with Disabilities Act of 1990, Pub. L. No. 101-336, 104 Stat. 328 (1990). At a minimum, provide information on how a consumer with a disability may access the policy in an alternative format.
 - e. Be available in an additional format that allows a consumer to print it out as a separate document.
- (3) The privacy policy shall be posted online through a conspicuous link using the word "privacy," on the business's website homepage or on the download or landing page of a mobile application. If the business has a California-specific description of consumers' privacy rights on its website, then the privacy policy shall be included in that description. A business that does not operate a website shall make the privacy policy conspicuously available to consumers.

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

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

- a. Explain that a consumer has the right to request that the business disclose what personal information it collects, uses, discloses, and sells.
- b. Provide instructions for submitting a verifiable consumer request to know and provide links to an online request form or portal for making the request, if offered by the business.
- c. ~~Describe the process the business will use to verify the consumer request, including any information the consumer must provide.~~
- d. Collection of Personal Information
 1. List the categories of consumers' personal information the business has collected about consumers in the preceding 12 months. The notice shall be written in a manner that provides consumers a meaningful understanding of the information being collected.
 2. For each category of personal information collected, provide the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties ~~with to~~ whom the business ~~sells shares~~ personal information. The notice shall be written in a manner that provides consumers a meaningful understanding of the categories listed.
- e. Disclosure or Sale of Personal Information
 1. State whether or not the business has disclosed or sold any personal information to third parties for a business or commercial purpose in the preceding 12 months.
 2. List the categories of personal information, if any, that it disclosed or sold to third parties for a business or commercial purpose in the preceding 12 months.
 3. ~~State whether or not the business sells the personal information of minors under 16 years of age without affirmative authorization.~~

(2) Right to Request Deletion of Personal Information

- a. Explain that the consumer has a right to request the deletion of their personal information collected ~~or maintained~~ by the business.
- b. Provide instructions for submitting a verifiable consumer request to delete and provide links to an online request form or portal for making the request, if offered by the business.

- c. Describe the process the business will use to verify the consumer request, including any information the consumer must provide.
- (3) Right to Opt-Out of the Sale of Personal Information
- a. Explain generally that the consumer has a right to opt-out of the sale of their personal information by a business.
 - b. Include the contents of the notice of right to opt-out or a link to it in accordance with section 999.306.
- (4) Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights
- a. Explain that the consumer has a right not to receive discriminatory treatment by the business for the exercise of the privacy rights conferred by the CCPA.
- (5) Authorized Agent
- a. Explain generally how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf.
- (6) Contact for More Information: Provide consumers with a contact for questions or concerns about the business's privacy policies and practices using a method reflecting the manner in which the business primarily interacts with the consumer.
- (6)
- (7) Date the privacy policy was last updated.
- (8) If subject to the requirements set forth section 999.317(g), the information compiled in section 999.317(g)(1) or a link to it.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.115, 1798.120, 1798.125 and 1798.130, Civil Code.

Article 3. Business Practices for Handling Consumer Requests

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

- (a) A business shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number, and if the business operates a website, an interactive webform accessible through the business's website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.
- (b) Subject to 999.312(a) above which shall be sufficient to comply with this section under all circumstances. A business shall provide two or more designated methods for submitting requests to delete. Acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a link or form available online through a business's

Formatted: Indent: Left: 0.77", No bullets or numbering

website, a designated email address, a form submitted in person, and a form submitted through the mail.

- (c) A business shall consider the methods by which it interacts with consumers when determining which methods to provide for submitting requests to know and requests to delete. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer, even if it requires a business to offer three methods for submitting requests to know. Illustrative examples follow:

- (1) *Example 1:* If the business is an online retailer, at least one method by which the consumer may submit requests should be through the business's retail website.

- (2) *Example 2:* If the business operates a website but primarily interacts with customers in person at a retail location, the business shall offer ~~three~~two methods to submit requests to know—a toll-free telephone number, and an interactive webform accessible through the business's website, ~~and or~~ a form that can be submitted in person at the retail location.

- ~~(2)(3)~~ *Example 3:* If the business operates a website and interacts with customers in person at a retail location, but primarily collects data online (such as a travel company website), the business can offer two methods to submit requests to know—a toll-free telephone number and an interactive webform accessible through the business's website. In this case, a form that can be submitted in person at the retail location is not necessary.

Formatted: Widow/Orphan control, Tab stops: Not at 0.77"

Formatted: Font: 11 pt, Underline

- (d) A business ~~shall may~~ use a two-step process for online requests to delete where the consumer must first, clearly submit the request to delete and then second, separately confirm that they want their personal information deleted.

- (e) If a business does not interact directly with consumers in its ordinary course of business, at least one method by which a consumer may submit requests to know or requests to delete shall be online, such as through the business's website or a link posted on the business's website.

- ~~(e)(f)~~ A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

- ~~(f)~~ If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either:

- ~~(1)~~ Treat the request as if it had been submitted in accordance with the business's designated manner, or

- ~~(2)~~ Provide the consumer with specific directions on how to submit the request or remedy any deficiencies with the request, if applicable.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140, and 1798.185, Civil Code.

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

- (a) Upon receiving a request to know or a request to delete, a business shall confirm receipt of the request through either mail, email, or another notification method, within 10 days and provide information about how the business will process the request. The information provided shall describe the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request.
- (b) Businesses shall respond to complete requests to know and requests to delete within 45 days. The 45- day period will begin on the day that the business receives the request, unless the request is incomplete, or the consumer fails to provide information necessary to verify the request, regardless of time required to verify the request. If necessary, businesses may take up to an additional 45 days to respond to the consumer's request, for a maximum total of 90 days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.
- (c) Responding to Requests to Know
 - (1) For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the consumer that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (c)(2).
 - (2) For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall provide or direct the consumer to its general business practices regarding the collection, maintenance, and sale of personal information set forth in its privacy policy.
 - (3) A business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's or another consumer's account with the business, or the security of the business's systems or networks.
 - (4) A business shall not at any time disclose a consumer's Social Security number, driver's license number or other government-issued identification number, financial

account number, any health insurance or medical identification number, an account password, or security questions and answers. This subsection does not apply to requests seeking portability of information where such identifiers enumerated in section 999.313(c)(4) are necessary to support portability.

- (5) If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception pursuant to the CCPA, the business shall inform the requestor and explain the basis for its denial. provided however that a business shall be deemed to be in compliance with the requirement if bases for denial are set forth in its privacy policy and the business refers the consumer to its privacy policy. If the request is denied only in part, the business shall disclose the other information sought by the consumer.
- (6) A business shall use reasonable security measures when transmitting personal information to the consumer.
- (7) If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 4.
- (8) Unless otherwise specified, the 12-month period covered by a consumer's verifiable request to know referenced in Civil Code section 1798.130(a)(2) shall run from the date the business receives the request, regardless of the time required to verify the request.
- (9) In responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response to the consumer as required by the CCPA. It shall not refer the consumer to the businesses' general practices outlined in its privacy policy unless its response would be the same for substantially all or most consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories.
- (10) In responding to a verified request to know categories of personal information, the business shall provide for each identified category of personal information it has collected about the consumer:
 - a. The categories of sources from which the personal information was collected;
 - b. The business or commercial purpose for which it collected the personal information;
 - c. The categories of third parties to whom the business sold or disclosed the category of personal information for a business purpose; and or, as requested by the consumer.

d. The business or commercial purpose for which it sold or disclosed the category of personal information.

~~(11)~~ A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner, such as described in this section, that provides consumers a meaningful understanding of the categories listed.

~~(12)~~ A business need not additionally fulfill a consumer's request to provide categories of information collected if it is also providing specific pieces of information.

~~(13)~~ A business shall identify the personal information responsive to a request to know by conducting a commercially reasonable search of its records for documents that are responsive, considering the sensitivity of the personal information the business holds and the expense of compliance. A business does not violate the CCPA when it conducts a commercially reasonable search of its records in good faith but fails to identify a responsive record.

(d) Responding to Requests to Delete

(1) For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete.

The business shall inform the requestor that their identity cannot be verified ~~and shall instead treat the request as a request to opt out of sale.~~

(2) A business shall comply with a consumer's request to delete their personal information by:

- a. Permanently and completely erasing the personal information on its existing systems with the exception of archived or back-up systems;
- b. De-identifying the personal information; or
- c. Aggregating the personal information.

(3) If a business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the data on the archived or backup system is next accessed or used.

(4) In its response to a consumer's request to delete, the business shall specify the manner in which it has deleted the personal information.

(5) In responding to a request to delete, a business shall disclose that it will maintain a record of the request pursuant to Civil Code section 1798.105(d).

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

Commented [VBM(2): Priority recommendation would be to strike this provision entirely noting there are separate requests for separate reasons. In the alternative, recommendation would be to focus on a process for making an unverifiable request to delete become a verified request to delete

- a. Inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including any statutory and regulatory exception therefor, provided however, that a business shall be deemed to be in compliance with this requirement if the bases for denial are set forth in its privacy policy and the business refers the consumer to its privacy policy;
- b. Delete the consumer's personal information that is not subject to the exception; and
- c. Not use the consumer's personal information retained for any other purpose than provided for by that exception or any other exception pursuant to the CCPA.

(7) In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information only if a global option to delete all personal information is also offered, and more prominently presented than the other choices. The business shall still use a two-step confirmation process where the consumer confirms their selection as required by section 999.312(d).

(7)(8) A business shall identify the personal information responsive to a request to delete by conducting a commercially reasonable search of its records for documents that are responsive, considering the sensitivity of the personal information the business holds and the expense of compliance. A business does not violate the CCPA when, it conducts a commercially reasonable search of its records in good faith but fails to identify a responsive record.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

§ 999.314. Service Providers

- (a) To the extent that a person or entity provides services to a person or organization that is not a business, no obligations under CCPA shall apply to such person or entity and would otherwise meet the requirements of a "service provider" under Civil Code section 1798.140(v), that person or entity shall be deemed a service provider for purposes of the CCPA and these regulations.
- (b) To the extent that a business directs a person or entity to collect personal information directly from a consumer on the business's behalf, and would otherwise meet all other requirements of a "service provider" under Civil Code section 1798.140(v), that person or entity shall be deemed a service provider for purposes of the CCPA and these regulations.
- (c) A service provider shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider, without the agreement of such person, entity, or consumer, for the purpose of providing services that result in the sale of a consumer's personal information to another person or entity to a third party. A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, in order to provide the services specified in a contract with the business, or

to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.

- (d) If a service provider receives a request to know or a request to delete from a consumer regarding personal information that the service provider collects, maintains, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial. ~~The service provider shall also inform the consumer that it should submit the request directly to the business on whose behalf the service provider processes the information and, when feasible, provide the consumer with contact information for that business.~~
- (e) A service provider that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140, and 1798.185, Civil Code.

§ 999.315. Requests to Opt-Out

- (a) A business shall provide two or more designated methods for submitting requests to opt-out, including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information,” or “Do Not Sell My Info,” on the business’s website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information. The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should: (i) ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business; (ii) ensure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer, and does not require that the consumer provide additional information beyond what is necessary; (iii) clearly represent a consumer’s intent and be free of defaults constraining or presupposing such intent; and (iv) ensure that the opt-out preference signal does not conflict with other commonly-used privacy settings or tools that consumers may employ.
- (b) A business shall consider the methods by which it interacts with consumers when determining which methods consumers may use to submit requests to opt-out, the manner in which the business sells personal information to third parties, available technology, and ease of use by the average-typical consumer. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer.
- (c) If a business collects personal information from consumers online, the business ~~shall~~ may treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120

for that browser or device, or, if known, for the consumer, provided that the consumer undertakes an affirmative action to opt out of the sale of their information. Default opt-outs shall not constitute an affirmative step to opt out.

- (d) In responding to a request to opt-out, a business that sells personal information may present the consumer with the choice to opt-out of sales of certain categories of personal information as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices.
- (e) Upon receiving a request to opt-out, a business shall act upon the request as soon as feasibly possible, but no later than 15-30 days from the date the business receives the request.
- (f) ~~A business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the consumer's request that the consumer has exercised their right to opt out and instruct them not to further sell the information. The business shall notify the consumer when this has been completed.~~
- (g) A consumer may use an authorized agent to submit a request to opt-out on the consumer's behalf if the consumer provides the authorized agent written permission to do so. A business may deny a request from an authorized agent that does not submit proof that they have been authorized by the consumer to act on the consumer's behalf. User-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall may be considered a request directly from the consumer, not through an authorized agent if they represent the consumer's affirmative choice.
- (h) A request to opt-out need not be a verifiable consumer request. If a business, however, cannot verify the identity of a person making a request concerning personal information sold for purposes other than advertising or marketing, the business has a good faith, reasonable, and documented belief that a request to opt out is fraudulent, the business may deny the request. The business and shall inform the requestor that their identity cannot be verified. ing party that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent.

Note: Authority cited: Sections 1798.135 and 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140, and 1798.185, Civil Code.

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

- ~~(a) Requests to opt in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt in and then second, separately confirm their choice to opt in.~~
- (b)(a) A business may inform a consumer who has opted-out when a transaction requires the sale of their personal information as a condition of completing the transaction, along with instructions on how the consumer can opt-in.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, and 1798.185, Civil Code.

§ 999.317. Training; Record-Keeping

- (a) All individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA shall be informed of all the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.
- (b) A business shall maintain records of consumer requests made pursuant to the CCPA and how the business responded to said requests for at least 24 months.
- (c) The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.
- (d) A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.
- (e) Information maintained for record-keeping purposes shall not be used for any other purpose.
- (f) Aside from this record-keeping purpose, a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.

~~(g) A business that alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers, shall:~~

- ~~(1) Compile the following metrics for the previous calendar year:
 - a. The number of requests to know that the business received, complied with in whole or in part, and denied;
 - b. The number of requests to delete that the business received, complied with in whole or in part, and denied;
 - c. The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and
 - d. The median number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.~~
- ~~(2) Disclose the information compiled in subsection (g)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy.~~
- ~~(3) Establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests or the business's compliance with the~~

Commented [VBM(3): Alternatively, add to 317(g), "except as otherwise exempted under the CCPA" and amend 313(g)(1)(d) from "median" to "average" number of days.

~~CCPA are informed of all the requirements in these regulations and the CCPA.~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.135, and 1798.185, Civil Code.

§ 999.318. Requests to Access or Delete Household Information

- (a) Where a consumer does not have a password-protected account with a business, a business may respond to a request to know or request to delete as it pertains to household personal information by providing aggregate household information, subject to verification requirements set forth in Article 4.
- (b) If all consumers of the household jointly request access to specific pieces of information for the household or the deletion of household personal information, and the business can individually verify all the members of the household subject to verification requirements set forth in Article 4, then the business shall comply with the request. This obligation exists for businesses only if (i) all users have verified their identity, and (ii) they can verify that these are all of the members of the household.
~~(b)~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.140, and 1798.185, Civil Code.

Article 4. Verification of Requests

§ 999.323. General Rules Regarding Verification

- (a) A business shall establish, document, and comply with a reasonable method for verifying that the person making a request to know or a request to delete is the consumer about whom the business has collected information.
- (b) In determining the method by which the business will verify the consumer's identity, the business shall:
 - (1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section.
 - (2) Avoid collecting the types of personal information identified in Civil Code section 1798.81.5(d), unless necessary for the purpose of verifying the consumer.
 - (3) Consider the following factors:
 - a. The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive or valuable personal information shall warrant a more stringent verification process. The types of personal information identified in Civil Code section 1798.81.5(d) shall be considered presumptively sensitive.

Formatted: Indent: Left: 0.38", No bullets or numbering

- b. The risk of harm to the consumer posed by any unauthorized access or deletion. A greater risk of harm to the consumer by unauthorized access or deletion shall warrant a more stringent verification process;
 - c. The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be;
 - d. Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated;
 - e. The manner in which the business interacts with the consumer; and
 - f. Available technology for verification.
- (c) ~~A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however,~~ the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, and for security or fraud-prevention purposes. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 999.317.
- ~~(d) A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information.~~
- ~~(e)(d)~~ If a business maintains consumer information that is de-identified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request

Commented [VBM(4): Primary recommendation is to strike Section 999.323(d). In the alternative, recommendation is to revise the language as follows:

"A business shall implement reasonable security measures, as defined in guidance documents provided by the Attorney General, to detect fraudulent identity- verification activity and prevent the unauthorized access to or deletion of a consumer's personal information."

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140, and 1798.185, Civil Code.

§ 999.324. Verification for Password-Protected Accounts

- (a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 999.323. The business shall also require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data.
- (b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to know or request to delete until further verification procedures determine that the consumer request is authentic

and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 999.325 to further verify the identity of the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

§ 999.325. Verification for Non-Accountholders

- (a) If a consumer does not have or cannot access a password-protected account with the business, the business shall comply with subsections (b) through (g) of this section, in addition to section 999.323.
- (b) A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business, and/or any other information which the business has determined to be reliable for the purpose of verifying the consumer.
- (c) ~~A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer, together with a signed declaration under penalty of perjury and/or any other information that the business determines in necessary to confirm that the requestor is the consumer whose personal information is the subject of the request. Businesses shall maintain all signed declarations as part of their record-keeping obligations.~~
- (d) A business's compliance with a request to delete may require that the business verify the identity of the consumer to a reasonable degree or a reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion. For example, the deletion of family photographs and documents may require a reasonably high degree of certainty, while the deletion of browsing history may require a reasonable degree of certainty. A business shall act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with the regulations set forth in Article 4.
- (e) Illustrative scenarios follow:
 - (1) If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if the business maintains the consumer's name and credit card number, the business may require the consumer to provide the credit card's security code and identifying a recent purchase made with the credit card to verify their

Commented [SLD(5)]:

(1) The Chamber recommends deleting 999.325(c). In the event this request is not accepted, the language should be clarified to provide that a business may choose to execute or maintain "a signed declaration under penalty of perjury" or any other higher standard in order to verify requests.

OR, in the alternative

(2) A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury and/or any other information that the business determines in necessary to confirm that the requestor is the consumer whose personal information is the subject of the request. Businesses shall maintain all signed declarations as part of their record-keeping obligations.

identity to reasonable degree of certainty.

- (2) If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the non-name identifying information. This may require the business to conduct a fact-based verification process that considers the factors set forth in section 999.323(b)(3).
- (f) If there is no reasonable method by which a business can verify the identity of the consumer to the degree of certainty required by this section, the business shall state so in response to any request and, if this is the case for all consumers whose personal information the business holds, in the business's privacy policy. The business shall also explain why it has no reasonable method by which it can verify the identity of the requestor. The business shall evaluate on a yearly basis whether such a method can be established and shall document its evaluation.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

§ 999.326. Authorized Agent

- (a) When a consumer uses an authorized agent to submit a request to know or a request to delete, the business may require that the consumer:
 - (1) Provide the authorized agent written permission to do so; and
 - (2) Verify their own identity directly with the business.
- (b) This section permits businesses to require (1) instruction directly from the consumer regarding agent authorization, (2) the agent to make requests only after accessing the consumer's account, and (3) return personal information only through the consumer's account (rather than to the agent directly).
- ~~(b)~~
- (c) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4000 to 4465.
- (d) A business may deny a request from an agent that does not submit proof that they have been authorized by the consumer to act on their behalf.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

Article 5. Special Rules Regarding Minors

§ 999.330. Minors Under 13 Years of Age

- (a) Process for Opting-In to Sale of Personal Information

Commented [SLD(6)]: In the alternative, the AG's office should provide more detailed guidance on the minimum level of proof a business should obtain regarding agent authorization and an express safe harbor for businesses that meet that level of proof. The concern here is that the current regulations provide inadequate guidance for businesses to follow and thereby could subject consumers' privacy to risks.

- (1) A business that has actual knowledge that it collects or maintains the personal information of children under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. This affirmative authorization is in addition to any verifiable parental consent required under the Children’s Online Privacy Protection Act, 15 U.S.C. sections 6501, *et seq.*
- (2) Methods that are reasonably calculated to ensure that the person providing consent is the child’s parent or guardian include:
 - a. Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;
 - b. Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;
 - c. Having a parent or guardian call a toll-free telephone number staffed by trained personnel;
 - d. Having a parent or guardian connect to trained personnel via video-conference;
 - e. Having a parent or guardian communicate in person with trained personnel; ~~and~~
f. Verifying a parent or guardian’s identity by checking a form of government-issued identification against databases of such information, where the parent or guardian’s identification is deleted by the business from its records promptly after such verification is complete and;
f.g. Any other method permitted by the Children’s Online Privacy Protection Act (COPPA).

- (b) When a business receives an affirmative authorization pursuant to subsection (a) of this section, the business shall inform the parent or guardian of the right to opt-out at a later date and of the process for doing so on behalf of their child pursuant to section 999.315.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, and 1798.185(a)(6), Civil Code.

§ 999.331. Minors 13 to 16 Years of Age

- (a) A business that has actual knowledge that it collects or maintains the personal information of minors at least 13 and less than 16 years of age, and wishes to sell such personal information, shall establish, document, and comply with a reasonable process for allowing such minors to opt-in to the sale of their personal information, pursuant to section 999.316.
- (b) When a business receives a request to opt-in to the sale of personal information from a minor at least 13 and less than 16 years of age, the business shall inform the minor of the right to opt-out at a later date and of the process for doing so pursuant to section 999.315.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, and 1798.185, Civil Code.

§ 999.332. Notices to Minors Under 16 Years of Age

- (a) A business subject to section 999.330 and 999.331 shall include a description of the processes set forth in those sections in its privacy policy.
- (b) A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell the personal information of such minors without their affirmative authorization, or the affirmative authorization of their parent or guardian for minors under 13 years of age, is not required to provide the notice of right to opt-out.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, and 1798.185, Civil Code.

Article 6. Non-Discrimination

§ 999.336. Discriminatory Practices

- (a) A financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations.

(b) Notwithstanding subsection (a) of this section, a business may offer a price or service difference if it is reasonably related to the value provided to the business by the consumer's data of the consumer's data as that term is defined in section 999.337.

~~(c)~~ A business may require (1) instruction directly from the consumer regarding agent authorization; (2) the agent to make requests only after accessing the consumer's account; and (3) return personal information only through the consumer's account (rather than to the agent directly).

~~(d)~~ Illustrative examples follow:

(1) *Example 1:* A music streaming business offers a free service and a premium service that costs \$5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale of their personal information, then the practice is discriminatory, unless the \$5 per month payment is reasonably related to the value of the consumer's data to the business.

~~(2) *Example 2:* A retail store offers discounted prices to consumers who sign up to be on their mailing list. If the consumer on the mailing list can continue to receive discounted prices even after they have made a request to know, request to delete, and/or request to opt out, the differing price level is not discriminatory.~~

~~(e)~~ A business's denial of a consumer's request to know, request to delete, or request to opt-out for reasons permitted by the CCPA or these regulations shall not be considered

discriminatory.

~~(e)(f)~~ A business shall notify consumers of any financial incentive or price or service difference subject to Civil Code section 1798.125 that it offers in accordance with section 999.307.

~~(f)(g)~~ A business's charging of a reasonable fee pursuant to Civil Code section 1798.145(g)(3) shall not be considered a financial incentive subject to these regulations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130, and 1798.185, Civil Code.

§ 999.337. Calculating the Value of Consumer Data

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

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130, and 1798.185, Civil Code.

Article 7. Severability

Commented [SLD(7): In the alternative, align language with CCPA 1798.125 such that this section reads "reasonably related to the value provided to the business by the consumer's data."

Formatted: Indent: Left: 0.77", No bullets or numbering

§ 999.341.

- (a) If any article, section, subsection, sentence, clause or phrase of these regulations contained in this Chapter is for any reason held to be unconstitutional, contrary to statute, exceeding the authority of the Attorney General, or otherwise inoperative, such decision shall not affect the validity of the remaining portion of these regulations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.145, 1798.185, and 1798.196, Civil Code.

Message

From: Kevin Gould [REDACTED]
Sent: 12/6/2019 9:37:05 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: California Consumer Privacy Act of 2018 -- Proposed Rulemaking Comment Letter
Attachments: California Consumer Privacy Act of 2018 Proposed Rulemaking Comment Letter.pdf

Thank you for the opportunity to provide written comments during the proposed rulemaking pertaining to the California Consumer Privacy Act of 2018. Please find attached a comment letter prepared by the American Bankers Association, the California Bankers Association, the California Mortgage Bankers Association, and the Mortgage Bankers Association. Please let us know if you have any questions. Thank you.



Kevin Gould
SVP, Director of Government Relations
California Bankers Association
1303 J Street, Suite 600 | Sacramento, CA 95814
[REDACTED]
Connect: [Website](#) | [Twitter](#) | [LinkedIn](#)



December 6, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

RE: California Consumer Privacy Act of 2018 – Proposed Rulemaking Comment Letter

Dear Attorney General Xavier Becerra:

The American Bankers Association (ABA), the California Bankers Association (CBA), the California Mortgage Bankers Association (California MBA), and the Mortgage Bankers Association (MBA) appreciate the opportunity to submit written comments in response to the proposed rulemaking undertaken by the California Department of Justice pertaining to the California Consumer Privacy Act of 2018 (CCPA).

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

CBA is a division of the Western Bankers Association, one of the largest banking trade associations and regional educational organizations in the United States. CBA advocates on legislative, regulatory and legal matters on behalf of banks doing business in the state of California.

California MBA is a California corporation operating as a non-profit association that serves members of the real estate finance industry doing business in California. California MBA's membership consists of approximately three hundred companies representing a full spectrum of residential and commercial lenders, servicers, brokers, and a broad range of industry service providers.

The Mortgage Bankers Association is the national association representing the real estate finance industry, an industry that employs more than 280,000 people in virtually every community in the country. Headquartered in Washington, DC, the association works to ensure the continued strength of the nation's residential and commercial real estate markets; to expand homeownership; and to extend access to affordable housing to all Americans. MBA promotes fair and ethical lending practices and fosters professional excellence among real estate finance employees through a wide range of educational programs and a variety of publications. Its membership of over 2,200 companies includes all elements of real estate finance: mortgage companies, mortgage brokers, commercial banks, thrifts, REITs, Wall Street conduits, life insurance companies, and others in the mortgage lending field.

As your office prepares to issue final regulations in accordance with the CCPA, we respectfully urge that you consider the following requests to clarify aspects of the proposed regulations and the CCPA. These requests should not be considered an effort to undermine the CCPA but rather they are intended to assist in clarifying aspects of the law as a means to enhance compliance for financial institutions.

ARTICLE 2: NOTICES TO CONSUMERS. (SECTIONS 999.305-999.308).

➤ **Notice at Collection of Personal Information. (Section 999.305).**

Section 999.305(a)(3) of the draft regulations requires explicit consent to use a consumer's personal information for a purpose that was not specifically included in the required notice provided to the consumer at the time of collection. Pursuant to Civil Code Section 1798.100(b) of the CCPA, the only requirement in these scenarios is to deliver another notice that is compliant with the same notice to provide a consumer when information is first collected. As such, there is no additional statutory requirement that the business obtain the explicit consent from the consumer, as now required in the proposed rule.

Accordingly, we believe that this provision impermissibly amends the statute in place of implementing the intent of the Legislature. Moreover, this requirement creates a conflict between the statute and the regulations. A financial institution that provides notice consistent with the requirements of the law may nonetheless be charged with violating the statute because the regulations provide that a "violation of these regulations shall constitute a violation of the CCPA, and be subject to the remedies provided for therein." Given that this concept of obtaining explicit consent for the use of a consumer's personal information for a new purpose goes beyond the text of the CCPA, we request that it be removed.

➤ **Notice of Right to Opt-Out of Sale of Personal Information. (Section 999.306).**

Section 999.306(d)(2) requires businesses to treat as an opt-out any collection of personal information where a "Do Not Sell My Personal Information" button is not present. Under Civil Code Section 1798.100, a business must notify consumers of the purposes for which their

and the personal information that the business disclosed for a business purpose. Further, as it relates to personal information that is sold, Civil Code Section 1798.115(a)(2) states specifically, that the business must disclose “the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.” This different treatment is a logical consequence of the fact that the statute gives consumers the right to opt-out of sale. A consumer exercising that right has an interest in knowing which information is sold to which third party. Because there is no right to opt-out of the collection or sharing of personal information for a business purpose, a lower level of granularity will provide a less complex and more meaningful disclosure to the consumer.

ARTICLE 3: BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS. (SECTIONS 999.312-999.318).

➤ **Responding to Requests to Know and Requests to Delete. (Sections 999.313).**

Section 999.313(c)(5) requires that a business must specifically disclose the basis for denying a request to know or a request to delete if the denial was based on a conflict with federal or state laws or an exception to the CCPA. This is understandable. However, Section 999.313(d)(6)(c), applicable to a denial of a request to delete, provides that the business is not permitted to use the consumer’s personal information for any other purpose than provided for by that exception. This restriction improperly prevents a business from using the consumer’s personal information for other lawful purposes including fighting fraud or even completing a consumer’s transaction if that reason was not included in the denial letter. Accordingly, we request that these provisions be removed from the regulation.

Section 999.313(d)(1) requires that where a business cannot verify the identity of a requester seeking deletion, the business shall instead treat the request as a request to opt-out of the business selling the consumer’s personal information. This form of automatic opt-out is inconsistent with the CCPA and could have the unintended consequence of opting out consumers who do not wish to opt-out of sales. Further, if the request is not from the named consumer, such a requirement could lead to businesses opting out the wrong consumer infringing on the rights of consumers who have not chosen to opt-out from a sale.

The CCPA goes into great length to explain and reiterate that the consumer’s right to opt-out requires an affirmative act by the consumer. Examples of the law’s intent may be found in Civil Code Sections 1798.120 and 1798.135. If a requestor’s identity cannot be verified, all that should be required is notifying the requestor, stating that more information is needed for verification. Since this provision in the proposed regulation is inconsistent with the corresponding provision in the CCPA and since consumers are adequately protected by existing law, we request that this provision be removed from the regulations.

Section 999.313(d)(2) provides three methods of complying with a consumer's request to delete their personal information: permanently and completely erasing, de-identifying, and aggregating. In complying with Section 999.313(d)(4), a business apparently must specify the manner in which it has deleted personal information by identifying one of these three methods. This requirement is burdensome, confusing, and irrelevant to consumers and we request that it be removed.

➤ **Requests to Opt-Out. (Section 999.315).**

Section 999.315(e) requires that a business must act on a consumer's request to opt-out of the sale of their personal information in no more than 15 days. This period of time is significantly less than the time period provided to a business responding to a request to know or delete (45 days). Where a consumer makes an opt-out request, particularly a consumer who has authorized another person to opt-out of sale on their behalf, this proposed 15-day deadline fails to provide sufficient time to confirm that the individual making the request has the proper authorization. We request that this provision be removed or the time extended to 45 days.

Section 999.315(f) requires a business to (i) notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the opt-out request, (ii) instruct them not to further sell the information, and (iii) notify the consumer when this has been completed. This requirement is inconsistent with the corresponding provisions in CCPA, wherein a business is only required to cease selling the information it has collected from the consumer. There is no corresponding provision in the CCPA that the business takes further action and notify all third parties in this regard. Since this provision in the regulation is inconsistent with the corresponding provision in CCPA and given that consumers are adequately protected by existing law, we request that this section be removed from the regulations.

Proposed regulations have introduced a new method for a consumer to opt-out that is not included in the CCPA. The concept of "user-enabled privacy controls" in Section 999.315(g) is entirely new. In this regard, the regulations recognize the use of "user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information..." This new requirement is inconsistent with the CCPA.

Existing law has established robust provisions on how a business must message the consumer's right to opt-out and provides acceptable methods to evidence the consumer's intent to opt-out. Moreover, there has been no opportunity to assess the meaningfulness of this concept or the value that this may offer to consumers. In addition, businesses may not be able to comply with this new requirement if there is no technological capability to track or respond to such browser plugins or similar mechanisms.

Since this provision in the regulation is inconsistent with the corresponding provision in CCPA and given that consumers are adequately protected by existing law, we request that this provision be removed from the regulations. In the alternative, we request that the effective date of this provision be delayed, thereby allowing businesses the opportunity to investigate the current technological status of the functionality of user-enabled controls, and an opportunity to make adjustments to ensure they can comply with the provision.

➤ **Training: Record-Keeping. (Section 999.317).**

Section 999.317(g) of the proposed regulations expand record-keeping obligations for businesses that buy, receive, sell or share the personal information of four million or more consumers. For companies who meet this threshold, the regulation requires releasing consumer request metrics in the business's privacy policy or posted on their website. This mandate is not derived from the existing law and does not benefit consumers. Nor do the regulations provide any guidance relating to the calculation of the four million consumers.

We urge that this provision be removed from the regulations or alternatively that these metrics not be released publicly in privacy policies, but instead be provided to your office upon request. Should this provision remain, the regulations should clarify that businesses are required to calculate the 4 million threshold and compile metrics based on consumers who have the right to make requests under the CCPA. Including consumers who are not eligible to make requests, as a result of existing CCPA exemptions, skews the results in a manner that would make the results meaningless.

➤ **Requests to Access or Delete Household Information. (Section 999.318).**

While the draft regulations in Section 999.318 attempt to offer guidance with respect to requests to know or delete personal information for "households," we remain concerned with these requirements.

While we support the clarification that a business may comply with an individual request for household personal information by providing only aggregate personal information, if the requestor does not have a password protected account, the proposed regulations still expose individuals to the release or deletion of their personal information without their knowledge and consent. Aggregation is helpful but is not sufficient to protect people if the household consists of only two or three people.

Moreover, the proposed regulations do not address how the business should respond if the requestor has a password protected account. The implication is that if the requestor has a password protected account, the business must provide the household personal information to the requestor, or delete household personal information. Likewise, we believe it is virtually impossible for a financial institution to determine whether all members of a household jointly request access or deletion, without a level of investigation into a particular household that

would be extraordinarily burdensome—if not impossible. Our members are concerned about the transient nature of households – spouses may separate, or adult children may return or leave the household – and there is no practical method for a financial institution to determine the makeup of the household when a request is received.

For these reasons, we urge the deletion of “household” from the definition of “personal information.” We believe the unauthorized disclosure or deletion of personal information by one household member is an unintended consequence of the CCPA.

If the final rule does not delete “household” from the definition of personal information or otherwise exempt businesses from disclosing personal information or deleting personal information for a household, we respectfully request that the final rule create a safe harbor from liability if the business follows the procedures in the final regulation regarding verification of requests for access to or deletion of household personal information.

We would further request additional clarity as to the aggregate data that must be provided to the requesting household. It seems that the household information to be disclosed pursuant to this provision is that which applies to, and subject to inspection by, the household as a whole. It is not intended to include specific categories or pieces of information pertaining to a specific individual consumer residing in that household.

ARTICLE 4: VERIFICATION OF REQUESTS. (SECTIONS 999.323-999.326).

- **Provide additional clarity around what is necessary, and what will be deemed in compliance, when authenticating a verifiable consumer request and include a safe harbor. (Sections 999.323-999.325).**

As part of routine transactions with consumers, financial institutions collect personal information in order to facilitate customer requests. Furnishing personal information to consumers purporting to exercise their rights under the CCPA, in response to a verifiable consumer request, may result in unintended risk and harm to the consumer, including misuse of personal information to perpetrate fraud and identity theft.

A business receiving a consumer’s request will need sufficient data from the consumer as a safeguard to ensure the information provided in return is associated with the requesting individual. Regulations established by the Attorney General should provide flexibility for a business to decline a consumer’s request where the data presented by the consumer is insufficient to authenticate a request. Further, in circumstances where limited information is provided by the consumer, a business endeavoring to authenticate a request should have flexibility, but not be required, to furnish non-sensitive personal information (excluding personal information that if disclosed would otherwise result in a data breach) to the consumer as a means to satisfy its compliance and to protect the consumer against fraud and identity theft.

- **Affirm that the CCPA does not apply to a covered entity's intellectual property and that a business is not required to reveal data infringing on the rights of others.**

In subdivision (a)(3) of Section 1798.185, the CCPA grants the Attorney General 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."

In this regard, we urge rulemaking that establishes an exception from the Act for intellectual property or for data that, if disclosed, would have an adverse effect on the rights or freedoms of others. The CCPA should not apply to information that is the protected intellectual property of a business, including information subject to copyright, patent, service mark and/or trade secret protections. A business should not be required to disclose 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, or any information derived from such process or analysis.

In considering this request, your office may wish to consider the approach taken in the European General Data Protection Regulation (GDPR) which places reasonable limitations on the consumer privacy right it grants. Both the intellectual property exclusion and the avoidance of infringement on the rights of others are embedded in the GDPR. We believe that there should be similar recognition in the CCPA of circumstances where a business' attempt to comply with a consumer's request would place it in the position of violating the rights of others or placing it in jeopardy with its competitors.

Given the authority granted to your office pursuant to subdivision (a)(3) of Section 1798.185, we request that the final regulations affirm that intellectual property should not be disclosed in response to a verifiable consumer request.

- **Grant an 18-month delayed effective date with respect to the regulations.**

We urge your office to specify a later effective date for the regulations, such as 18 months after the final regulations are issued. When the CCPA was enacted, businesses were granted 18 months from the legislation's passage to its effective date. This period of time was granted recognizing the complexity of the CCPA, the potential for additional statutory revisions given the speed for which the CCPA was advanced through the Legislature, and was an acknowledgment of the time necessary for businesses to develop compliance protocols to implement the statutory provisions.

Financial institutions have been actively engaged in due diligence and establishing policies and procedures for compliance with the CCPA. The regulations will require financial institutions to re-evaluate their policies and procedures and adapt where necessary. In order to revise any

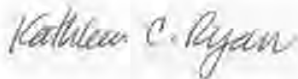
policies and procedures, financial institutions will require additional time to establish and test compliance procedures.

The authority for such as action may be found in Government Code section 11343.4(b)(2). That section provides that the agency issuing regulations can specify an effective date. In furtherance of this request, Section 11343.4(b)(1)'s limitations on an agency's ability to specify an effective date does not apply and that limitation only applies when the statute specifies an effective date.

Since the CCPA does not specify an effective date for the regulations and simply specifies that regulations should be adopted by July 1, 2020, with no reference to an effective date, we request an effective date for the regulations of no earlier than January 1, 2022.

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

Sincerely,



Kathleen C. Ryan
Vice President and Senior Counsel
American Bankers Association



Kevin Gould
SVP/Director of Government Relations
California Bankers Association



Susan Milazzo
Chief Executive Officer
California Mortgage Bankers Association



Pete Mills
Senior Vice President, Residential Policy &
Member Engagement
Mortgage Bankers Association



December 6, 2019

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

Dear Attorney General Becerra,

The protection of the free press is enshrined in the First Amendment to the U.S. Constitution. More than 120 million adults read a daily or Sunday print newspaper. The free press is on the front lines helping the American people hold accountable those who hold positions of power within our democracy and around the world. Digital advertising is a significant source of revenue to media outlets, large and small, and helps keep the press free from government control and affordable. With a well-designed privacy law, the press can continue to do its job as intended in the U.S. Constitution, and consumers can continue to have access to cost-efficient news sources and control of the use and exchange of their personal information.

The News Media Alliance (the “Alliance”) represents over 2,000 media outlets and is composed of nationally recognized organizations, international organizations, and hyperlocal organizations. The Attorney General’s proposed Regulations promulgated pursuant to the California Consumer Privacy Act (“CCPA”), while helpful on a number of levels, impose certain additional burdens on publishers that will render compliance difficult and provide no added benefit to consumers. Indeed, the Regulations may further confuse and convolute consumer control over personal information.

The Alliance believes in giving consumers more transparency and control regarding the use and collection of personal data. In an effort to be more fully compliant with the CCPA and the Regulations and to protect consumer personal information, the Alliance, joined by the California Newspaper Publishers Association, respectfully submits the following comments.

I. The Attorney General Should Clarify the New “Notice at Collection” Requirement.

Section 999.305 imposes new obligations on businesses to make additional disclosures above and beyond the privacy policy when collecting personal information. These new obligations are unclear with respect to what needs to be disclosed, and how, where, and when the notice should be appear.

A. The Attorney General Should Not Require the Posting of a “Notice at Collection” Until January 1, 2021.

The “notice at collection” is a new obligation set forth in the Regulations that is not required by the statute. While the CCPA goes into effect January 1, 2020, the anticipated effective date for the Regulations is sometime before July 1, 2020. The notice at collection obligations were revealed less than three months before the law’s effective date, and they are ambiguous and need clarification.

Because the notice at collection is a new obligation and consumers are likely to see inconsistent implementations that only create confusion, rather than transparency, the Attorney General should clarify that the notice at collection obligation is not effective until January 1, 2021.

B. The Attorney General Should Clarify the Required Placement of the “Notice at Collection.”

The Regulations provide:

The notice [at collection] shall “use a format that draws the consumer’s attention to the notice and makes the notice readable, including on smaller screens, if applicable.”¹

Because this is a new obligation and because other requirements such as the “Do Not Sell My Personal Information” button more clearly indicate where and how they should be presented to the consumer, it is difficult for businesses to understand, operationally, how the “notice at collection” should appear and where it should be placed. To remain consistent with existing consumer expectations, the Attorney General should permit businesses to use a link that conspicuously alerts California consumers of the notice on the homepage by being in close proximity to the existing privacy policy link in the website footer or mobile app menu.

C. The Attorney General Should Eliminate Inconsistent Language Regarding the Point in Time When Consumers Must See the “Notice at Collection.”

The Regulations provide:

The notice [at collection] shall...Be visible or accessible where consumers will see it before any personal information is collected.²

This subdivision is inconsistent with the statute³ and even other portions of the Regulations⁴ that permit disclosures regarding privacy practices to happen **at or before** the time of collection.

¹ 11 CCR §999.305(a)(2)(b).

² 11 CCR §999.305(a)(2)(e).

³ CIV. CODE §1798.100(b). “A business that collects a consumer’s personal information shall, *at or before* the point of collection, inform consumers as to the categories of personal

The Attorney General should revise §999.305(a)(2)(e) to be consistent with the CCPA and the other language in the Regulations and provide that the “notice at collection” can be provided **at or before** the time of collection.

II. The Attorney General Should Provide Further Clarification on How to Properly Post the Notice at Collection, Privacy Policy, and “Do Not Sell My Personal Information” Links on Mobile Applications.

The Regulations provide that the notice at collection,⁵ the privacy policy,⁶ and the “Do Not Sell My Personal Information”⁷ links must be conspicuously posted on the mobile application’s download or landing page.

From an operational standpoint, this is problematic because many mobile applications do not have footers, as is the case with actual websites viewed on a device. Often times, the links to the privacy policy and other applicable notices are found in a hamburger menu or gearbox, which consumers have come to associate with being a location for important additional information.

The Alliance requests that the Attorney General clarify that posting the notice at collection, the privacy policy, and the “Do Not Sell My Personal Information” links in the application’s hamburger menu or gearbox will be deemed conspicuous for purposes of by the Regulations.

information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.” (*emphasis added*).

⁴ 11 CCR §999.301(i). “‘Notice at Collection’ means the notice given by a business to a consumer *at or before* the time a business collects personal information from the consumer as required by Civil Code section 1798.100(b) and specified in these regulations.” (*emphasis added*). *See also* 11 CCR §999.305(a)(5) (“If a business does not give the notice at collection to the consumer *at or before* the collection of their personal information, the business shall not collect personal information from the consumer”) (*emphasis added*).

⁵ 11 CCR §999.305(a)(2)(e). “The notice shall...[b]e visible or accessible where consumers will see it before any personal information is collected. For example, when a business collects consumers’ personal information online, it may conspicuously post a link to the notice on the business’s website homepage or the mobile application’s download page, or on all webpages where personal information is collected.”

⁶ 11 CCR §999.308(a)(3). “The privacy policy shall be posted online through a conspicuous link using the word ‘privacy,’ on the business’s website homepage or on the download or landing page of a mobile application.”

⁷ 11 CCR §999.315(a). “A business shall provide two or more designated methods for submitting requests to opt-out, including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled ‘Do Not Sell My Personal Information,’ or ‘Do Not Sell My Info,’ on the business’s website or mobile application.”

III. The Attorney General Should Not Require a Notice of Right to Opt-Out of Sale of Personal Information for Businesses Not Currently Selling Personal Information.

The Regulations provide:

The purpose of the notice of right to opt-out of sale of personal information is to inform consumers of their right to direct a business that sells (*or may in the future sell*) their personal information to stop selling their personal information, and to refrain from doing so in the future.⁸

The emphasized portion of this subdivision implies that even businesses that do not currently sell personal information, but may possibly sell personal information in the future, are also required to provide a notice of right to opt-out of sale of personal information. This is inconsistent with the CCPA itself,⁹ which only requires businesses that are currently selling personal information to provide the notice of opt-out of sale of personal information.

The Alliance strongly recommends the Attorney General remove “or may in the future sell” from §999.306(a)(1) of the Regulations in order to avoid consumer confusion. The purpose of the CCPA is to provide transparency with respect to company practices regarding the collection, use, and disclosure of consumer personal information. If any business that does not currently sell personal information but that might theoretically sell personal information in the future is required to provide an opt-out notice, a consumer will never be sure, from the moment that consumer visits a website or sees the notice in a store, whether or not a site is selling personal information.

IV. The Regulations Should Not Require Businesses to Treat Unverified Requests to Delete as Requests to Opt-Out of Sale of Personal Information.

The Regulations provide:

For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified and shall instead treat the request as a request to opt-out of sale.¹⁰

⁸ 11 CCR §999.306(a)(1) (*emphasis added*).

⁹ CIV. CODE §1798.120(b). “A business that sells consumers’ personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the ‘right to opt-out’ of the sale of their personal information.”

¹⁰ 11 CCR §999.313(d)(1)

This new requirement (not found in the statute) to treat an unverified request to delete as a request to opt-out of sale is problematic on multiple levels, most obviously in situations where a business is not selling personal information in the first place, and in situations where the business does not have sufficient information to identify the consumer. There is also a major concern that businesses will be flooded with unverified deletion requests by simply taking names from a telephone book and inputting them into the request for deletion form, or by using an automated bot. The Attorney General should eliminate this requirement.

V. The Attorney General Should Support the Development of Industry Frameworks for a Consistent Opt-Out Approach Under the CCPA And Provide Time for Organizations to Implement Those Frameworks.

Many members of the Alliance are hyperlocal news organizations that cannot afford to build their own opt-out solutions for the CCPA. These businesses welcome the efforts of self-regulatory groups that have been working, across the advertising ecosystem, to develop proposed frameworks to support and facilitate consumer opt-out rights.¹¹ The Attorney General should support these industry efforts and provide additional time for organizations that choose to participate therein to implement those technical specifications.

The BEAR Study included in the Attorney General’s Initial Statement of Reasons points out that the costs associated with developing technological systems to meet the compliance standards of the CCPA are likely to be significant. Even the largest data owners in the world are struggling to figure out how to make the “Do Not Sell My Personal Information” button operational on their platforms, with no long-term viable solution in sight.

Members of the Alliance and others in the advertising ecosystem are engaged in a significant good-faith effort to comply with the CCPA. Given this new legal regime, and the challenges of implementing the opt-out requirements in the ad tech space, the Alliance asks the Attorney General to set forth a compliance grace period for such implementation, up to and including January 1, 2021.

VI. The Attorney General Should Not Restrict a Service Provider’s Ability to Use Information Collected from One Business to Benefit Another Business.

The Regulations provide:

A service provider shall not use personal information received either from a person or entity it services or from a consumer’s direct interaction with the service provider for the purpose of providing service to another person or entity.¹²

¹¹ See, e.g., *IAB CCPA Compliance Framework for Publishers and Technology Companies* (available at <https://www.iab.com/guidelines/ccpa-framework/>).

¹² 11 CCR §999.314(c).

This provision would have severe negative implications for publishers' ability to use any service provider that provides analytic services. Many technology service providers use a single piece of information such as an IP address, received from multiple businesses, to provide services to many different businesses. For example, frequency capping or sequencing functions are extremely helpful to consumers because they limit the number of times consumers see the same ad. Service providers are only able to bring this benefit to consumers if they are able to take information they receive from several businesses and use that information collectively. Another example is Google Analytics. Google Analytics provides a service that allows businesses to track consumer traffic on their websites and mobile applications. It provides insight as to how consumers landed on their website, what consumers did once they were on the website, and how long they stayed on the website. Google Analytics uses all this information from various businesses to provide businesses with online marketing plans that allow them to track and gauge their return on investment in a meaningful way when the Advertising Feature is turned on.

The Alliance recommends the following revised provision:

A service provider shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose of providing services to another person or entity, **unless the service provider is using the information solely for business purposes and provided those business purposes are disclosed to consumers when responding to requests to know.**

VII. Businesses that Honor Opt-Out Requests Through a "Do Not Sell My Personal Information" Link Should Not Also be Required to Treat the Ad Hoc Use of User-Enabled Privacy Controls as "Do Not Sell" Requests.

The Regulations provide:

If a business collects personal information from consumers online, the business shall treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.¹³

Given the existing requirement that businesses selling personal information include a "Do Not Sell My Personal Information" button on the homepage with direct access to methods to opt-out of the sale of personal information, adding user-enabled privacy controls as another method only exacerbates the complexity facing consumers as they seek to opt-out of sale of personal information. Without a clear delineation between an opt-out of sale and existing user-enabled privacy controls, a consumer may feel he or she must enable and disable privacy-setting controls prior to and after each visit to any number of websites through which he or she does want to

¹³ 11 CCR §999.315(c).

allow the businesses to sell their personal information. This is not the experience consumers want and it does not provide further transparency or control.

Further, under the Regulations as drafted, a business will not know how to reconcile a consumer's use of user-enabled privacy controls with a consumer's action or inaction vis-a-vis a "Do Not Sell" button. In addition, in this scenario, a business has no way to contact a consumer to confirm that it contacted all third parties to which it sold data in the previous 90 days.¹⁴ And if a consumer uses specific user-enabled controls, rather than a global opt-out, a business has no mechanism for contacting the consumer to provide the option to globally opt-out.¹⁵

Additionally, there are currently no standards for "Do Not Track" or other possible browser plug-ins. Requiring publishers to follow various standards created every day is an impossible burden with which small and large publishers will not be able to comply, but which unfairly enhances the power of browser manufacturers.

The Alliance recommends that the Attorney General remove the references to user-enabled privacy controls from the Regulations as they are unnecessary, provide no additional transparency for consumers, and impose undue burdens on businesses.

VIII. The 90-Day Lookback Requirement Exceeds the Scope of the Attorney General's Rulemaking Authority and Should be Eliminated.

The Regulations provide:

A business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the consumer's request that the consumer has exercised their right to opt-out and instruct them not to further sell the information. The business shall notify the consumer when this has been completed.

This proposed regulation is problematic for two reasons. First, it would require retroactive application to information collected up to 90 days before the effective date of the CCPA. Second, it would also require retroactive application generally of the do not sell obligation and thereby exceed the scope of the Attorney General's power to regulate. "New statutes are presumed to operate only prospectively absent some clear indication that the Legislature intended otherwise." *Elsner v. Uveges*, 34 Cal. 4th 915, 936 (2004). Here, there is no clear indication that the Legislature intended the do not sell obligation to apply retroactively. Moreover, the statute only requires a prospective obligation on businesses that honor do not sell requests.¹⁶

¹⁴ 11 CCR §999.315(f).

¹⁵ 11 CCR §999.315(d).

¹⁶ CIV. CODE 1798.135(a)(4) and (5). "For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer...[and] respect the consumer's decision to opt-out for at least 12

In order to avoid any retroactive application of the CCPA, the 90-day lookback should be eliminated.

IX. Businesses Should Have 45 Days from the Date a Request to Know or a Request to Delete is Verified to Fulfill or Deny that Request.

The Regulations provide:

Businesses shall respond to requests to know and requests to delete within 45 days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request.¹⁷

There are a number of verification requirements that must be followed for both requests to know and requests to delete. Because of the extensive nature of these requirements, it is clear that each request will need to be verified on a case-by-case basis.¹⁸

The Alliance recommends that the Regulations be revised such that the 45-day window to substantively respond to requests to delete and requests to know begins to run on the day the request is verified.

X. The Attorney General Should Not Require Publication of Metrics in the Privacy Policy for Businesses That Are Required to Maintain Consumer Request Metrics.

The Attorney General has proposed explicit metrics reporting requirements for businesses “that alone or in combination, annually buy[], receive[] for the business’s commercial purposes, sell[], or share[] for commercial purposes, the personal information of 4,000,000 or more consumers.”¹⁹

While the record-keeping requirements are sensible, publication of such metrics is more likely to confuse consumers, particularly if businesses are denying large volumes of frivolous or even fraudulent requests. The numbers themselves will not elucidate for consumers the underlying reasons for the denial, and will only further extend the length of already lengthy privacy policies.

The Alliance would strongly recommend that the Attorney General strike Section 999.317(g)(2) from the Regulations to remove the obligation to post the metrics publicly, and instead require that businesses in this category maintain such records internally and make them available to the Attorney General upon request.

months before requesting that the consumer authorize the sale of the consumer’s personal information.”

¹⁷ 11 CCR §999.313(b).

¹⁸ See generally 11 CCR §§ 999.323-999.326.

¹⁹ 11 CCR §999.317(g).

XI. The Attorney General Should Provide Clarity on How Businesses Should Operationalize the Obligation to Provide Aggregated Household Data in Response to Household Requests for Personal Information.

The Regulations provide:

Where a consumer does not have a password-protected account with a business, a business may respond to a request to know or request to delete as it pertains to household personal information by providing aggregate household information, subject to verification requirements set forth in Article 4.²⁰

The average household size is 2.6 people.²¹ It is unclear how any business could provide household information on an aggregated basis for 2.6 people. It is fundamentally inconsistent with the language and the spirit of the CCPA.

In addition, it is unclear whether “household” means any household in the United States or if it is restricted to requests that come from households located in California.

As numerous businesses have pointed out to the legislature and to the Attorney General, allowing one member of a household to obtain information about other individuals in the household – even in “aggregated” form – actually puts the privacy and safety of those household members at risk. The Attorney General should remove subsection (a) and instead require that all consumers of a household jointly request information (as provided in subsection (b)). In the alternative, if the Attorney General is not inclined to remove subsection (a), the Alliance strongly encourages the Attorney General to provide businesses who comply with subsection (a) a safe harbor in the event of a data breach regarding such household information.

The Attorney General should also make clear that this provision of the Regulations is intended to include only those requests received from households located in California.

XII. The Attorney General Should Provide Additional Guidance on the Two Steps Required for Opt-In for Minors, Opting-In After Opting-Out, and Requests to Delete.

The Regulations provide:

For consumers 13 years and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.²²

²⁰ 11 CCR §999.318(a).

²¹ Pew Research on the Increase in Household Size available at <https://www.pewresearch.org/fact-tank/2019/10/01/the-number-of-people-in-the-average-u-s-household-is-going-up-for-the-first-time-in-over-160-years/>

²² 11 CCR §999.301(a).

A business shall use a two-step process for online requests to delete where the consumer must first, clearly submit the request to delete and then second, separately confirm that they want their personal information deleted.²³

Requests to opt-in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.²⁴

This is a new obligation that does not appear in the statute and it lacks substantial compliance guidance. The Attorney General should use this opportunity to provide, at a minimum, examples of sufficient two-step opt-ins. The Alliance provides the following examples of what might be sufficient for purposes of two-step verification:

Example 1: If a business is responding to a verified request to delete via the toll-free number method, the business may ask the consumer to provide an email address. The business will then send a confirmation email to that account for the consumer to confirm they would like their personal information deleted.

Example 2: If a business receives an opt-in request from a minor between 13 and 16 years old via a webform, the business may give the minor an email with a deep link to click onto verify that they would like to opt-in to the sale of personal information.

Example 3: If a business receives a request to opt-in after opting-out via a webform, the business may give the consumer two separate screens – first filling out a request on a webform, and second clicking on a button on a confirmation page that states “confirm my request.”

XIII. The Attorney General Should Provide Guidance on How a Business Can Conclude that Any Given Visitor is a California Resident.

The CCPA and Regulations are both silent regarding how a business determines whether a visitor to a website is a California resident and therefore has certain rights under the CCPA.

The Alliance requests that the Attorney General provide businesses with the ability to use a website visitor’s IP address to determine if such visitor is a California consumer.

²³ 11 CCR §999.312(d).

²⁴ 11 CCR §999.316(a).

XIV. The Attorney General Should Provide Insight into What Constitutes “Reasonable Security” Measures.

The CCPA and the Regulations set forth obligations on businesses, and consequences associated with failing, to provide either “reasonable security procedures and practices” or “reasonable security measures” regarding the transmission,²⁵ verification,²⁶ and protection of personal information.²⁷ However, the Regulations offer no guidance regarding the appropriate standard for reasonable security measures and/or procedures and practices.

The Alliance strongly recommends the Attorney General explicitly set forth in the Regulations that the Center for Internet Security Controls, set forth in the California Attorney General’s 2016 Data Breach Report,²⁸ constitute the applicable baseline standard for reasonable security under the CCPA and the Regulations.

²⁵ 11 CCR §999.313(c)(6). “A business shall use reasonable security measures when transmitting personal information to the consumer.”

²⁶ 11 CCR §999.323(d). “A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer’s personal information.”

²⁷ CIV. CODE §1798.150(a)(1). “Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following...”

²⁸ *California Data Breach Report*, February 2016, available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>.

XV. The Attorney General Should Offer Regulations on the CCPA Amendments.

Governor Newsom signed additional amendments to the CCPA on October 11, 2019. These included, among other things, a business to business exemption and an employee exemption. Because the amendments were signed after the publication of the Regulations, the Attorney General should promulgate regulations on how to operationalize the above-mentioned exemptions, both of which are scheduled to sunset on January 1, 2021, only six months after the Attorney General begins enforcement of the law.

Sincerely,

A handwritten signature in black ink, appearing to read "David Chavern". The signature is written in a cursive style with a large, looped initial "D" and a smaller "C" that extends to the right.

David Chavern
President & CEO
News Media Alliance

Message

From: Monticollo, Allaire [REDACTED]
Sent: 12/6/2019 8:25:28 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Signorelli, Michael A. [REDACTED]
Subject: Advertising Trade Associations' Joint Submission of Comments on the Proposed CCPA Regulations
Attachments: Joint Ad Trade Comments on Proposed CCPA Regulations.pdf

Dear Attorney General Becerra:

Please find attached joint comments from the following advertising trade associations on the content of the proposed regulations interpreting the California Consumer Privacy Act: the Association of National Advertisers, the American Association of Advertising Agencies, the Interactive Advertising Bureau, the American Advertising Federation, and the Network Advertising Initiative.

If you have any questions, please feel free to reach out to Mike Signorelli at [REDACTED] or by phone at [REDACTED].

Best Regards,
Allie Monticollo

[Allaire Monticollo, Esq. | Venable LLP](#)

[REDACTED]
600 Massachusetts Avenue, NW, Washington, DC 20001

[REDACTED] | www.Venable.com

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



December 6, 2019

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

Dear Attorney General Becerra:

As the nation's leading advertising and marketing trade associations, we provide the following comments to offer input on the California Office of the Attorney General's ("OAG") proposed regulations implementing the California Consumer Privacy Act ("CCPA"). We and our members support the objectives of the CCPA and believe consumers deserve meaningful privacy protections supported by reasonable government policies. However, we have certain concerns about negative consequences the proposed regulations could create for consumers and businesses alike. Additionally, we are concerned that many of the proposed rules' provisions impose entirely new requirements on businesses that are outside of the scope of the CCPA and do not further the purposes of the law.

The undersigned organizations collectively represent thousands of companies in California and across the country, from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies, is responsible for more than 85 percent of the U.S. advertising spend and drives more than 80 percent of our nation's digital advertising spend. Locally, our members help generate some \$767.7 billion dollars for the California economy and support more than 2 million jobs in the state.¹ The companies we represent desire to comply with the CCPA by offering consumers robust privacy protections while simultaneously continuing to be able to do business in ways that benefit California's employment rate and its economy.

We provide the following comments to draw the OAG's attention to certain parts of the proposed regulations that are unsupported by statutory authority and other provisions that may have detrimental consequences for consumers and businesses alike. Below we provide a list of suggested updates to the proposed rules to bring them into conformity with the text of the CCPA and to rectify certain negative results they could cause for consumers and businesses. We also highlight certain provisions in the proposed regulations that we support for providing helpful clarity to the advertising and marketing industry. Some of the undersigned trades will file additional comments to the OAG.

¹ IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at <https://www.ana.net/magazines/show/id/rr-2015-ihs-ad-tax>.



I. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth

Today, the U.S. economy is increasingly fueled by the free flow of data. One driving force in this ecosystem is data-driven advertising. Advertising has helped power the growth of the Internet for decades by delivering innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet's largest players.

As a result of this advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.² Calculating against those figures, the interactive marketing industry contributed \$1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.³

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to create their own platforms to reach millions of other Internet users. Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored experience. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. Indeed, as the FTC noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.⁴ It is in this spirit—preserving the ad supported digital and offline media marketplace while helping to design privacy safeguards—that we provide these comments.

² John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017) <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>.

³ *Id.*

⁴ Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018) https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.



II. The OAG Should Ensure the Proposed Regulations' Definitions Conform with the Text of the CCPA and Are Given Consistent Meaning

Although the OAG has provided definitions for several new terms in the proposed regulations, some of the definitions contradict the text of the CCPA itself and others are used inconsistently throughout the proposed regulations, thereby obscuring the meaning of the defined terms. For example, the OAG defined “request to know” in a way that departs from the text of the CCPA. In addition, the use of the defined term “request to delete” in at least one section of the proposed regulations is at odds with its definition in the proposed regulations as well as the text of the CCPA. We respectfully ask the OAG to update the proposed regulations so that the defined terms conform with the text of the CCPA and are given consistent meaning throughout the entirety of the draft rules.

The OAG defined “request to know” as “a consumer request that a business disclose personal information that it has about the consumer... [including] [s]pecific pieces of personal information that a business has about a consumer...”⁵ This definition differs from the text of the CCPA, which states that “[a] consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer...” the categories and specific pieces of personal information “it has *collected about the consumer*.”⁶ To reduce business and consumer confusion and align the proposed regulations with California legislators’ intent and the text of the CCPA, the OAG should update the proposed rules so a “request to know” is defined as “a consumer request that a business disclose personal information that it has collected about the consumer... [including] [s]pecific pieces of personal information that a business has collected about a consumer.”

In addition, the OAG defined “request to delete” as “a consumer request that a business delete personal information about the consumer that the business has collected from the consumer...”⁷ This definition aligns with the deletion right as it is set forth in the CCPA, which states that “[a] consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.”⁸ However, in the section of the proposed regulations discussing the information that must be included in a privacy policy, the draft regulations note that a business must “[e]xplain that a consumer has a right to request the deletion of their personal information *collected or maintained* by the business.”⁹ The expression of the right to delete in the privacy policy section of the proposed regulations therefore contradicts with the CCPA’s stated expression of the right and the proposed regulations’ defined term “request to delete.” The OAG should update the privacy policy section of the CCPA so it states that a business must explain that consumers have the right

⁵ Cal. Code Regs. tit. 11, § 999.301(n)(1) (proposed Oct. 11, 2019).

⁶ Cal. Civ. Code §§ 1798.110(a)(1), (5) (emphasis added).

⁷ Cal. Code Regs. tit. 11, § 999.301(o) (proposed Oct. 11, 2019).

⁸ Cal. Civ. Code §§ 1798.105(a).

⁹ Cal. Code Regs. tit. 11, § 999.308(b)(2)(a) (proposed Oct. 11, 2019) (emphasis added).



“to request personal information about the consumer that the business has collected from the consumer” to align the section with the defined term “request to delete” and the CCPA.

As described above, we suggest that the OAG take steps to alter certain definitions in the proposed regulations so that they match and support the text of the CCPA and are used consistently throughout the draft rules. Such updates would help create certainty for businesses and consumers and would ensure that the text of the CCPA and the proposed regulations interpreting its terms are not in conflict.

III. Allow Flexibility for Businesses that Do Not Collect Information Directly to Provide Notice of Sale and an Opportunity to Opt Out

The CCPA states that a “third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out....”¹⁰ Through the proposed regulations, the OAG has provided that the business must: (1) contact the consumer directly to provide notice of sale and notice of the right to opt out, or (2) confirm the source provided a notice at collection to the consumer; obtain signed attestations from the source describing how it gave notice at collection, including an example of the notice given to the consumer; retain such attestations and sample notices for two years; and make them available to consumers upon request.¹¹ The OAG should change this provision of the draft rules so businesses are not required to maintain and make available examples of the notice provided to a consumer at the time of collection.

Requiring businesses to maintain sample notices creates a substantial new business obligation that was not contemplated by the legislature when it passed or amended the law. Requiring examples of the notice that was provided to a consumer at the time of collection constitutes a requirement that is beyond the text, scope, and intent of the CCPA, as the law itself only requires a third party to ensure a consumer has received explicit notice of sale and an opportunity to opt out. Second, little if any additional consumer benefit is provided through this new business duty to maintain example notices. The requirement to obtain attestations from data sources confirming that a notice at collection was given and describing how the notice was given provides consumers with the same transparency benefits as requiring businesses to obtain and maintain samples of the notice that was given to consumers.

Finally, mandating that businesses must maintain examples of notices provided to consumers at the time of collection is unreasonable, significantly burdensome, and could place a considerable strain on normal business operations. For example, it is possible the proposed regulations could be interpreted to require businesses to pass example notices from original sources of data to third party businesses who may later receive personal information. This obligation would impose significant new recordkeeping obligations on third party businesses and could stifle the free flow of information that powers the Internet. We therefore ask the OAG to

¹⁰ Cal. Civ. Code § 1798.115(d).

¹¹ Cal. Code Regs. tit. 11, § 999.305(d) (proposed Oct. 11, 2019).



remove the requirement for businesses to obtain examples of the notices at collection that were given to consumers to enable more flexibility for businesses to comply with the requirements the CCPA places on third parties who engage in personal information sale.

IV. Remove the Requirement to Respect Browser Signal Opt Outs so Consumers' Are Provided with Consumer Choice

The draft rules require businesses that collect personal information from consumers online to “treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt out of the sale of their personal information as a valid request...”¹² This requirement is extralegal and goes beyond the text and scope of the CCPA by imposing a substantive new requirement on businesses that was not set forth by the legislature and does not have any textual support in the statute itself. For this reason and others we describe below, we ask the OAG to eliminate this requirement, or, at a minimum, give businesses the option to either honor browser plugins or privacy settings or mechanisms, or decline to honor such settings if the business includes a “Do Not Sell My Personal Information” link and offers another method for consumers to opt out of the sale of personal information.

The browser-based signal requirement in the proposed rules has no textual support in the CCPA itself. The California legislature could have included a browser-based signal mandate when it initially passed the CCPA, or when it amended it via multiple bills thereafter,¹³ but the legislature never chose to impose such a requirement. Moreover, the California legislature already considered imposing a similar browser setting requirement in 2013 when it amended the California Online Privacy Protection Act.¹⁴ The legislature ultimately decided against imposing a single, technical-based solution to enabling consumer choice and instead chose to offer consumers multiple avenues through which they may communicate their preferences. Together, these decisions reveal that the California legislature had the opportunity to enact a browser-based signal requirement on multiple occasions, but never chose to do so, and as such, the proposed regulation mandating that such signals be treated as verifiable consumer requests does not further legislative intent and is outside the scope of the CCPA.

If the OAG ultimately maintains this requirement, we suggest that the OAG modify it so that a business engaged in the sale of personal information must *either* abide by browser plugins or privacy settings or mechanisms, or may not honor such settings if the business includes a “Do Not Sell My Personal Information” link and offers another method for consumers to opt out of personal information sale by the business. The latter approach is more consistent with the spirit of the CCPA and the intentions of the legislature, as it affords consumers with robust choice and control over the sale of personal information. In contrast, browser-based signals or plugins would broadcast a single signal to all businesses opting a consumer out from the entire data

¹² *Id.* at § 999.315(c).

¹³ See AB 1121 (Cal. 2018); AB 25 (Cal. 2019); AB 874 (Cal. 2019); AB 1146 (Cal. 2019); AB 1355 (Cal. 2019); AB 1564 (Cal. 2019).

¹⁴ AB 370 (Cal. 2013).



marketplace. It is not possible through these settings for a consumer to make discrete choices among businesses allowing the consumer to restrict certain businesses while permitting other businesses to transfer data to benefit the consumer. Furthermore, it is not possible for a business to verify if a consumer set the browser setting or some intermediary did so without the authorization of the consumer.

In addition, certain intermediaries in the online ecosystem stand between consumers and businesses and therefore have the ability to interfere with the data-related selections consumers may make through technological choice tools. These intermediaries, such as browsers and operating systems, can impede consumers' ability to exercise choices via the Internet that may block digital technologies (*e.g.*, cookies, javascripts, and device identifiers) that consumers can rely on to communicate their opt out preferences. This result obstructs consumer control over data by inhibiting consumers' ability to communicate preferences directly to particular businesses and express choices in the marketplace. The OAG should by regulation prohibit such intermediaries from interfering in this manner.

We ask the OAG to eliminate the requirement to honor browser plugins or privacy settings or mechanisms, or, alternatively, revise the draft rules so that businesses have the option of honoring such settings or providing a "Do Not Sell My Personal Information" link along with another method for consumers to opt out of the sale of personal information by the business. We also ask the OAG to update the proposed rules to prohibit intermediaries from blocking or otherwise interfering with the technology used to effectuate consumer preferences in order to protect the opt out signals set by consumers via other tools.

V. Enable Effective Opt Out Mechanisms for Businesses that Do Not Maintain Personally Identifiable Personal Information

The proposed regulations require businesses to offer consumers a webform through which they may opt out of the sale of personal information.¹⁵ However, webforms may not work to facilitate opt outs for online businesses that do not maintain personally identifiable information about consumers. Many businesses in the online ecosystem may maintain personal information that does not identify a consumer on its own, for example, IP addresses, mobile advertising identifiers, cookie IDs, and other online identifiers. For businesses that maintain this non-identifying information, webforms may not work to facilitate consumer requests to opt out, because the consumer's submission of identifying information such as a name, email address, or postal address may not be easily matched to the non-personally identifiable information the business does maintain. This provision could undermine the privacy-protective elements of the CCPA by forcing companies to attempt re-identification techniques which are widely avoided by industry in its efforts to enhance consumer privacy.¹⁶ Consequently, the proposed rules should provide businesses with flexibility to offer mechanisms for consumers to opt out of personal information sale. The OAG has indicated it may issue another button or logo to enable a

¹⁵ Cal. Code Regs. tit. 11, § 999.315(a) (proposed Oct. 11, 2019).

¹⁶ See Fix CCPA, *Don't Force Companies to Connect Online Identities to Real Names*, located at <https://www.fixccpa.com/>.



consumer to opt out of the sale of personal information.¹⁷ We encourage the OAG to consider industry leading implementations that already have consumer recognition in crafting another acceptable opt out mechanism. We also ask the OAG to clarify that online businesses that do not maintain personally identifying information may use an effective method to enable a consumer to opt out other than a webform.

VI. Clarify Businesses Are Not Required to Collect or Maintain More Personal Information to Verify a Consumer

Pursuant to the draft regulations, “[a] business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, and for security or fraud-prevention purposes.”¹⁸ The AG should clarify by regulation that businesses are not required to collect data they do not maintain or collect in the regular course of business in order to verify a consumer’s identity.

Some businesses may maintain personal information in a manner that is not associated with a named actual person. For example, IP addresses and cookie IDs are kinds of personal information that could be associated with or linked to information from many consumers rather than information from a single consumer. Moreover, businesses often keep information that could identify a consumer’s identity separate from other information that may not be identifying on its own. This practice is privacy protective, as it separates consumer identities from certain information collected about the consumer. The draft rules’ current text could require businesses that do not maintain information that is associated with a named actual person to collect additional information from consumers in order to verify their identities. While the draft regulations acknowledge that “fact-based verification process[es]” may be required in such circumstances,¹⁹ this provision of the proposed regulations could force businesses to investigate consumer identities by procuring more data than they normally would in their normal course of business in order to verify consumers.

A business should not be required to obtain additional information from consumers in order to comply with the CCPA. The purpose of the law is to enhance privacy protections for consumers, and forcing businesses to collect data they would not otherwise collect, maintain, or normally associate with a named actual person has the potential to undermine consumer privacy rather than enhance it.²⁰ The OAG should clarify that while businesses *may* collect additional

¹⁷ Cal. Code Regs. tit. 11, at § 999.306(e) (proposed Oct. 11, 2019).

¹⁸ *Id.* at § 999.323(c).

¹⁹ *Id.* at 999.325(e)(2).

²⁰ For example, this mandate would force businesses to collect more information from consumers than they typically do in their normal course of business. Reports on the General Data Protection Regulation (“GDPR”) in Europe have revealed that unauthorized individuals can exploit the law to access personal information that does not



information from a consumer to verify the consumer's identity, the business does not need to do so to comply with the law.

VII. Ensure that Businesses May Provide User-Friendly Privacy Policies to Consumers

The proposed regulations set forth certain requirements for businesses in providing privacy-related notices to consumers. Some of these requirements, such as the obligation to provide relevant disclosures with respect to *each category of personal information collected*, represent new obligations that are not expressly included in the text of the CCPA and may force businesses to produce excessively long and confusing privacy notices that would do little to further consumers' understanding of business data practices. Other notice-related requirements in the draft rules are unclear. For example, the draft regulations do not clearly state whether the required notice at collection, notice of right to opt out, and notice of financial incentive may be provided to consumers in a privacy policy. We urge the OAG to update the draft rules so that consumers may receive understandable privacy notices and so that businesses may provide all required privacy-related notices in a single privacy policy disclosure.

According to the proposed regulations, in privacy policies business must list the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties with whom the business shares personal information “[f]or *each category of personal information collected*...”²¹ However, the terms of the CCPA itself do not require businesses to make disclosures relevant to each category of personal information collected, but rather require businesses to make disclosures with respect to all personal information collected. As such, requiring granular, category-by-category disclosures for each type of personal information collected imposes a significant new substantive requirement on businesses that has no textual basis for support in the CCPA.

Additionally, requiring granular disclosures for each category of personal information collected could impede businesses from ensuring privacy policies are “written in a manner that provides consumers [with] a meaningful understanding of the categories listed.”²² If businesses must make disclosures about sources, purposes, and third parties for each category of personal information collected, privacy notices could be excessively complicated, lengthy, and incomprehensible for consumers, thereby impeding the purpose of providing an informative and understandable consumer privacy notice. Moreover, consumers would be less likely to read and understand such lengthy notices, which could impede the CCPA's goal of enhancing the transparency of business data practices. The OAG should align the regulations with the text of the CCPA by removing the “for each category of personal information collected” language. This change would enable consumers to receive meaningful privacy policies that sensibly disclose

belong to them, causing risks of identity theft. See BBC News, *Black Hat: GDPR privacy law exploited to reveal personal data* (Aug. 9, 2019), located at <https://www.bbc.com/news/technology-49252501>.

²¹ Cal. Code Regs. tit. 11, § 999.308(b)(1)(d)(2) (proposed Oct. 11, 2019).

²² *Id.*



required information in an undaunting and clear format and would advance California legislators' aim of enabling comprehensible, workable consumer notices more effectively than requiring disclosures pertaining to each category of personal information collected.

VIII. Allow Businesses to Satisfy All CCPA-Related Notice Requirements in a Privacy Policy

Pursuant to the proposed rules, businesses must provide a privacy policy and certain other particular notices to consumers. Specifically, in addition to a privacy policy, businesses must provide a notice at collection, a notice of the right to opt out of the sale of personal information, and a notice of financial incentive.²³ However, the proposed rules do not clearly state whether the notice at collection, notice of the right to opt out of the sale of personal information, or notice of financial incentive may be offered to consumers through the privacy policy. The OAG should clarify that all required notices may be provided in a privacy policy.

The draft rules state that a notice at collection may be provided through a conspicuous link on the business's website homepage, mobile application download page, or on all webpages where personal information is collected, which represent typical methods through which privacy policies are normally offered to consumers.²⁴ However, the draft rules do not expressly confirm that a notice at collection may be provided through the privacy policy. Similarly, while a notice of the right to opt-out must include certain particular information or link to the section of the business's privacy policy that contains such information, there is no explicit confirmation that the opt out notice requirement may be satisfied by providing the necessary information in a privacy policy.²⁵ Finally, if a business offers a financial incentive or price of service difference online, the business must link to the section of the business's privacy policy that contains the required information, but it is unclear whether making such a disclosure counts as the required notice of financial incentive that must be offered to consumers.²⁶

We ask the OAG to update the proposed rules so they remove the requirement to provide disclosures with respect to each category of personal information collected, and so that they explicitly state that the notice at collection, notice of right to opt-out, and notice of financial incentive may be provided to consumers in a privacy policy. These updates would lessen the possibility for consumer notice fatigue by enabling more concise, readable notices. They would also be consistent with consumer expectations and would enable more effective and less confusing consumer disclosures, as all privacy-related information could be housed in a unified location. Moreover, such a rule would help businesses in their efforts to meet the CCPA's requirements, because business would be able to focus on reviewing and updating one notice as needed instead of multiple notices. The OAG should clarify that all required notices may be

²³ *Id.* at §§ 999.305, 306, 307.

²⁴ *Id.* at § 999.305(a)(2)(e).

²⁵ *Id.* at § 999.306(b)(1).

²⁶ *Id.* at § 999.307(a)(3).



provided in a privacy policy, because such a clarification would reduce confusion for consumers and better enable CCPA compliance for businesses.

IX. Clarify that Requesting Verifying Information from a Consumer Pauses the Time Period Within Which a Business Must Respond to the Request

The proposed regulations set forth a risk-based process by which businesses may engage in efforts to verify consumers before acting on their requests to delete and requests to know.²⁷ We support the non-prescriptive, risk-based framework for verifying consumer requests that is outlined in the proposed regulations. It provides businesses the flexibility they need to create verification mechanisms that fit their business models while being robust enough to accurately identify consumers submitting CCPA requests. However, despite the beneficial nature of the risk-based approach for verifying consumer requests that is outlined in the proposed rules, we are concerned that the draft rules do not provide businesses with enough time to verify consumers before they are responsible for effectuating CCPA requests.

The draft rules require a business to comply with requests to know and delete within 45 days of receiving the request regardless of the period of time it takes for the business to verify the request.²⁸ We ask the OAG to reconsider this requirement and update the draft rules so a business's request for information to verify a consumer's identity before effectuating a consumer request tolls or pauses the 45-day window within which the business must respond to the request. Consumer verification is necessary for businesses to accurately effectuate consumers' CCPA rights. Robust and accurate verification is in the interest of consumers, because without it, businesses run the risk of erasing or returning data that does not pertain to the requesting consumer. Such a result could have two distinct consumer harms: first, it would fail to fulfill the wishes of the consumer who actually submitted the request, and second, it could impact personal information about a consumer that did not make the request. Consequently, we urge the OAG to update the proposed rules so a business's request for verifying information tolls or pauses the 45-day period within which the business must respond to consumer requests to know and delete.

X. Clarify that a Business May Provide a General Toll-Free Number for Receiving CCPA Requests

According to the draft rules, a business must enable consumers to submit requests to know via a toll-free number and may provide a toll-free number to receive requests to delete and opt out of personal information sale. The proposed rules as currently drafted do not clarify if a business may offer its general toll-free number to receive CCPA requests or if a business must create a separate, CCPA-specific number through which it should receive consumer requests under the law. We ask the OAG to clarify that a business may offer consumers its general toll-free number to receive consumer CCPA requests and does not need to create or staff an entirely new phone number for such requests. Such an update to the proposed rules would decrease consumer confusion by funneling all business-related inquiries through one contact phone

²⁷ *Id.* at §§ 999.323, 324, 325.

²⁸ *Id.* at § 999.313(b).



number. It would also help businesses by refraining from imposing an unnecessary cost on them to staff and maintain a separate number for CCPA requests. Consequently, we urge the OAG to update the draft rules to clarify that a business can provide its general consumer telephone number as the toll-free phone number through which it may receive consumer CCPA requests.

XI. Remove the Requirement to Flow Down Opt Out Requests to Third Parties to Whom the Business has Sold Personal Information in the Prior 90 Days

The proposed rules would require businesses to pass on the opt out requests they receive to third parties. Specifically, a business must “notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business’s receipt of the consumer’s request that the consumer has exercised their right to opt out and instruct them not to further sell the information.”²⁹ This requirement does not further meaningful consumer choice, as it takes a consumer’s opt out selection with respect to one business and propagates it throughout the ecosystem without the consumer’s express consent to do so. Furthermore, it represents a departure from the text of the CCPA by imposing a brand-new requirement on businesses that was not contemplated by the text of the law itself.

Requiring businesses to pass on opt out requests to third parties that received the consumer’s personal information in the prior 90 days could impede a consumer’s ability to exercise specific choices that are effective against particular businesses. A consumer’s choice to opt out of one business’s ability to sell personal information does not mean that the consumer meant to opt out of every business’s ability to sell personal information. This proposed rule has the potential to cause consumers to lose access to online offerings and content that they did not expect or choose to lose by submitting an opt out request to a single business. The law should not require businesses to understand a consumer’s opt out choice as a decision that must apply throughout the entire Internet ecosystem. In addition, requiring businesses to communicate opt out requests to third parties is a substantial new obligation that does not give businesses enough time to build processes to comply with the requirement before January 1, 2020.³⁰ The CCPA, as passed by the Legislature, already provides a means for consumers to control onward sales by third party businesses. The law requires that consumers be provided explicit notice and opportunity to opt out from sale.³¹ The new obligation to pass opt out requests on to third parties that received the consumer’s personal information within the past 90 days moves beyond the text and intent of the CCPA by imposing material and burdensome new obligations on businesses

²⁹ *Id.* at § 999.315(f).

³⁰ The Standardized Regulatory Impact Assessment (“SRIA”) analyzing the proposed regulations’ economic effect on the California economy is also deficient on this point. *See* SRIA at 25-26. The SRIA indicates “[t]he incremental compliance cost associated with this regulation is the extra work required by businesses to notify third parties that further sale is not permissible.” *Id.* at 25. This comment overlooks the ripple effect that the requirement to pass opt out requests on to third parties that have received a consumer’s personal information in the past 90 days would have throughout the Internet ecosystem and the economy. Under the draft rules, a consumer’s single opt out of sale request would restrict beneficial uses of personal information, including those generally occurring subsequent to the initial sale. The OAG should consider how restricting the sale of personal information by third parties in this way can “increase or decrease... investment in the state.” *See* Cal. Gov. Code § 11346.3(c)(1)(D).

³¹ Cal. Civ. Code § 1798.115(d).



without textual support in the CCPA. We therefore encourage the OAG to update the proposed rules so businesses are not required to pass opt out requests along to third parties. Alternatively, the OAG should limit the requirement to information the business actually sold to third parties in the previous 90 days.

XII. Align the Draft Rules with Consumer Choices by Removing the Requirement to Convert Unverifiable Requests to Delete into Requests to Opt Out

If a business cannot verify a consumer who has submitted a request to delete, the proposed rules would require the business to “inform the requestor that their identity cannot be verified and... instead treat the request as a request to opt out of personal information sale.”³² Compelling businesses to convert unverifiable consumer deletion requests into opt out requests could hinder or even completely impede meaningful consumer choice in the marketplace. This mandate has the potential to force a result that the consumer neither intended nor approved. Consequently, we ask the OAG to update the proposed rules so that businesses are not forced to transform unverified deletion requests into opt out requests unless the consumer specifically asks the business to do so.

The CCPA provides separate consumer rights for deletion and opting out of personal information sale because these two rights achieve different policy aims and consumer goals. While deletion is structured to erase the consumer’s personal information from the databases and systems *of the business to which the consumer communicates the request*, the opt out right empowers consumers to stop the transfer of data to *other businesses* in the chain. Because these two rights achieve two different objectives, the law should not compel consumers to opt out of personal information sale if a business cannot verify their request to delete. This outcome, which would be legally required by the proposed regulations, it is not likely to reflect the consumer’s desires in submitting a deletion request.

To illustrate this point, the OAG’s proposed rule requiring businesses to communicate opt out requests to third parties to whom they have sold personal information in the prior 90 days and instruct them not to further sell personal information could cause a consumer’s unverified deletion request to be transformed into an opt out request that is imposed on many other parties other than the business that is the recipient of the request. As a result, a business may be required to transform a deletion request a consumer may have thought she served on one business alone into an opt out request by that business and pass that opt out request along to other businesses without obtaining the consumer’s consent to take this action. This obligation therefore has the potential to unknowingly expose the consumer to potential loss of products and services she did not wish to lose. This result deprives consumers of the ability to make particularized selections about businesses who may and may not sell personal information. We therefore respectfully ask the OAG to align the draft rules with consumer choices by removing the requirement to convert unverifiable requests to delete into requests to opt out unless the consumer affirmatively requests that the business take such an action.

³² Cal. Code Regs. tit. 11, § 999.313(d)(1) (proposed Oct. 11, 2019).



* * *

Thank you for the opportunity to submit input on the content of the proposed regulations interpreting the CCPA. We look forward to continuing to engage with your office as it finalizes the draft rules. Please contact us with any questions you may have regarding these comments.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
[REDACTED]

Dave Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
[REDACTED]

Christopher Oswald
SVP, Government Relations
Association of National Advertisers
[REDACTED]

Alison Pepper
Senior Vice President
American Association of Advertising
Agencies, 4A's
[REDACTED]

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
[REDACTED]

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
[REDACTED]

CC: Mike Signorelli, Venable LLP

Message

From: Michael Pepson [REDACTED]
Sent: 12/6/2019 7:53:38 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: AFPP Coalition Comment on CCPA Regulations
Attachments: 2019.12.06 AFPP Coalition CCPA Regulatory Comment.pdf

To whom it may concern:

Please see the attached AFPP Coalition Comment pertaining to the proposed CCPA regulations.

Thank you for your attention to this matter.

Sincerely,

Michael Pepson

December 6, 2019



Via E-Mail

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

Re: Proposed California Consumer Privacy Act Regulations

To whom it may concern:

On behalf of the undersigned organizations, we appreciate the opportunity to comment on the California Attorney General's ("AG") proposed California Consumer Privacy Act ("CCPA" or "the Act") Regulations. As discussed below, we believe that although consumer data privacy is an important subject that should be addressed at the national level, the U.S. Constitution categorically bars individual states from seeking to regulate the Internet on a national level, as California has sought to do here. The Internet is a subject requiring national uniformity that can only be regulated by the federal government, as opposed to through a burdensome and conflicting patchwork of flatly unconstitutional extraterritorial state laws like the CCPA.

In January 2019, a coalition of privacy experts warned the California Legislature about the CCPA's fatal constitutional flaw: "The CCPA's purported application to activity outside of California raises substantial Constitutional concerns and potentially exposes the state to expensive and distracting litigation."¹ They urged the California Legislature to "clarify the CCPA's applicability to activities outside of California."² The California Legislature has not heeded these privacy experts' clarion call for amendments to the CCPA to bring it in line with constitutional limits on the scope of California's regulatory authority.

The CCPA specifically directs the AG to adopt regulations "[e]stablishing any exceptions [to the CCPA]

¹ Letter from Professor Eric Goldman *et al.* to The Honorable Toni Atkins *et al.*, 3 (Jan. 17, 2019), <http://bit.ly/2DgP0by>.

² *Id.*

necessary to comply with state or federal law,”³ which includes the federal Constitution. Accordingly, we urge you to amend the CCPA regulations to formally, and permanently, disavow any intention of bringing enforcement actions under the CCPA outside of California, due to the statute’s blatant unconstitutionality,⁴ as well as permanently prohibit private parties from any attempt to sue companies outside California for alleged violations of the CCPA. Businesses and California’s sister States should not be forced to sue in federal court to protect their federal constitutional rights.

I. EXECUTIVE SUMMARY

The CCPA is California’s misguided attempt to regulate privacy on a national level to impose its vision of public policy on the entire country. As the California Department of Justice has acknowledged in connection with this rulemaking: “California standards often become national standards because, given the size of the California economy, companies find it easier to adopt a uniform approach rather than differentiating their offerings.”⁵ So too here.

The Act imposes draconian compliance obligations on a host of companies, has a sweeping extraterritorial effect, subjects businesses to an inconsistent patchwork of regulations, and threatens to stifle not only technology and innovation but also free speech. The CCPA is also unconstitutional. *First*, the CCPA is invalid because it has the practical effect of regulating wholly out-of-state conduct and burdening interstate commerce in violation of the dormant Commerce Clause. *Second*, the CCPA’s restrictions on free speech violate the First Amendment. *Third*, the CCPA violates due process for failure to give fair notice of prohibited or required conduct.

II. STATUTORY AND REGULATORY BACKGROUND

A. Overview of CCPA

In 2018, pursuant to a deal struck with the California real estate developer responsible for the ballot initiative, California enacted Assembly Bill 375 (AB 375), now known as the CCPA. In return, the developer pulled the ballot initiative.⁶

The CCPA is an unprecedented state privacy law that will impose sweeping restrictions on the handling of California residents’ data that will affect most businesses with any online presence, imposing draconian compliance costs.⁷ As the Standardized Regulatory Impact Assessment

³ Cal. Civ. Code § 1798.185(a)(3).

⁴ *Cf. Lockyer v. City & Cnty. of S.F.*, 95 P.3d 459, 501–02 (2004) (Moreno, J., concurring) (arguing “there are at least three types of situations in which a local government’s disobedience of a[n] unconstitutional statute would be reasonable”).

⁵ Cal. Dep’t of Justice, Notice of Proposed Rulemaking Action [hereinafter “NPRO”], at 13 (Oct. 11, 2019), available at <http://bit.ly/33jGZxl>; accord Cal. Dep’t of Justice, Office of the Attorney General, Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations [hereinafter “SRIA”], at 32 (Aug. 2019) (“Given the size of the California economy, previous legislation that was unique to California has in turn set national standards[.]”), available at <http://bit.ly/2qItKJ2>.

⁶ See SRIA at 7 (“Before reaching the ballot however, the California legislature offered AB 375 in exchange for the withdrawal of the ballot measure.”).

⁷ The Act grants California residents a number affirmative rights, which covered businesses must accommodate at their expense, including the right to request that a business that sells consumer information or discloses it for a business purpose discloses to the consumer the categories of information collected or disclosed, Cal. Civ. Code § 1798.115;

(“SRIA”) explains, the CCPA and its implementing regulations impose a diverse array of costly new obligations, including:

1. Legal: Costs associated with interpreting the law so that operational and technical plans can be made within a business.
2. Operational: Costs associated with establishing the non-technical infrastructure to comply with the law’s requirements.
3. Technical: Costs associated with establishing technologies necessary to respond to consumer requests and other aspects of the law.
4. Business: Costs associated with other business decisions that will result from the law, such as renegotiating service provider contracts and changing business models to change the way personal information is handled or sold.⁸

The SRIA correctly recognizes that the legal “costs can be quite large”; the “[o]perational costs . . . can include substantial labor costs”; and that “[t]echnology costs, which cover the websites, forms, and other systems necessary to fulfill the CCPA compliance obligations, are also quite substantial due to passage of the CCPA.”⁹ “Small firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises. . . . Another significant risk to small businesses is uncertainty.”¹⁰

Accordingly, as the California AG found, the CCPA and its implementing “regulations may have a significant, statewide adverse economic impact directly affecting business[.]”¹¹ “These businesses fall within most sectors of the California economy, including agriculture, mining, utilities, construction, manufacturing, wholesale trade, retail trade, transportation and warehousing, information, finance and insurance, real estate, professional services, management of companies and enterprises, administrative services, educational services, healthcare, arts, accommodation and food services, among others.”¹² Worse still, the new law was designed to, and will apply, extraterritorially to businesses operating outside of California, so long as there is any nexus to California. Companies that are not prepared to comply with the Act’s onerous requirements will face the threat of severe civil penalties and class action lawsuits.

right to opt out of sale of “personal information,” *id.* § 1798.120; *see also id.* § 1798.135; and right to deletion of “personal information.” *id.* § 1798.105. The CCPA also affirmatively requires covered businesses to provide notice and disclosure of “personal information” they collect, *id.* § 1798.100(b), and effectively mandates an overhaul of consumer-facing websites, micromanaging the content, *id.* § 1798.135. The Act further specifies how businesses are supposed to receive and respond to various requests propounded by California residents and sets a timeline for response. *Id.* § 1798.130. This means that, as a practical matter, covered businesses must revise their websites and privacy policies, undertake the onerous process of determining what data they have about California consumers and where it is located, and pay for the compliance costs associated with responding to various California consumers’ requests under the Act. The Act also imposes training requirements. *See id.* § 1798.130(a)(6).

⁸ SRIA at 10.

⁹ *See id.* at 10–11.

¹⁰ *Id.* at 31.

¹¹ NPRA at 11.

¹² *Id.*

As discussed below, in addition to the CCPA’s policy-related and practical problems, as drafted in its current form, the Act violates the federal Constitution in a several ways.

B. Extraterritorial Scope of Compliance Obligations

The CCPA’s onerous compliance obligations apply to a wide array of commercial entities that in any way “do[] business in the State of California,” if certain threshold requirements are met.¹³ Specifically, companies with any California nexus—regardless of whether they have any physical presence within California—must comply with the Act if any one of the following requirements are met: (A) “annual gross revenues in excess of twenty-five million (\$25,000,000),” regardless of profit margin; (B) any company that “[a]lone or in combination, annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices[]”; or (C) “[d]erives 50 percent or more of its annual revenues from selling consumers’ personal information.”¹⁴ As a practical matter, these definitions, particularly coupled with the Act’s very broad definition of “[p]ersonal information,”¹⁵ threaten to sweep in most companies operating in the United States with any significant online presence.

The Act purports to apply even to companies that do not have any nexus whatsoever with California (including those that do not have a single California customer), such as commonly branded parents and subsidiaries of covered businesses.¹⁶ Thus, for example, a parent company based overseas and conducting no business whatsoever within the United States would be subject to the Act if a subsidiary without any physical presence in California was subject to the Act by virtue of any nexus with California coupled with meeting any of the threshold requirements. Indeed, the Act contains a provision that purports to extend globally to transactions that have no nexus whatsoever to California except for the possession of California residents’ personal information, even if that information was originally received by some other entity located outside of California, by creating a legal fiction: that the out-of-state entity that somehow “received” the “personal information” from some other out-of-state entity that does business in California should be deemed to both do business with California and also “collect” the information.¹⁷ Just as the CCPA applies broadly to a host of commercial enterprises, many of which have tenuous or nonexistent physical contacts with California, the CCPA contains a sweeping and vague definition of “personal information” to which it applies.¹⁸

¹³ See Cal. Civ. Code § 1798.140(c)(1).

¹⁴ *Id.* § 1798.140(c)(1)(A)-(C).

¹⁵ *Id.* § 1798.140(o).

¹⁶ *Id.* § 1798.140(c)(2) (defining “business” to include “Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business”).

¹⁷ *Id.* § 1798.115(d) (“A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out[.]”); *Id.* § 1798.140(w) (broad definition of “third party”); *Id.* § 1798.140(t) (broad definition of “sell”). See also California Senate Judiciary Committee Report, AB 375, at 9 (June 25, 2018). *Cf.* Cal. Civ. Code § 1798.190.

¹⁸ See Cal. Civ. Code § 1798.140(o)(1) (“‘personal information’ means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household” and providing a non-exhaustive list of examples); see also *id.* § 1798.80(e).

Businesses and service providers that are subject to the Act must take a number of affirmative actions or risk civil penalties and class action lawsuits.¹⁹ Importantly, the Act’s civil penalties provision is not limited to “businesses,” as defined in the Act, and purports to broadly apply to a variety of third parties that have no nexus whatsoever with California.²⁰ Indeed, the Initial Statement of Reasons (“ISOR”) admits that CCPA “regulations may be enforceable against businesses located in other states that have their own attorneys general.”²¹ Yet California refused even to attempt to assess the economic effects of its CCPA regulations on out-of-state entities.²²

Perhaps recognizing the extraterritorial effect of the Act—and the attendant constitutional problems with said effect, discussed below—the Act attempts to bring itself within constitutional bounds through a provision that purports to exempt wholly out-of-state conduct from its purview.²³ Similarly, the CCPA only grants rights and privileges to natural persons who are “California residents . . . however identified, including by unique identifier.”²⁴ However, these superficial bows to the U.S. Constitution are woefully insufficient.

III. THE CCPA VIOLATES THE COMMERCE CLAUSE.

A. The CCPA Has the Practical Effect of Regulating Wholly Out-of-State Conduct.

As described above, the CCPA regulates extraterritorially in violation of the dormant Commerce Clause.²⁵ “[S]tate regulation violates the dormant Commerce Clause . . . if it regulates conduct occurring entirely outside of a state’s borders.”²⁶ When a state statute directly regulates interstate commerce, whether facially or in practical effect, the Court generally has “struck down the statute without further inquiry.”²⁷ The dormant Commerce Clause’s bright-line *per se* bar against extraterritorial regulation is rooted in federalism. It is fundamental to our system of federalism that “[n]o state can legislate except with reference to its own jurisdiction.”²⁸ A state’s regulatory authority “is not only subordinate to the federal power over interstate commerce, but is

¹⁹ See Cal Civ Code § 1798.155(b) (civil penalties of up to \$2,500 for each violation and \$7,500 for each intentional violations); Cal Civ Code § 1798.150 (private right of action, including class action, for data breach).

²⁰ See Cal Civ Code § 1798.155(b) (“Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty[.]” (emphasis added)); see also Cal Civ Code § 1798.140(v) (defining “service provider”); Cal Civ Code § 1798.140(w) (broad definition of “third party”).

²¹ ISOR at 3.

²² See SRIA at 21.

²³ See Cal Civ Code § 1798.145(a)(6).

²⁴ See Cal Civ Code § 1798.140(g).

²⁵ See also Jeff Kosseff, *Hamiltonian Cybersecurity*, 54 Wake Forest L. Rev. 156, 193-203 (2019) (state regulation of the Internet may be vulnerable to constitutional challenges); Jennifer Huddleston and Ian Adams, “Potential Constitutional Conflicts in State and Local Data Privacy Regulations,” at 6-9 (Dec. 2019), at <http://bit.ly/2LiRIIK>.

²⁶ *Am. Fuel & Petrochemical Mfrs. v. O’Keefe*, 903 F.3d 903, 911 (9th Cir. 2018); see *Rosenblatt v. City of Santa Monica*, 940 F.3d 439, 445 (9th Cir. 2019) (“A *per se* violation of the dormant Commerce Clause occurs [w]hen a state statute directly regulates or discriminates against interstate commerce[.] . . . A local law directly regulates interstate commerce when it directly affects transactions that take place across state lines or entirely outside of the state’s borders.” (cleaned up)); see also *Legato Vapors, LLC v. Cook*, 847 F.3d 825, 830 (7th Cir. 2017). Courts have held that actual inconsistency between state regulations is not required; “the threat of inconsistent regulation, not inconsistent regulation in fact, is enough[.]” *Id.* at 834.

²⁷ *Brown-Forman Distillers Corp. v. New York State Liquor Auth.*, 476 U.S. 573, 579 (1986).

²⁸ *Bonaparte v. Tax Court*, 104 U.S. 592, 594 (1881).

also constrained by the need to respect the interests of other States.”²⁹ The rule that one state has no power to project its legislation into another state embodies the Constitution’s concern both with the maintenance of a national economic union unfettered by state-imposed limitations on interstate commerce and with the autonomy of the individual States within their respective spheres.³⁰

The CCPA violates this rule. Numerous state statutes regulating the Internet have been found unconstitutional on these grounds.³¹ The CCPA is no different. The Act on its face and in practical effect regulates wholly out-of-state contractual relationships between out-of-state entities and wholly out-of-state sales. For example, the CCPA purports to reach the sale of “personal information” by a covered “business” located in New York to a service provider or third party located in Florida, or the use of “personal information” by a third party located in North Dakota or England that somehow receives it from a “business” located in New Jersey. The only nexus to California is the fact that “personal information” from California residents located in California was “collected” by one of the out-of-state entities involved. This California may not do under Ninth Circuit precedent because both parties to the contract are located out-of-state.³²

“[A] statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State’s authority and is invalid regardless of whether the statute’s extraterritorial reach was intended by the legislature. The critical inquiry is whether the practical effect of the regulation is to control conduct beyond the boundaries of the State.”³³ The Commerce Clause “precludes the application of a state statute to commerce that takes place wholly outside of the State’s borders, whether or not the commerce has effects within the State.”³⁴ Thus, “States and localities may not attach restrictions to exports or imports in order to control commerce in other States.”³⁵ “[T]he Commerce Clause [also] protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State.”³⁶ “[T]he practical effect of the statute must be evaluated not only by considering the

²⁹ *BMW of N. Am., Inc. v. Gore*, 517 U.S. 559, 571-72 (1996) (citations omitted).

³⁰ See *Healy v. Beer Inst.*, 491 U.S. 324, 335-36 (1989); *Baldwin v. G.A.F. Seelig, Inc.*, 294 U.S. 511, 521 (1935); see also *N.Y. Life Ins. Co. v. Head*, 234 U.S. 149, 161 (1914) (territorial constraint is an “obvious[]” and “necessary result of the Constitution”); *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 293 (1980) (“The sovereignty of each State implic[s] a limitation on the sovereignty of all of its sister States” that is inherent in “the original scheme of the Constitution[.]”).

³¹ See, e.g., *Publius v. Boyer-Vine*, 237 F. Supp. 3d 997 (E.D. Cal. 2017) (O’Neil, J.) (finding First Amendment and dormant Commerce Clause extraterritoriality violations with respect to California statute regulating out-of-state posting of truthful personal information about California legislators on the Internet); *Am. Booksellers Found. v. Dean*, 342 F.3d 96, 104-05 (2d Cir. 2003); *Backpage.com, LLC v. Hoffman*, No. 13-03952, 2013 U.S. Dist. LEXIS 119811, at *33 (D.N.J. Aug. 20, 2013) (“Because the internet does not recognize geographic boundaries, it is difficult, if not impossible, for a state to regulate internet activities without project[ing] its legislation into other States. The Act is likely in violation of the dormant commerce clause, and thus cannot stand.”).

³² See *Sam Francis Found. v. Christies, Inc.*, 784 F.3d 1320, 1322 (9th Cir. 2015) (en banc).

³³ *Healy*, 491 U.S. at 336; see also *BMW of N. Am. v. Gore*, 517 U.S. 559, 572 (1996) (“a State may not impose economic sanctions on violators of its laws with the intent of changing the tortfeasors’ lawful conduct in other States.”). Cf. *C & A Carbone v. Town of Clarkstown*, 511 U.S. 383, 394 (1994) (even a regulation that does not expressly regulate interstate commerce may do so “nonetheless by its practical effect and design”).

³⁴ *Healy*, 491 U.S. at 336 (internal citations omitted).

³⁵ *C & A Carbone*, 511 U.S. at 393 (citing *Baldwin*, 294 U.S. 511).

³⁶ *Healy*, 491 U.S. at 336-37.

consequences of the statute itself, but also by considering how the challenged statute may interact with the legitimate regulatory regimes of other States and what effect would arise if not one, but many or every, State adopted similar legislation.”³⁷

“The mere fact that some nexus to a state exists will not justify regulation of wholly out-of-state transactions. For example, an attempt by California to regulate the terms and conditions of sales of artworks outside of California simply because the seller resided in California was a violation of the dormant Commerce Clause.”³⁸ As the Ninth Circuit explained in *Sam Francis v. Christie’s, Inc.*: “The Supreme Court has held that ‘our cases concerning the extraterritorial effects of state economic regulation stand at a minimum for the following proposition[]: . . . the Commerce Clause precludes the application of a state statute to commerce that takes place wholly outside of the State’s borders, whether or not the commerce has effects within the State.’”³⁹

Under controlling Ninth Circuit precedent, the CCPA violates the dormant Commerce Clause’s ban on regulation of wholly out-of-state conduct. Just as in *Sam Francis*, the Act applies to sales and contracts that are wholly out-of-state. Unlike cases involving “products that are brought into or are otherwise within the borders of the State,”⁴⁰ the CCPA governs what businesses must do with “personal information” that has *left* California’s borders and is physically stored in other states—even businesses that merely receive “personal information” from another out-of-state entity.⁴¹ In *Daniels Sharpsmart v. Smith*, the Ninth Circuit addressed a similar circumstance: “we are faced with an attempt to reach beyond the borders of California and control transactions that occur wholly outside of the State after the material in question—medical waste—has been removed from the State.”⁴² The Ninth Circuit held the fact the medical waste originated in-state did not allow California to “regulate waste treatment” after it was transported outside the state.⁴³

That is exactly what the CCPA does here as applied to certain out-of-state businesses. The mere fact that the “personal information” at issue originated from California is an insufficient nexus to justify California regulating wholly out-of-state conduct. The CCPA’s downstream regulation of data processors and other third parties who contract with out-of-state businesses that “collect” the “personal information” of California residents is unconstitutional because it directly regulates wholly out-of-state commerce, including wholly out-of-state sales where the only contracts are between out-of-state entities. It is an insufficient jurisdictional hook to link this to

³⁷ *Daniels Sharpsmart, Inc. v. Smith*, 889 F.3d 608, 614-15 (9th Cir. 2018) (cleaned up).

³⁸ *Id.* at 615 (citing *Sam Francis Found. v. Christies, Inc.*, 784 F.3d 1320, 1322 (9th Cir. 2015) (en banc)); *Ass’n for Accessible Meds. v. Frosh*, 887 F.3d 664, 674 (4th Cir. 2018).

³⁹ *Sam Francis Found.*, 784 F.3d at 1323-24 (quoting *Healy*, 491 U.S. at 336).

⁴⁰ *See Daniels Sharpsmart*, 889 F.3d at 615.

⁴¹ The Act on its face also appears to regulate contractual agreements between wholly out-of-state entities. *See* Cal. Civ. Code § 1798.140(v). The CCPA also contains a provision that incentivizes covered “businesses” to include provisions in contracts with service providers effectively dictated by the Act. *See id.* § 1798.140(w)(2). It does this to bring these outside entities within the scope the statute by effectively mandating that these “service providers” agree to a contractual term that operates as a jurisdictional hook and ensures that these entities will be held responsible for CCPA compliance.

⁴² *Daniels Sharpsmart*, 889 F.3d at 615.

⁴³ *Id.* at 616. *Cf. Ass’n for Accessible Med.*, 887 F.3d at 672 (striking down Maryland statute that “effectively seeks to compel manufacturers and wholesalers to act in accordance with Maryland law outside of Maryland”).

the mere fact that the truthful information came from a California resident who was at that time located in California when it was collected.

California “may not project its legislation into other states,” and it may not control conduct beyond the boundaries of the State.⁴⁴ Such extraterritorial regulation categorically violates the dormant Commerce Clause.⁴⁵ California may not project its preferred law and policy outside of California to directly regulate the conduct and contractual arrangements between wholly out-of-state entities. California may not control the out-of-state use and sale of lawfully obtained information, regardless of whether the information was sent from California by a California resident. And California may not micromanage the training and record-retention practices of out-of-state entities, particularly those with tenuous, at best, contacts with the state.

B. Only the Federal Government May Regulate the Internet.

The CCPA is also unconstitutional because the U.S. Constitution’s Commerce Clause categorically bars state-level regulation of the Internet. The Supreme Court has long made clear that certain subjects require uniform national regulation.⁴⁶ This strand of case law, whether rooted in the very structure of the federal Constitution or the Commerce Clause, suggests that the power to regulate certain subjects is categorically reserved exclusively for the federal government, *i.e.*, state regulation of these subjects is categorically prohibited.⁴⁷ As numerous federal courts have explained, the Internet is the type of subject that, by necessity, must only be regulated by the federal government.⁴⁸ Put simply, “the unique nature of cyberspace necessitates uniform national treatment and bars the states from enacting inconsistent regulatory schemes.”⁴⁹

⁴⁴ *Brown-Forman Distillers*, 476 U.S. at 582.

⁴⁵ See *Healy*, 491 U.S. at 336 (state statute is invalid per se if practical effect is extraterritorial). Strict scrutiny applies to any State attempt to “control conduct beyond the boundary of the state,” *id.* at 336–37, “whether or not the commerce has effects within the State,” *Edgar v. MITE Corp.*, 457 U.S. 624, 642–43 (1982).

⁴⁶ See *Cooley v. Bd. of Wardens*, 53 U.S. (12 How.) 299, 319 (1852) (“Whatever subjects of this power are in their nature national, or admit only of one uniform system, or plan of regulation, may justly be said to be of such a nature as to require exclusive legislation by Congress.”). See generally *South Dakota v. Wayfair, Inc.*, 138 S. Ct. 2080, 2090 (2018) (discussing *Cooley*); *Korab v. Fink*, 797 F.3d 572, 594 (9th Cir. 2014) (Bybee, J., concurring).

⁴⁷ See *Cooley*, 53 U.S. (12 How.) at 319; *Japan Line, Ltd. v. Cnty. of L.A.*, 441 U.S. 434, 457 (1979) (“The problems to which appellees refer are problems that admit only of a federal remedy. They do not admit of a unilateral solution by a State.”) (cleaned up).

⁴⁸ See, e.g., *Am. Booksellers Found.*, 342 F.3d at 104 (“We think it likely that the internet will soon be seen as falling within the class of subjects that are protected from State regulation because they imperatively demand a single uniform rule.”) (cleaned up); *Am. Libraries Ass’n v. Pataki*, 969 F. Supp. 160, 183 (S.D.N.Y. 1997) (“The Internet . . . requires a cohesive national scheme of regulation so that users are reasonably able to determine their obligations. . . . Haphazard and uncoordinated state regulation can only frustrate the growth of cyberspace. The need for uniformity in this unique sphere of commerce requires that New York’s law be stricken as a violation of the Commerce Clause.”); *ACLU v. Johnson*, 194 F.3d 1149, 1162 (10th Cir. 1999) (“[C]ertain types of commerce have been recognized as requiring national regulation. The Internet is surely such a medium.” (citations omitted)).

⁴⁹ *Am. Libraries Ass’n*, 969 F. Supp. at 184; see also *Huddleston & Adams*, *supra* note 25, at 7–8, 12.

C. CCPA's Burdens on Interstate Commerce Vastly Outweigh Putative Local Benefits.

As the Supreme Court recently reaffirmed: “States may not impose undue burdens on interstate commerce.”⁵⁰ As explained below, even if the CCPA did not violate the dormant Commerce Clause’s *per se* bar against extraterritorial regulations, it should be stricken because the concrete real-world burdens it places on interstate commerce are clearly excessive in relation to its putative local, purely speculative “privacy” benefits to California consumers.⁵¹

1. *The CCPA’s Local Benefits Are Speculative and Illusory.*

Protecting citizens’ privacy is, in the abstract, a legitimate state interest. But the extent to which the CCPA furthers that interest is unclear. To begin with, a host of state and federal statutes already address particularly important privacy-related matters. Examples of such laws include the Gramm-Leach Bliley Act (“GLBA”), Children’s Online Privacy Protection Act (“COPPA”), Fair Credit Reporting Act (“FCRA”), Driver’s Privacy Protection Act (“DPPA”), Health Insurance Portability and Accountability Act (“HIPPA”), the California Financial Information Privacy Act (“CFIPA”), Confidentiality in Medical Information Act (“CMIA”), Student Online Personal Information Protection Act (“SOPIPA”), and the Insurance Information Privacy Act (“IIPA”). In addition, the CCPA may actually facilitate privacy violations. As one commenter explained: “Consider an abusive relationship: A consumer’s safety or confidentiality may be placed at risk if his/her personal information is revealed as part of another consumer’s access request. . . . Scenarios for other compromises to consumer safety and protection are limitless.”⁵²

The CCPA’s alleged local benefits are speculative and abstract. For instance, according to the Initial Statement of Reasons “Summary of Benefits”:

Privacy is one of the inalienable rights conferred on Californians by the state Constitution. The CCPA enumerates specific privacy rights. In giving consumers greater control over their personal information, the CCPA, operationalized by these regulations, mitigates the asymmetry of knowledge and power between individuals and businesses. This benefits not only individuals, but society as a whole. The empowerment of individuals to exercise their rights is particularly important for a democracy, which values and depends on the autonomy of the individuals who constitute it.⁵³

Indeed, the SRIA made no effort to quantify the value California *consumers* place on the privacy rights granted by the CCPA, instead attempting to estimate the value of the data to the companies that collected it using average revenue per user (“ARPU”).⁵⁴ As the SRIA states:

The CCPA’s benefits to consumers derive from the privacy protections granted by the law. These protections . . . give consumers the right to assert control over the use of their personal information. The economic value to consumers of these

⁵⁰ *Wayfair*, 138 S. Ct. at 2091 (citing *Pike v. Bruce Church, Inc.*, 397 U. S. 137, 142 (1970)).

⁵¹ See *Pike*, 397 U.S. at 142.

⁵² Perkins Coie Comments (General Industry) at 8 (CCPA00000966).

⁵³ ISOR at 2.

⁵⁴ See SRIA at 12–15.

protections can be measured as the total value of consumers' personal information, which they can choose to prevent the sale of or even delete. *Although the subjective value of this information to consumers is generally agreed to be great*, it is extremely difficult to quantify the precise value of consumers' personal information in the marketplace and estimates can vary substantially.⁵⁵

Put different, the putative value of the claimed local benefits to the *consumers* who purportedly benefit from the law is entirely subjective and unsupported by empirical research or data. Nor is it even clear how many Californians will exercise their rights under the CCPA. And as the SRIA recognizes: “consumers only receive maximal benefits if they choose to exercise the privacy rights given to them and not everyone is likely to do so[.]”⁵⁶

2. *The CCPA Substantially Burdens Interstate Commerce.*

Any putative privacy benefits flowing from the CCPA are inconsequential in relation to the severe burdens it imposes on interstate commerce. “Balanced against the limited local benefits resulting from the . . . [CCPA] is an extreme burden on interstate commerce. . . . [The CCPA] casts its net worldwide[.]”⁵⁷ The CCPA substantially burdens interstate (and indeed international) commerce in myriad ways, imposing draconian compliance costs on hundreds of thousands of in-state (and out-of-state) businesses and threatening thousands of jobs. Indeed, California's own Economic Impact Statement found that the CCPA will “eliminate[.]” nearly 10,000 jobs in California alone.⁵⁸ As the SRIA found, “[s]ome industries will be forced to completely revise their business models” because of the CCPA.⁵⁹ As the Chief Economist for California's Department of Finance noted, “[t]he SRIA estimates that the initial cost of compliance may be up to \$55 billion”⁶⁰—and that staggering figure is for California alone. The SRIA did not even attempt to evaluate the CCPA's economic impact on out-of-state and overseas businesses.⁶¹ “Small firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises.”⁶² The CCPA regulations also threaten to “creat[e] additional barriers to entry for future [out-of-state] competitors [with California companies] considering entering into the California market.”⁶³

As numerous comments have made clear, the practical compliance challenges are astronomical for both in-state *and* out-of-state businesses that meet the low compliance thresholds.⁶⁴ Even comparatively small businesses (such as convenience stores and restaurants)

⁵⁵ *Id.* at 12.

⁵⁶ *Id.* at 15; see Huddleston & Adams, *supra* note 25, at 5 (explaining that “the potential benefits of . . . [state privacy] laws are not readily calculable as an empirical matter and are, as a result, more difficult to discern.”).

⁵⁷ See *Am. Libraries Ass'n*, 969 F. Supp. at 179.

⁵⁸ Economic Impact Assessment, <http://bit.ly/2OM3PIm>.

⁵⁹ See SRIA at 30.

⁶⁰ Letter from Irena Asmundson, Chief Economist, Cal. Dep't of Fin., to Stacey Schesser, at 2 (Sept. 16, 2019) (Appendix B to ISOR), available at <http://bit.ly/2QQozBq>.

⁶¹ SRIA at 21 (“The economic impact of the regulations on these businesses located outside of California is beyond the scope of the SRIA and therefore not estimated.”).

⁶² *Id.* at 31.

⁶³ *Id.* at 32 (Aug. 2019)

⁶⁴ See, e.g., California Chamber of Commerce Comments (CCPA00000067-CCPA00000116); Toy Association Comment (CCPA00000185-CCPA00000196); BakerHostetler Comment (CCPA00000273-CCPA00000284); CTIA

with any significant online presence may be compelled to comply. Among other things, the CCPA creates perverse incentives for out-of-state companies that may potentially have any contact with a California consumer involving the collection of information to avoid expanding beyond the \$25-million-per-year-in-gross-revenue threshold requiring CCPA compliance. Alternatively, CCPA incentivizes out-of-state companies to stop selling to California customers or, alternatively, block California customers from their websites. The CCPA threatens to deter and punish innovation as well, particularly with respect to small startups ill-equipped to bear its compliance costs.

The CCPA's burdens on interstate commerce are compounded by the Sisyphean practical challenges companies face in attempting to comply not only with the CCPA but also GDPR and other state privacy laws, which differ in salient respects from the CCPA. For instance, as the AG has been made aware, the CCPA diverges from GDPR in many material respects.⁶⁵ Indeed, the Initial Statement of Reasons itself highlights the "incompatibility" of CCPA with GDPR, noting that they "have different requirements, different definitions, and different scopes."⁶⁶ In addition, the CCPA is inconsistent with federal law such as COPPA, as commenters have previously explained.⁶⁷ Further, other states have followed in California's footsteps to add their own gloss on state-level Internet regulation.⁶⁸

Comment (CCPA00000393-CCPA00000409); AAF, ANA, IAB, and NAI Comment (CCPA00000432-CCPA00000442); ACRO Comment (CCPA00000444-CCPA00000446); Randall-Reilly Comment (CCPA00000483-CCPA00000484); Mayer Brown Comment (CCPA00000522-CCPA00000527); Mapbox Comment (CCPA00000535-CCPA00000540); Auto Alliance Comment (CCPA00000568-CCPA00000586); SIIA Comment (CCPA00000755-CCPA00000756); ESA Comments (CCPA00000741-CCPA00000747); HERE Comment (CCPA00000850-CCPA00000855); ITIF Comment (CCPA00000873-CCPA00000885); Perkins Coie Comments (Financial Services Industry) (CCPA00000927-CCPA00000951); Perkins Coie Comments (General Industry) (CCPA00000952-CCPA00000968); Engine Comment (CCPA00000991-CCPA00000995); U.S. Chamber of Commerce Comment (CCPA00001108-CCPA00001118); Orange County Business Council Comment (CCPA00001370-CCPA00001371); Software Alliance Comments (CCPA00001373-CCPA00001380); Innovative Lending Platform Association Comment (CCPA00001383-CCPA00001385).

⁶⁵ See Comparing Privacy Laws: GDPR vs. CCPA (CCPA00000782-CCPA00000823); see also Jehl & Friel, CCPA and GDPR Comparison Chart, available at <http://bit.ly/34qefV2>.

⁶⁶ ISOR at 44.

⁶⁷ See Toy Association Comment (CCPA00000185-CCPA00000196); see also ACRO Comment (CCPA00000444-CCPA00000446).

⁶⁸ See IAPP, State Comprehensive-Privacy Law Comparison, <http://bit.ly/2OgTcyl>; Akin Gump, Comparison Chart of Pending CCPA and GDPR-Like State Privacy Legislation (May 2019), available at <http://bit.ly/2OavEv8>; see also Huddleston & Adams, *supra* note 25, at 8.

IV. THE CCPA VIOLATES THE FIRST AMENDMENT.

The CCPA is also unconstitutional because, as First Amendment law scholars and practitioners have explained, some of the CCPA's provisions violate companies' First Amendment rights.⁶⁹ Their insightful commentary on the unconstitutionality of the CCPA under Supreme Court cases such as *Sorrell v. IMS Health Inc.*⁷⁰ is part of the record in this rulemaking.⁷¹

As these First Amendment experts point out, the CCPA “violates settled First Amendment principles by restricting the dissemination of accurate, publicly available information”⁷²:

The CCPA's provisions restricting the dissemination of publicly available information are unconstitutional for three independent reasons. First, these limitations are content-based restrictions on speech that are not justified by a sufficiently weighty governmental interest to satisfy strict scrutiny, or even intermediate scrutiny. Second, the regulation limiting dissemination of information publicly disclosed by government agencies is unconstitutionally vague. Third, the CCPA's restrictions unconstitutionally distinguish among speakers and among different types of speech.⁷³

To date, the California Legislature has refused to legislatively remedy the Act's myriad constitutional shortcomings.

Among other constitutional flaws, “[t]he CCPA on its face favors some speakers and some uses of information while disfavoring others. It also allows consumers to use the power of the State to suppress particular speakers and facts. And it does so in a frankly content-based way[.]”⁷⁴ As these constitutional experts explain: “[T]he law's practical effect is to enable California residents to suppress the communication of particular facts. Moreover, the Act authorizes consumers to ban speech selectively, allowing some businesses to speak about them while silencing others. . . . Indeed, the Act appears designed to encourage . . . [content and viewpoint] censorship.”⁷⁵ “This creates the potential for groups of consumers to burden disproportionately the speech of unpopular speakers, effectively censoring their communications in a manner that violates First Amendment principles.”⁷⁶

As discussed above, the CCPA's purported local privacy benefits are highly abstract and uncertain, at best, and greatly outweighed by the excessive burdens on interstate commerce that California's extraterritorial Internet regulation imposes. Nor can these putative privacy benefits justify the CCPA's unconstitutional restrictions on truthful speech. As First Amendment experts

⁶⁹ See Andrew Pincus, Miriam Nemetz, & Eugene Volokh, *Invalidity Under the First Amendment of the Restrictions on Dissemination of Accurate Publicly Available Information Contained in the California Consumer Privacy Act of 2018* (Jan. 24, 2019) [hereinafter “Mayer Brown Memo”].

⁷⁰ 564 U.S. 552 (2011).

⁷¹ See CCPA00000757-CCPA00000769.

⁷² Mayer Brown Memo at 1.

⁷³ *Id.* at 4.

⁷⁴ *Id.* at 11.

⁷⁵ *Id.* at 12.

⁷⁶ *Id.* at 13.

have explained: “The government cannot defend a speech restriction ‘by merely asserting a broad interest in privacy.’ ‘[P]rivacy may only constitute a substantial state interest if the government specifically articulates and properly justifies it.’ ”⁷⁷ California has utterly failed to do so here.⁷⁸

V. THE CCPA VIOLATES DUE PROCESS FOR FAILURE TO GIVE FAIR NOTICE OF PROHIBITED OR REQUIRED CONDUCT.

Businesses have a due-process right to fair notice of the CCPA’s requirements.⁷⁹ The AG bears the responsibility to promulgate clear, unambiguous standards.⁸⁰ To provide sufficient notice, a statute or regulation must “give the person of ordinary intelligence a reasonable opportunity to know what is prohibited so that he may act accordingly.”⁸¹ Due-process requirements are heightened where, as here, civil penalties may be imposed. Corporations should not be subject to civil penalties that are not clearly applicable by either statute or by regulation.⁸²

The CCPA and its implementing regulations fail this test. To begin with, it is impossible for many companies to predict whether they are even subject to the CCPA. For example, how is a company that currently has an annual gross revenue of \$24 million in 2019 supposed to predict or know whether its annual gross revenue in 2020 will exceed \$25 million, thereby triggering CCPA compliance obligations? Similarly, how are small businesses supposed to reliably determine whether they have received “personal information” from “50,000 or more consumers, households, or devices” on an annual basis and thus must comply with the CCPA? Indeed, as one commenter aptly pointed out:

Without access to geolocation data a business cannot determine if information collected via mobile phone or a portable personal computer was collected while the individual was in California. If an individual in California attempts to shield their location from the business (ex. through use of a virtual private network (VPN)), and the business has no other indication the individual is in California, will the business be in violation of the law if it collects or sells that information? This also raises questions over whether it is constitutionally permissible for California to regulate business that occurs in other states or as part of interstate commerce.⁸³

These problems are exacerbated by the fact that neither the statute nor the regulations define “doing business” in California, leaving companies in the dark as to whether they must meet the CCPA’s onerous compliance requirements or risk enforcement actions. That is flatly unconstitutional.

⁷⁷ *Id.* at 6 (quoting *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1235 (10th Cir. 1999)).

⁷⁸ *See id.* at 6-9.

⁷⁹ *See Fed. Comm’n Comm’n v. Fox TV Stations, Inc.*, 567 U.S. 239, 253 (2012) (“A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required.”); *Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156, 2167 (2012).

⁸⁰ *See Marshall v. Anaconda Co.*, 596 F.2d 370, 377 n.6 (9th Cir. 1979); *see also Ga. Pac. Corp. v. OSHRC*, 25 F.3d 999, 1005–06 (11th Cir. 1994) (ascertainable certainty standard); *Gen. Elec. Co. v. Envtl. Protection Agency*, 53 F.3d 1324, 1329 (D.C. Cir. 1995) (same).

⁸¹ *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972); *see Connally v. Gen. Constr. Co.*, 269 U.S. 385, 391 (1926).

⁸² *See, e.g., United States v. Trident Seafoods Corp.*, 60 F.3d 556, 559 (9th Cir. 1995).

⁸³ AFSA Comment at CCPA00000005.

VI. THE CCPA, IF ENFORCED, WILL IRREPARABLY HARM COVERED BUSINESSES, CONTRARY TO THE PUBLIC INTEREST

The CCPA, if enforced, will cause irreparable harm to businesses, as recognized under equity. *First*, covered businesses will suffer irreparable harm in the form of un-recoupable compliance costs.⁸⁴ *Second*, the CCPA’s violations of the dormant Commerce Clause and businesses’ First Amendment rights is also irreparable harm.⁸⁵ “[E]nforcement of an unconstitutional law is always contrary to the public interest.”⁸⁶ The AG should thus refuse to enforce the CCPA.

For the foregoing reasons, we respectfully submit that the AG should revise the CCPA regulations to comply with statutory and constitutional limits on its authority. If you have any questions about this request, please contact me at [REDACTED]. Thank you for your attention to this matter.

Sincerely,

Americans for Prosperity Foundation
Cardinal Institute for West Virginia Policy
Christopher Koopman
Freedom Foundation of Minnesota
James Madison Institute

Libertas Institute of Utah
Mississippi Center for Public Policy
Mississippi Justice Institute
Pelican Institute
Washington Policy Center

⁸⁴ See *Morales v. Trans World Airlines, Inc.*, 504 U.S. 374, 381 (1992) (holding that a plaintiff would suffer “irreparable harm” if forced to choose to incur either the civil enforcement liability of violating a preempted state law or the costs of complying with the law during the pendency of the proceedings); see also *Chamber of Commerce v. Edmondson*, 594 F.3d 742, 770–71 (10th Cir. 2010) (“Imposition of monetary damages that cannot later be recovered for reasons such as sovereign immunity constitutes irreparable injury.”).

⁸⁵ *Elrod v. Burns*, 427 U.S. 347, 373 (1976) (holding that deprivation of constitutional rights “unquestionably constitutes irreparable harm”); see *Am. Libraries Ass’n*, 969 F. Supp. at 168 (“Deprivation of the rights guaranteed under the Commerce Clause constitutes irreparable injury.”).

⁸⁶ *Gordon v. Holder*, 721 F.3d 638, 653 (D.C. Cir. 2013); see also *Legend Night Club v. Miller*, 637 F.3d 291, 302–03 (4th Cir. 2011) (state “is in no way harmed by issuance of an injunction that prevents the state from enforcing unconstitutional restrictions.”).

Message

From: Matt Kownacki [REDACTED]
Sent: 12/7/2019 12:01:36 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: AFSA-CFSA comment letter
Attachments: AFSA-CFSA comment letter - CCPA Regs.pdf

On behalf of the American Financial Services Association and the California Financial Services Association, attached is a comment letter regarding the proposed CCPA regulations.

Thank you for your consideration of our comments.

Matt Kownacki
Director, State Research and Policy
American Financial Services Association
[REDACTED]



December 6, 2019

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

Re: CCPA proposed regulations

On behalf of the American Financial Services Association (“AFSA”)¹ and the California Financial Services Association (“CFSA”),² thank you for the opportunity to provide comments on the regulations proposed by the Office of the Attorney General (“OAG”) to implement the California Consumer Privacy Act (“CCPA”). We appreciate your consideration of our comments during the preliminary rulemaking process and reiterate our previous concerns about vague terms and the substantial burdens these regulations place on covered entities.

We appreciate the OAG’s efforts to provide guidance to businesses on how to comply and to clarify the law’s requirements through the implementing regulations. However, though our members share the state’s goal of protecting the privacy of consumers, promoting understanding by consumers of the personal information about them that is collected, sold, and shared for a business purpose, and guarding personal information from unauthorized access, we have significant concerns about the regulations as proposed. There are certain areas where we believe consumers and the business community would benefit from increased clarity and certainty.

Enforcement Delay

Although the effective date and issues of enforcement are not addressed directly in the proposed regulations, our members believe that some clarity in this area is warranted. The CCPA was largely effective on September 23, 2018, and will be operative on January 1, 2020, and enforceable by the OAG on July 1, 2020. It appears that the OAG intends for the regulations to also be enforceable on July 1, 2020, which is likely to be the earliest date that the regulations could be made effective. A delayed enforcement date would give affected businesses the opportunity to evaluate the specific requirements set forth in the regulations and implement new systems and processes needed to be fully in compliance with the law.

¹ Founded in 1916, the American Financial Services Association (AFSA), based in Washington, D.C., is the primary trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including direct and indirect vehicle financing, traditional installment loans, mortgages, payment cards, and retail sales finance. AFSA members do not provide payday or vehicle title loans.

² The California Financial Services Association is a non-profit trade association representing major national and international corporations and independent lenders with operations in the State of California to provide a broad range of financial services, including consumer and commercial loans, retail installment financing, automobile and mobile home financing, home purchase and home equity loans, credit cards, and lines of credit.

In addition, we request that the OAG include in the final regulations a statement to the effect that any enforcement actions will be based on conduct that takes place after the statutory enforcement date of July 1, 2020, or such later date as the regulations may become enforceable. In making this request, we note that the proposed regulations address all the major aspects of the CCPA: how to provide notices, content of the privacy policy, the process for handling submitted requests, verification, and calculating the value of consumer data. Without having final regulations in place to govern compliance, businesses lack clarity that the solutions they are readying for January 1, 2020, will, in fact, meet regulatory requirements. We request that businesses have all the applicable rules and requirements, in final form, with a reasonable timeframe to achieve compliance, before their actions can be determined to be unlawful. Recognizing the time necessary for the OAG to draft and implement comprehensive regulations, we believe that the outlined enforcement delay would be consistent with the legislature’s intended delayed enforcement date.

§ 999.301. Definitions

Section 999.301(h) broadly defines “household” as *a person or group of people occupying a single dwelling*. Such a broad definition based merely on temporary occupancy of a dwelling rather than a requirement that persons be related and domiciled, as defined in Section 17014 of Title 18 of the California Code of Regulations, would sweep in groups in living arrangements who should not have access to the personal information of others, such as multiple roommates linked by mutual tenancy, a landlord and tenant, persons using a house sharing app for the weekend, and at the most extreme end, all the residents of a college dormitory. Because this broad access would be contrary to the purpose of the CCPA, we recommend striking the requirement that businesses accept requests from household members—except those from a parent or guardian on behalf of a minor—or, at the very least, that persons whose only relationship is that they share a housing unit should not be included in the definition of household. Instead, we recommend that the OAG consider adopting a definition of household similar to the definition of “family group” used by the U.S. Census Bureau, which defines a family group as “any two or more people (not necessarily including a householder) residing together, and related by birth, marriage, or adoption.”³

Section 999.301(n) provides a definition of “request to know” that includes *any or all of* six categories of information. Section 999.313 describes different processes depending on whether a consumer is requesting specific pieces of information or categories of information. Providing this kind of flexibility was not envisioned in the statute, and many of our members have already started building solutions that do not afford multiple choices of this kind. We request that the OAG clarify that this multi-tier approach is not mandatory and confirm that businesses that build their process to meet the more conservative requirements associated with a request for specific pieces of information will be in compliance with the law.

§ 999.305. Notice at Collection of Personal Information

This section describes a comprehensive, detailed consumer notice, which suggest there may be a specific form notice the OAG might want covered entities to use. If the OAG intends to be more

³ <https://www.census.gov/programs-surveys/cps/technical-documentation/subject-definitions.html#familyhousehold>.

prescriptive regarding the notice requirements, then we request it release a sample form and that the use of such sample form of notice provide a safe harbor for compliant businesses. As many covered entities are likely already working on their own notice in advance of the impending compliance date, we request that notices substantially similar to the sample form notice also be deemed compliant.

Both the statute and the proposed regulation require a collecting business to notify consumers of the categories of personal information to be collected and the purposes for which they will be used. The statute specifies that disclosures required by section 1798.100 must be provided in accordance with the requirements of section 1798.130. The only part of section 1798.130 that a business can look to for instruction on providing the advance notice is section 1798.130(a)(5), which specifies the information that must be in the online privacy policy. Accordingly, businesses that rely on their online privacy policies to provide advance notice should be considered in compliance with the statute. We request that the OAG remove any language from the draft regulations that suggests otherwise.

Section 999.305(a)(2) requires a business present a notice that is “understandable to an average consumer.”⁴ While we support the goal of clear communications to consumers, the proposed standard is vague and requires additional guidance. If the OAG does not intend to provide a sample notice, we request a clearer and more measurable standard.

Section 999.305(a)(3) requires a business to obtain explicit consent from the consumer to use personal information for a new purpose that may not have been originally disclosed. This requirement goes beyond the existing statutory requirements, which require only notice, and as noted above, could be provided through changes to the online privacy policy. Further, a requirement to obtain explicit consent for new uses would unnecessarily encourage covered entities to draft broad disclosure language that would cover as wide a range of uses as possible. Such disclosures would be longer and less meaningful for consumers seeking to truly understand how their personal information may be used.

Section 999.305(d) restricts the sale of personal information collected from a source other than the consumer unless the business provides a notice at collection to the consumer or contacts the source, but this requirement has no statutory basis in the CCPA and is overly burdensome for businesses that share any information with third parties.

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

Section 999.306(a)(1) arguably suggests that a business that does not currently sell personal information must, nevertheless, build an intake function to collect opt outs from consumers who would like to prevent their personal information from being sold in the future.⁵ This is an unreasonable outcome for businesses that do not sell and could create a perverse incentive for businesses to decide to sell since they must build the opt-out infrastructure regardless of their

⁴ This same terminology is repeated in §§ 999.306, .307, .308, and the comment applies equally to each section.

⁵ Stating that “the purpose of the notice of right to opt-out of sale of personal information is to inform consumers of their right to direct a business that sells (or may in the future sell) their personal information to stop selling their personal information, and to refrain from doing so in the future.”

current practices. Further, recognizing that the statute does not speak to such a requirement, the OAG should remove from the proposed regulations all such forward looking obligations.

Section 999.306(b)(2) requires a business that *substantially* interacts with consumers offline to also provide the opt-out notice by an offline method. This vague standard does not define what qualifies as substantially offline to trigger the offline notice requirement.

§ 999.307. Notice of Financial Incentive

We request confirmation that businesses that do not offer financial incentives or a price or service difference in exchange for retention or sale of a consumer's personal information do not have to provide the Notice of Financial Incentive or related information in the privacy policy.

§ 999.308. Privacy Policy

Section 999.308(b)(1)(c) requires that the privacy policy include a description of "the process the business will use to verify the consumer request." For security reasons, this requirement should be removed. Describing the process for verification invites fraudsters to circumvent the measures that businesses must put in place to protect consumers. There is minimal additional consumer benefit to publishing the details of how the verification process works when businesses have a legitimate concern that providing too much information in a publicly facing document will put consumer security at risk.

We recommend removing Section 999.308(b)(1)(d)(2), which requires that the privacy policy include for each category of personal information collected, the categories of sources from which each category was collected, the business or commercial purpose for collecting each category, and the categories of third parties with whom the business shares each category of personal information. This disclosure requirement is overly burdensome, requiring businesses to specifically tie source, use, and recipients to each category of personal information collected, to no good effect, and attempts to impose a requirement on all personal information collected when the statute specifies that this degree of granularity only applies to personal information that the business has sold.⁶

Section 1798.115 treats information that the business sold differently from both the personal information that the business collected and the personal information that the business disclosed for a business purpose. Section 1798.115(a)(2) specifically states with regard to the personal information sold that the business must disclose "the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold." This different treatment is a logical consequence of the fact that the statute gives consumers the right to opt out of sale. A consumer exercising that right has an interest in knowing which information is sold to which third party. Because there is no right to opt out of collection or sharing for a business purpose, a lower level of granularity will provide a less complex and more meaningful disclosure to the consumer.

⁶ Section 1798.110 of the statute lists four categories of information that a business must provide regarding personal information the business has collected. Unlike Section 1798.115, this section does not require that the categories be cross-referenced against each other. In fact, cross-referencing the categories would create a lengthy and confusing document.

Section 999.308(b)(3) requires that the privacy policy for all covered entities disclose that a consumer has a right to opt-out of the sale of their personal information. If a business does not currently sell personal information, it should not be required to include such a disclosure in its privacy policy. The exemption provided in 999.306(d)(1) only applies if the business's privacy policy states that the business "does not and will not sell" the personal information. Without the forward-looking statement, a business that does not currently sell personal information would be required to provide the notice of opt out. This disclosure would be unnecessary, irrelevant to the business, and may lead consumers to wrongly believe that the business does in fact sell personal information when it does not.

Section 999.308(b)(5)(a) requires that a privacy policy explain how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf, but the proposed regulations do not make clear the level of information that a business must provide regarding the designation. For example, it is not clear whether a business must describe the requirements regarding agent request verification found at § 999.326, or whether they may be covered when a request is made. It is also unclear whether businesses may require particular forms or indicia of authority, such as powers of attorney.

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

Section 999.312(f) assigns to businesses the responsibility for redirecting responses that are not submitted through established channels and for advising a consumer how to remedy a deficient request. The section raises practical questions regarding the requirements for timing and tracking and should be removed.

The statute requires that a business implement at least two methods for submitting requests and, importantly, provide notices to consumers explaining how to make requests. Requests submitted outside of the options provided cannot be addressed in an efficient fashion, creating risk that the business cannot meet the deadlines established by the statute. For example, a request e-mailed to a local branch may not be timely routed to the appropriate location for response, but a business has limited options when it cannot provide a response within the 45 days allowed under the statute.⁷ Without the ability to control how requests are submitted, businesses may be challenged both to provide the extension notice within 45 days and to provide the response within 90 days.

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

§ 999.313(c)(5) requires a business, when a request to know is denied based on a conflict with federal or state law, to disclose to the consumer the basis for the denial. There may be times when the precise legal basis cannot be provided to the consumer because such a disclosure would itself violate law. To avoid this potential scenario, we suggest that the OAG include language in this paragraph clarifying that disclosing the existence of the conflict, without detailing the particular law or exception at issue, will be an adequate response under the regulation.

⁷ The regulation specifies that a business must respond to a request within 45 days, beginning on the day the business receives the request. If necessary, the business "may take up to an additional 45 days to respond to the consumer's request, for a maximum total of 90 days from the day the request is received." § 999.313(b).

Section 999.313(c)(6) requires a business to use reasonable security measures when transmitting personal information to the consumer. Our member companies recognize the importance of protecting personal information when it is being transmitted, and we request that compliance with this requirement constitute a safe harbor to any cause of action that alleges that the transmission resulted in unauthorized access, acquisition, destruction, modification or disclosure of personal information. Understanding that some consumers may choose to have their personal information delivered by mail, we request that the OAG confirm that delivery through the mail at the request of the consumer absolves the business of liability for any unauthorized access, acquisition, or disclosure of personal information that may occur after the personal information is placed in the mail. Moreover, we request that the OAG confirm that using security measures that the business uses in standard operating procedures, such as e-mail encryption and Secure Message Delivery, will meet this requirement and constitute reasonable security procedures and practices under the CCPA.

Section 999.313(c)(7) states that if a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal. We request verification that while a financial institution subject to the Gramm-Leach Bliley Act (GLBA) may use the secure portal for this purpose, it would not be required to deliver non-GLBA data through the consumer's GLBA account portal.

Section 999.313(d)(1) requires that if a business cannot verify the identity of a requestor seeking deletion it shall instead treat the request as a request to opt out of sales. This requirement has no statutory basis, and, in fact, runs counter to the CCPA's principles by giving control over consumer data based on unverified requests. The CCPA treats the right to delete and the right to opt out of sale of personal information as separate requests, with different statute sections and different exceptions. There is no legal basis to convert a deletion request to an unrequested, unrelated action because the requestor's identity could not be verified. If an identity cannot be verified, the only required action should be to inform the requestor of that fact.

Section 999.313(d)(3) allows a business to delay compliance with a request to delete, where personal information is stored in an archive or backup, until the archive or backup is next accessed. This requirement fails to recognize the technological complexity of database systems and the purpose of archives and backups. Information is generally archived with an established destruction date, determined by the type of data, when a business needs to retain it to meet business or legal requirements and maintain compliance with other state or federal laws. Backups, primarily used for disaster recovery, may never be accessed but may be overwritten on a regular schedule to retain current information. Without more clarity around the word "access," this language could require deletion when unrelated information is automatically added to the database or the database is accessed for purposes of maintenance or recovery.

A requirement to delete triggered by any access to the archive or backup is overly burdensome for businesses, as the next access to the archive or backup may be for unrelated information and not for the specific personal information requested. Accessing the archive or backup for other business needs wholly unrelated to the data subject to CCPA should not trigger a deletion requirement. We request that the deletion requirement for personal information in an archive or

backup system only trigger in the event that the business accesses such data with the intent to use it in the course of its day to day functions.

Section 999.313(d)(4) requires that a business specify the manner in which it has deleted the requestor's personal information. This requirement is burdensome, vague, and has no statutory basis. Deletion of information, especially in large businesses, can be complicated, involving several systems and business units, and a detailed description of this process does not serve the consumer. We recommend that this section only require a business to inform a consumer that the personal information has been deleted, or if it cannot be deleted, the reason why, consistent with the requirements of Section 999.313(d)(6).

§ 999.318. Training; Record-keeping

Section 999.317(g) requires a business that alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers to compile certain metrics regarding consumer requests and publish these metrics in the business' privacy policy. This section provides no further guidance as to how the 4,000,000 consumer threshold is calculated. We request that the OAG provide such guidance and that the guidance clarify that the calculation should not include consumers whose information is exempt from the CCPA's disclosure and deletion requirements, such as information subject to the Gramm-Leach Bliley Act, as including such information would skew the results and make the data effectively meaningless. Additionally, the public disclosure of these metrics would not further the purposes of the CCPA and could present fraud or cybersecurity risks. Instead, we recommend that these metrics be provided to the OAG upon request.

§ 999.318. Requests to Access or Delete Household Information

Section 999.318(b) requires a business to disclose or delete personal information for all members of a household if jointly requested. Businesses will not, however, be able to verify whether all members of a household agree to the request, particularly because the business has no practical way to know who all the members of the household are and to verify whether a request was actually received from all members. The broad definition of household members, in that it includes individuals of all ages and physical or mental capacity, regardless of relationship, means that a business can never be certain that a request to disclose or delete is made with appropriate authority. As a result, businesses cannot respond affirmatively to such a request, and this provision should be removed from the regulations.

§ 999.325. Verification for Non-Accountholders

Sections 999.325(b)-(d) require different tiers of authentication for right to know requests depending on the specific categories of personal information requested, but most identity verification techniques do not know how many data points will be needed for verification ahead of time, and most third party verification services do not provide this level of differentiation. The multiple verification tiers could increase the potential for mishandling consumer information. The regulations should allow businesses to instead set their own verification standards based on the business' own assessment.

Section 999.325(c) requires that consumers must submit a signed declaration under penalty of perjury to submit a request for specific pieces of personal information. We request further clarification regarding standards for these declarations, including whether the declaration must be notarized.

Accessibility and Language Requirements

The regulations require throughout—999.305(a)(2)c-d; 306(a)(2)c-d; 307(a)(2)c-d; 308(a)(2)c-d—that notices and privacy policies be accessible to customers with disabilities and available in the languages in which the business provides contracts, disclaimers, notices, sales, or other information. For businesses to have more certainty, the OAG should provide some additional clarity on the requirements for accessibility. For example, the regulations should clarify that if the documents are provided on a website that meets accessibility standards such as Web Content Accessibility Guidelines (WCAG) 2.0, it meets this requirement. We further request that the OAG provide additional clarity regarding how to apply the language requirement. For example, financial institutions may take assignment of installment sales contracts negotiated in other languages. Such contracts should not drive the languages for the financial institution’s notices and policies, particularly if the underlying contracts are subject to the GLBA exemption.

Deletion Requests in a 12-month Period

The CCPA, in providing consumers with the right to request their personal information, recognized that identifying and supplying personal data to the consumer places a burden on businesses. The statute requires the business to provide the information not more than twice in a 12-month period.⁸ The information must be provided at no charge to the consumer.⁹ If, however, the consumer makes more than two requests, the business can opt to charge the consumer for the administrative costs of fulfilling the request or refuse to take action if the requests are manifestly unfounded or excessive.¹⁰ This language suggests that more than two requests in a 12-month period can be considered excessive, and a business is not required to take action.

The CCPA does not expressly state that a consumer can only make two deletion requests in a 12-month period. However, for a business, the process of validating a consumer request, searching for personal information, evaluating whether the information is subject to an exception, deleting or destroying data, and responding to the consumer is not less burdensome than the effort that a business must put into responding to a disclosure request, and may actually be more burdensome. Accordingly, we request that the OAG clarify in the regulations that delete requests should be treated in the same manner as disclosure requests, and no more than two in a 12-month period should be required.

Look Back Period

The CCPA provides that a response to a disclosure request “shall cover the 12-month period preceding the business’s receipt of the verifiable request.”¹¹ A business also must include in its

⁸ 1798.100(d), 1798.130(b).

⁹ 1798.100(d); 1798.130(a)(2).

¹⁰ 1798.145(g)(3).

¹¹ 1798.130(a)(2).

online privacy policy “the categories of personal information it has collected about consumers in the preceding 12 months.”¹² This reference to a 12-month look back period is repeated in several other sections of the CCPA as well.

As noted above, the CCPA provides that the law is generally “operative” on January 1, 2020, notwithstanding that many sections became effective immediately upon enactment. The enforcement date adds additional confusion. The various dates for implementation raise questions about how the look back period should be treated when the law becomes enforceable. The OAG’s regulations should clarify that the look back period will not extend farther back than the effective date of the regulations because businesses will not have final and binding guidance for complying with their requirements until that date.

For example, a business is only required to respond to a disclosure request after receiving a verified request. A business cannot receive a verified request until the OAG regulations specify how businesses will determine that a request is valid. Additionally, in response to a disclosure request, a business must identify the information collected in the past 12 months by reference to the definition of personal information.¹³ However, the OAG’s final regulations may modify or expand the definition of personal information and unique identifiers.¹⁴ As a result, businesses will not be able to fully identify and categorize information until final regulations are published. Accordingly, businesses should not be required to look back beyond the effective date of the regulations to respond to a disclosure request.

Thank you in advance for your consideration of our comments. If you have any questions or would like to discuss this further, please do not hesitate to contact Matt Kownacki at AFSA at [REDACTED] or [REDACTED].

Sincerely,

/s/ Matthew Kownacki

Matthew Kownacki
Director, State Research and Policy
American Financial Services Association
919 Eighteenth Street, NW, Suite 300
Washington, DC 20006

/s/ David Knight

David Knight
Executive Director
California Financial Services Association
1127 11th Street, Suite 400
Sacramento, CA 95814

¹² 1798.130(a)(5)(B).

¹³ 1798.130(a)(3)(B); 1798.130(c).

¹⁴ 1798.185(a).



December 6, 2019

Submitted electronically in reference to the matter identified below, via PrivacyRegulations@doj.ca.gov

Subject: Alight Solutions LLC's Comments on:

- **The California Attorney General's ("AG") proposal to adopt sections §§ 999.300 through 999.341 of Title 11, Division 1, Chapter 20, of the California Code of Regulations (CCR) concerning the California Consumer Privacy Act (CCPA) (Published October 11, 2019)**

To Whom It May Concern:

Alight Solutions LLC ("Alight") is a leader in benefits, payroll and cloud solutions, supporting more than 3,250 clients, including 50% of the Fortune 500. On behalf of its clients, Alight serves 26 million people and their family members including more than 5.5 million defined benefit participants, nearly 5 million defined contribution participants, and over 11 million health and welfare plan participants.

We appreciate the Attorney General's effort to provide detailed regulations related to the California Consumer Privacy Act (CCPA), and the opportunity to submit comments. Through the services we provide for our clients and their people we are well-versed in the practical and regulatory factors impacting modern consumers and their data. We believe individual privacy and the security of people's personal information and data are critically important, and support clear standards for all stakeholders. However, we are concerned about cumbersome regulations that will result in confusion for individuals, companies, and regulators. In our view the proposed regulations further complicate the already broad CCPA. The proposed regulations also stretch the applicability of the law beyond the statutory definitions in contravention of California's Administrative Procedure Act ("APA"), CA Gov't Code Sec. 11340 *et seq.* We focus our comments on one of the proposed regulations that we expect could at minimum have unintended negative consequences on businesses, service providers, and consumers.

- I. We urge the AG to strike or clarify Section 999.314(a) related to service providers, which appears to significantly expand who is a covered service provider, create a direct conflict between service providers and any non-"business" client otherwise not covered by CCPA, and potentially subject such non-"business" clients to CCPA's requirements indirectly.**

The definition of "service provider" set forth in Section 1798.140(v) is a person or entity that processes "information on behalf of a **business....**" (emphasis added). Additionally, the term "business" is defined in Section 1798.140(c) to mean a for-profit entity that is covered by CCPA. As a result, an entity providing services to a company that is not a "business" will not be subject to CCPA's service provider requirements. Proposed regulation 999.314(a), however, does away with the "business" limitation in the express terms of the CCPA. As a result, entities not contemplated as "service providers" under the CCPA statute itself may nonetheless be deemed "service providers" for purposes of the regulations. We expect many entities that, for example, provide services to not-for-profits (or state, municipal, or other governmental units), will not be prepared to meet the service provider requirements of CCPA and that there will be conflict and confusion about this expansion. Additionally, the APA, does not seem to grant the AG the authority to enlarge the scope of the CCPA through regulation.

For entities that would not be service providers but for proposed regulation 999.314(a), or entities that are service providers but have clients that are a mix of “business” and non-“business” companies, this provision will either create a conflict with the non-“business” client over the need to comply regarding such client’s population, or effectively subject the non-“business” client to CCPA’s requirements by virtue of the deemed service provider status.

For example, in the event an entity was servicing clients that were not-for-profit companies, those clients may assert that they are not subject to CCPA; which would be accurate under both the text of the CCPA as well as the proposed regulations. The servicing entity would be holding the data of the non-profit clients, but does not own that data and generally would not take independent action regarding that data. However, if the servicing entity were to be deemed a service provider with regards to, in this example, non-profit clients, there may be a conflict between the responsibilities of a service provider under the CCPA and the direction provided by a non-profit client (not subject to the CCPA). The servicing entity would be caught between its own responsibilities under the CCPA and the non-profit client’s position that the CCPA does not apply to the client’s data. If the client directed, for example, that the service provider not respond or take any action on requests related to personal data obtained from that client’s employees, it is unclear how the service provider could assert that such action was required if the CCPA does not apply to the client who owns the data.

In addition to the deemed service provider’s conflicted position, a non-“business” client would be essentially forced to choose between voluntarily following the CCPA requirements despite it not applying or contending with the conflict and challenges described above.

For these reasons, we urge the AG to strike Section 999.314(a) from the proposed regulations and allow the statutory definitions of “business” and “service provider” to control. Although we believe this section should be struck and that failing to do so will have negative consequences, as an alternative, we suggest the AG, at minimum, clarify that when a service provider performs services for an entity that is not a business and to which the CCPA does not apply, the service provider may follow such entity’s otherwise lawful direction deviating from the CCPA with regards to any action otherwise required under the CCPA.

* * * * *

Thank you for the opportunity to submit these comments on the proposed regulations. Alight would welcome the opportunity to meet and discuss our comments in greater detail or to answer any questions that you may have.

Respectfully submitted,
Alight Solutions LLC

M. Garrett Hohimer
Assistant General Counsel & Director, Government Relations



Tola Sobitan
Chief Privacy Officer & Senior Counsel



Message

From: Holden, Robert A. [REDACTED]
Sent: 12/6/2019 8:21:06 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: American Association of Payers, Administrators and Networks Comments
Attachments: AAPAN's Comments to the California Office of the Attorney General on CCPA 12.6.2019.pdf

Please find our comments attached. Thank you for your consideration.

Robert A. Holden
[REDACTED]



December 6, 2019

Via Email to PrivacyRegulations@doj.ca.gov

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

RE: Comments Concerning the Proposed California Consumer Privacy Act Rules

Dear Coordinator:

I am writing on behalf of the American Association of Payers Administrators and Networks ("AAPAN") to comment on the proposed rulemaking implementing the California Consumer Privacy Act (CCPA). AAPAN is the leading national association of preferred provider organizations ("PPOs"), networks, and administrators providing services to health plan enrollees, self-funded employer plans, and injured workers. Through our members, we work on behalf of thousands of California residents. Our comments on the rulemaking are addressed towards gaining greater clarity on how the rules will address information exchanged between covered entities, business associates, and health care providers subject to federal regulations pursuant to the Health Insurance Portability and Availability Act of 1996 (HIPAA).

Clarifications on the Application of Rules Pursuant to CCPA Section 1798.145

AAPAN members would like to seek clarification in the application of CCPA section 1798.145(c)(1) concerning the responsibility of a "Business Associate" as it relates to a "Covered Entity" as both those terms are defined and regulated under 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e). Many AAPAN members are Business Associates under HIPAA and they would like clarification as to the extent of the exemptions provided under CCPA 1798.145, so long as their activities as Business Associates support a Covered Entity's obligation to patients. In particular, would like to understand how these exemptions extend to the exchange of health care provider personal information which may not be considered PHI. This is additionally instructive should the business to business exemptions under the CCPA sunset.

Claims Processing and the Provider Exclusion

Many AAPAN members process claims on behalf of a Covered Entity. This results in two questions as to the application of the exemption under CCPS section 1798.145. First, we would

Message

From: Dan Jaffe [REDACTED]
Sent: 12/6/2019 2:48:04 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: ANA Detailed Comments on Proposed CCPA Regulations
Attachments: ANA Comments on Proposed CCPA Regulations FINAL.pdf
Importance: High

Dear Attorney General Becerra,

Attached please find detailed comments by the Association of National Advertisers (ANA) in response to your office's proposed regulations regarding the California Consumer Privacy Act (CCPA). We hope that you will take this document under careful consideration and work to make the CCPA better for both consumers and businesses.

If you have any questions please feel free to reach me at [REDACTED] or by calling the Washington Office of ANA at [REDACTED]

Best wishes,
Dan Jaffe

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
2020 K Street N.W. Suite 660
Washington DC 20006



Visit my [Regulatory Rumbblings Blog](#)





LEADERSHIP AND
MARKETING EXCELLENCE

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

COMMENTS

of the

ASSOCIATION OF NATIONAL ADVERTISERS

on the

California Consumer Privacy Act Proposed Regulations

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

Counsel:
Stu Ingis
Mike Signorelli
Tara Potashnik
Allaire Monticollo
Venable LLP
600 Massachusetts Ave., NW
Washington, DC 20011
[REDACTED]

December 6, 2019

On behalf of the Association of National Advertisers (“ANA”), we provide the following comments in response to California Office of the Attorney General’s (“CA AG”) October 11, 2019 request for public comment on the proposed regulations implementing the California Consumer Privacy Act (the “CCPA”).¹ We appreciate the opportunity to engage with the CA AG on the important subject of consumer privacy and the content of the rules that will help implement the CCPA.

ANA participated in the CA AG’s preliminary rulemaking public forums in San Marcos on January 14, 2019 and Sacramento on February 2, 2019, and ANA also testified at a February 20, 2019 informational hearing on the CCPA held by the California State Assembly Committee on Privacy and Consumer Protection. In addition, ANA participated in the CA AG’s December 4, 2019 San Francisco public hearing to offer input on the proposed regulations. We and our members are committed to helping ensure that consumers enjoy meaningful privacy protections in the marketplace and that businesses can continue operations that support and sustain the California economy.

The ANA’s mission is to drive growth for marketing professionals, for brands and businesses, and for the industry. Growth is foundational for all participants in the ecosystem. The ANA seeks to align those interests by leveraging the 12-point ANA Masters Circle agenda, which has been endorsed and embraced by the ANA Board of Directors and the Global CMO Growth Council. The ANA’s membership consists of more than 1,600 domestic and international companies, including more than 1,000 client-side marketers and nonprofit organizations and 600 marketing solutions providers (data science and technology companies, ad agencies, publishers, media companies, suppliers, and vendors). Collectively, ANA member companies represent 20,000 brands, engage 50,000 industry professionals, and invest more than \$400 billion in marketing and advertising annually. The vast majority of them are either headquartered, or do substantial business, in California.

The issues and problems we highlight concerning the CCPA and the proposed regulations in the ensuing comments, if not remedied, could have grave and substantial effects on consumers. Every point we discuss below may have significant and detrimental consequences to consumers by threatening their ability to access products and services they enjoy and expect. The CCPA is poised to impose limitations on the free flow of data that has fueled the economy for decades and has empowered consumers to receive appropriate products and services in the right place and at the right time. Data has created untold consumer benefit by enabling free and low-cost services and has directly facilitated consumers’ exposure to new products and offerings that may interest them. The CCPA stands to detrimentally impact this status quo and could curtail the use of data that has improved consumers’ lives and enriched their experiences.

Our members support the responsible use of data and the underlying goal of enhancing consumer privacy that is inherent in the CCPA and the CA AG’s proposed rules. For decades, our industry has championed consumer transparency and choice regarding businesses’ data practices, including by promoting strong codes of conduct and self-regulatory programs. ANA has, for example, supported the Digital Advertising Alliance’s (“DAA”) consumer-centric notice

¹ California Department of Justice, *Notice of Proposed Rulemaking Action* (Oct. 11, 2019), located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf>.

and choice program and its corresponding Self-Regulatory Principles for Online Behavioral Advertising for over ten years.² There have been over 100 million unique visits to the DAA self-regulatory site for consumers to exercise their privacy choices. In addition, ANA is the home of the Guidelines for Ethical Business Practice, a self-regulatory code designed to provide individuals and entities in all media that are involved in data-driven marketing with generally accepted principles of conduct.³ ANA has consistently maintained and reinforced industry standards that place responsible data practices and consumer privacy at the forefront of business considerations.

ANA members also play a significant role in the California economy. For example, in California, advertising helps generate \$767.7 billion or 16.4% of the state's economic activity and helps produce 2.7 million jobs or 16.8% of all jobs in the state.⁴ Moreover, many of our members employ California residents and nearly all of them provide goods and services to consumers in the state. It is no secret that advertising and marketing contribute to the health and growth of the economy overall. ANA-member businesses are committed to affording California consumers robust privacy protections while also continuing to bolster and enrich the state's economic activity and employment.

The underlying principles of transparency, control, and accountability included in the CCPA are aligned with ANA members' values. Several clarifications the CA AG provided in its proposed rules have offered helpful guidance for businesses in furthering CCPA compliance. Other provisions, however, set forth in the proposed rules represent departures from the text and scope of the CCPA as enacted by the legislature and could stand to decrease consumer choice and privacy rather than advance it. Additionally, because the CA AG's own timetable for the rulemaking makes clear that it is highly unlikely to finalize the rules implementing the law before its January 1, 2020 effective date, businesses could have significant difficulties complying accurately with the CCPA without the benefit of the finalized rules. The CCPA represents a highly complex and in many respects ambiguous law, and without final rules to sufficiently clarify its terms in advance of its effective date, the CCPA could prove to be extremely disruptive to consumers and business alike.

The Standardized Regulatory Impact Assessment, put forward by the CA AG's Office, on the CCPA highlights the costs the law could impose on the California economy.⁵ According to the assessment, the initial costs for state businesses to comply with the CCPA could be as high as \$55 billion, equivalent to 1.8% of California Gross State Product in 2018. The report also estimates that the additional costs to comply with the CA AG's regulations implementing the law could reach \$16.454 billion over the next decade, depending on the number of businesses impacted. It is clear from the impact analysis that the CCPA could have a substantial impact on

² DAA, Self-Regulatory Principles for Online Behavioral Advertising (Jul. 2009), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/seven-principles-07-01-09.pdf.

³ ANA, Guidelines for Ethical Business Practice (2017), located at <https://thedma.org/accountability/ethics-and-compliance/dma-ethical-guidelines/>.

⁴ IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at <https://www.ana.net/magazines/show/id/rr-2015-ihs-ad-tax>.

⁵ State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* (Aug. 2019), located at http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

the state's business community and economy, effects that would also be felt elsewhere in the country. The report's wide-ranging estimates of future costs reflect the uncertainty and potential disruption the law presents for businesses, regulators, and consumers. ANA urges the CA AG to work to reduce the economic and operational burdens of the CCPA while maintaining privacy protections for consumers.

As our members continue to design systems, policies, and technical processes to operationalize the CCPA, the industry would benefit from additional clarity surrounding certain provisions in the law and the proposed regulations so businesses can facilitate the regime's consumer rights and provide notice and choice consistent with its requirements. Moreover, the CA AG should take steps to ensure the final regulations, when promulgated, align with the text and scope of the CCPA. We provide the following suggestions to the CA AG to clarify certain points of the CCPA and proposed regulations, and we encourage the office to update parts of the proposed rules to better align with the CCPA itself and to ensure consumers have the ability to make meaningful choices. Our comments first address three issues of paramount importance that we raised in San Francisco at the CA AG's December 4, 2019 public hearing on the content of the proposed rules. The remainder of our comments are organized thematically, addressing several topics in a number of general issue areas. Our comments proceed by discussing the following:

- I. Issues ANA Addressed in its December 4, 2019 Verbal Testimony
- II. Consumer Requests to Opt Out and Opt In to Personal Information Sale
- III. Consumer Requests to Know and Delete
- IV. Service Providers
- V. Consumer Verification
- VI. Privacy Policies
- VII. Other Required Notices
- VIII. Provisions of the Proposed Regulations that ANA Supports

I. Issues ANA Raised in its December 4, 2019 Verbal Testimony

a. Clarify Requirements Surrounding Loyalty Programs So Businesses May Continue to Offer Such Programs to Consumers

Per the proposed rules, a business may offer a price or service difference, *i.e.*, a loyalty program, to a consumer if the difference is reasonably related to the value provided to the business by the consumer's data.⁶ The proposed regulations also require businesses to include a good-faith estimate of "the value of the consumer's data," which is defined as "the value provided to the business by the consumer's data," in addition to the method of computing such value, in a notice of financial incentive before they may offer loyalty programs.⁷ The CA AG should clarify how a business may justify that a price or service difference is reasonably related to the value provided to the business by the consumer's data. The CA AG should further clarify that a business does not need to provide the method of calculating the value of a consumer's data or a good faith estimate of such value in a notice of financial incentive if this information would constitute confidential, proprietary business information or put the business's competitive position at risk. At a minimum, the CA AG should clarify that a business may provide an estimate of the aggregate value of consumer data instead of an estimate of the value of data pertaining to an individual consumer to satisfy this requirement.

Consumers participate in loyalty and rewards programs on an opt-in basis. Consumers understand that as they provide data to businesses in order to participate in loyalty programs, they obtain value through those programs by gaining access to lower prices and special offers. Loyalty programs take many different forms. For example, gas dollar programs, frequent flyer programs, grocery "valued customer" rewards, and many other similar offerings constitute loyalty programs that could be hindered in California due to the CCPA. Consumer data makes loyalty programs possible, but consumers who make deletion or opt out requests restrict the very data that allows them to participate in loyalty programs. The proposed regulations' requirement for businesses to ensure that any price or service difference offered to consumers is reasonably related to the value they receive from consumer data constitutes a requirement that may be impossible for businesses to meet. As a result, this requirement has the potential to impede the offering of loyalty programs that consumers enjoy and have come to expect. Without clarification on how businesses may reasonably justify that a price or service difference is reasonably related to the value provided to the business by the consumer's data, many loyalty programs could cease altogether when the CCPA becomes effective on January 1, 2020.

In addition, if a business offers a financial incentive or a price or service difference to a consumer, the business must provide a notice of the financial incentive that offers (1) "a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and" (2) "a description of the method the business used to calculate the value of the consumer's data."⁸ While the proposed regulations clarify that "the value of the consumer's data" is the value provided to the business by such data, the requirement to provide an estimate of such value is unworkable. It is unclear whether a financial incentive

⁶ Cal. Code Regs. tit. 11, §§ 999.336(b), 337(a) (proposed Oct. 11, 2019).

⁷ *Id.* at §§ 999.307(b)(5)(a), 337(a).

⁸ *Id.* at § 999.307(b)(5).

must justify the price or service difference offered to consumers on a product-by-product basis (e.g., discounts for coffee must be justified independently and separately from discounts for pastries), or if businesses may justify their price or service differences for CCPA purposes in a more holistic sense. The method by which a business values personal information associated with a consumer may vary based on the situation at hand, the discount being offered at a particular time or in a particular place, and a variety of other factors. Additionally, the actual value the business attributes to such data may, in many cases, be difficult to quantify.

From an operational standpoint, the value provided to a business by data pertaining to consumers may be calculated on an aggregate basis rather than an individual consumer basis. The proposed regulations do not clarify whether a business may satisfy the nondiscrimination and financial incentive requirements by providing an estimate of the *aggregate value* of data as opposed to an estimate of the value of data pertaining to an individual consumer. The proposed regulations also do not account for how businesses should quantify nontangible value created in terms of fostering consumer loyalty and goodwill. Several varying and proprietary considerations make these calculations complex and have the potential to confuse consumers rather than enlighten them to business practices. ANA encourages the CA AG to revise the draft rules to explicitly state that a business may satisfy the nondiscrimination and financial incentive requirements by providing an estimate of the aggregate value of consumer data as opposed to an estimate of the value of data pertaining to an individual consumer.

Moreover, the requirement to include an estimate of “the value of the consumer’s data” and the method of calculating such value could reveal confidential information about a business that could jeopardize the business’s competitive position in the marketplace. Information about the value the business attributes to the consumer’s data and the method of calculating the value could constitute proprietary information about businesses’ commercial practices. A requirement to divulge this information risks distorting the market by forcing companies to reveal confidential data. In many instances, such calculations could harm businesses if divulged, as they would reveal proprietary or confidential information to competitors. Consequently, the requirement to disclose a reasonable estimate of the value of the consumer’s data and the business’s method for calculating such data presents significant risks to competition and business proprietary information. The CA AG should clarify how a business may justify that a price or service difference is reasonably related to the value provided to the business by the consumer’s data so that businesses may continue to offer loyalty programs to consumers. In addition, we ask the CA AG to clarify that businesses need not provide the method by which they calculate “the value of the consumer’s data” or the actual estimated value if such a disclosure could lead to anticompetitive consequences in the marketplace, or, at the very least, businesses may satisfy this requirement by providing an estimate of the aggregate value of consumer data instead of an estimate of the value of data pertaining to an individual consumer. Consumers clearly see the value of loyalty programs as demonstrated by the broad participation in such programs by both California consumers and the country at-large. Therefore, rules in regard to these programs should be carefully calibrated so as to not undermine their value to consumers.

b. Clarify that Intermediaries Must Allow Consumers to Express Opt Out Choices Through Browsers and May Not Block Opt Out Selections

According to the proposed regulations, a business that collects personal information from consumers online must treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt out of the sale of personal information as "a valid request submitted... for that browser or device, or if known, for the consumer."⁹ This requirement goes beyond the intent of the legislature and scope of the CCPA. It represents an entirely new business duty that does not further the purposes of the CCPA, but rather exceeds the law's scope by imposing material obligations on businesses that have no textual support in the statute. The legislature previously considered browser settings when it amended California Online Privacy Protection Act ("CalOPPA") in 2013, and at the time chose to not mandate a single, technical-based approach to effectuating consumer choice.¹⁰ Instead, the legislature offered alternative approaches, which is best for consumer and businesses. The legislature could have included such a mandate when it passed the CCPA and amended the law in September of 2018 and 2019, but each time chose not to. The CCPA itself does not direct the CA AG to implement such rules or such an approach. ANA believes that mandating that businesses honor the suggested signals undermines consumer choice and could harm consumers. Such tools are a blunt instrument broadcasting a single signal to all businesses. Consumers are not provided an option to set granular choices, business-by-business selections, allowing certain business to sell data while restricting others. This does not allow a consumer to maximize their enjoyment and participation in the data economy. In addition, a business is not able to authenticate whether a consumer has affirmatively set such signals. Such tools are ripe for intermediary tampering.

If the CA AG nevertheless pursues this approach, we suggest that the CA AG adopt a rule that requires a business engaged in the sale of personal information to either: (1) honor browser plugins or privacy settings or mechanisms, or (2) not be required to honor such settings where the business includes a "Do Not Sell My Info" link and offers another mechanism or protocol for opting out of sale by the business. This approach would be consistent with CalOPPA and the CCPA, as passed by the legislature. It would also provide consumers with meaningful choices.

Regardless of the mechanism offered to effectuate a consumer opt out, the CA AG's rules should protect the signals set by the consumer. Some browsers, operating systems, and other intermediaries have the ability to interfere with consumers' ability to use choice tools via the Internet. This interference can occur when these intermediaries block the technology that is used to signal an opt out (*e.g.*, cookies, JavaScript, mobile ad identifiers, etc.), often through default settings. When browsers take cookie and other technological opt out tools out of the equation, consumers are ultimately harmed because their opt out preferences fail to be communicated to the business. If consumers are unable to deliver a choice signal to a business due to an intermediary's blockage of the technology used to signal that choice, meaningful consumer choice would be removed from the marketplace.

c. Remove the Requirement For Businesses to Pass Consumer Opt Outs to Parties to Whom They Sold Personal Information in the Prior 90 Days

⁹ *Id.* at § 999.315(c).

¹⁰ AB 370 (Cal. 2013).

Per the proposed rules, upon receipt of a consumer opt out request, a business must: (1) “notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business’s receipt of the consumer’s request that the consumer has exercised their right to opt-out,” and (2) “instruct [the third parties] not to further sell the information.”¹¹ This provision places requirements on businesses to communicate opt out requests to third parties and instruct those third parties not to further sell information, which are obligations that are not included in the CCPA. To avoid regulatory provisions that are not within the scope of the statutory text of the CCPA and could cause significant unintended consequences that could result from these entirely new business obligations, the CA AG should update the proposed regulations to align with the CCPA such that businesses are not required to pass opt out requests along to third parties. At a minimum, the CA AG should clarify that businesses are not required to pass opt out requests along to third parties if such third parties are contractually prohibited from selling personal information received from the business.

First, requiring businesses to communicate opt out requests to third parties is a significant new requirement imposed by the CA AG after businesses have spent over a year designing novel, resource-intensive, and costly processes and technical controls for the CCPA. The requirement exceeds the law’s scope by levying entirely new substantive obligations on businesses without a basis in the CCPA to do so, and it does nothing to “further the purposes of the title,” which the California legislature has required of all regulations implementing the CCPA. As a result, the CA AG’s implementation of a new requirement to pass opt outs along to third parties represents a substantial change from the text of the CCPA and is outside of the scope of the law. It does not provide businesses with enough time to build the systems necessary to accomplish this requirement before the law’s January 1, 2020 effective date. Moreover, the new requirement to pass opt out request to third parties is unclear and may be contrary to consumers’ actual preferences. The requirement is also superfluous and unnecessary, as the CCPA itself already addresses downstream data sales by requiring third parties that receive personal information from a sale to ensure the consumer has received explicit notice and an opportunity to opt out of future sales.¹² Consequently, third party businesses are already obligated under the CCPA to offer consumer rights with respect to personal information.

Second, the proposed regulations’ mandate that businesses must communicate opt out requests to third parties does not serve to further meaningful consumer choice. If a consumer opts out of one business’s ability to sell personal information, that business should not be obligated to proliferate that request to other third parties. In addition, if third parties effectuate the opt out requests they receive from a business that the consumer originally directed to the business alone, consumers stand to lose access to products, services, and content that they did not wish to lose access to by sending an opt out request to a business. The outcome the CA AG is proposing with this opt out flow-down provision is not reflective of consumer choice; it would take the consumer’s expressed choice in one instance and apply that choice to others. The CCPA should enable consumers to choose which businesses and third parties can and cannot sell personal information. The law should not structure a system that interprets a consumer’s opt out choice with respect to one business as a choice that should apply across the entire marketplace.

¹¹ Cal. Code Regs. tit. 11, § 999.315(f) (proposed Oct. 11, 2019).

¹² Cal. Civ. Code § 1798.115(d).

Finally, the requirement to pass opt out requests on to third parties is not practical given the modern data-driven advertising ecosystem. This new obligation could require businesses to terminate rights to data they have already passed on to third parties. This limitation would stifle the free flow of data that powers the economy, thereby decreasing consumers' access to products and services. In the context of online commerce, the requirement would threaten to break the Internet by decreasing the amount of advertising revenue available to subsidize the online content consumers enjoy and have come to expect, particularly if third parties must further pass consumers' initial opt out selections down the chain to other third-party businesses. This requirement could also cause economic and valuation issues, as the potential would always exist for a third-party data recipient to lose their rights to use or further sell the data they have lawfully acquired from businesses. Businesses would not be able to reliably quantify their products and services, and the overall economy could suffer as a result. ANA therefore respectfully asks the AG to update the proposed rules so businesses are not required to pass opt out requests along to third parties in the prior 90 day period.

II. Consumer Requests to Opt Out and Opt In to Personal Information Sale

a. Remove the Requirement for Businesses that Do Not Collect Information Directly to Obtain Examples of Notices Provided to Consumers by Data Sources

The proposed regulations state that businesses that do not collect information directly from consumers do not need to provide a notice at collection.¹³ Before selling personal information, however, the proposed rules state that such businesses must: (1) contact the consumer to provide notice of sale and notice of the opportunity to opt out; or (2) obtain signed attestations from the data source describing how it provided notice at collection, including an example of the notice; maintain those attestations for a two-year period; and make them available to consumers upon request.¹⁴ The CA AG should update the proposed rules so that entities may rely on contractual attestations from the business who passed the data along to them and do not need to obtain and maintain examples of the notice provided to consumers before engaging in personal information sale. In addition, a business should not be required to produce the attestations it receives from data sources or any sample notices it may be required to maintain to a consumer in response to an access request.

The CCPA itself only requires third parties to provide consumers with “explicit notice” and an opportunity to opt out of the sale of personal information.¹⁵ Moreover, the consumer benefit achieved by the obligation to maintain examples of the notices provided to consumers is unclear, and this requirement would be extremely burdensome for entities to manage. Mandating that entities must receive contractual attestations from the data source that the consumer was notified before engaging in information sale provides the consumer with the same benefit as requiring businesses to maintain an example of the notice. Both achieve the goal of consumer transparency, and consumers' knowledge of data practices would not be enhanced by requiring businesses to maintain examples of the notice provided to specific consumers.

¹³ Cal. Code Regs. tit. 11, § 999.305(d) (proposed Oct. 11, 2019).

¹⁴ *Id.*

¹⁵ Cal. Civ. Code § 1798.115(d).

Furthermore, this provision could be interpreted to require businesses to pass example notices down the chain from the original source of data to other businesses who may receive personal information as part of the process. This would undermine privacy protections rather than enhance them. In dynamic data markets such as the one that powers the Internet, it is impossible to pass model notices to third parties and provide a taxonomy for tracking notices and tying them to the data source. For instance, in a programmatic market where billions of data transactions are occurring in the matter of seconds, there is no reasonable method of passing along model notices to entities that receive data. This requirement is therefore unclear, unrealistic, and would be difficult if not impossible for businesses to satisfy.

Moreover, businesses should not be required to return the sample notices they may be required to maintain or the attestations they receive from data sources to consumers in response to access requests. This requirement is not based in the CCPA, does nothing to further the purposes of the law, and provides no discernible consumer benefit. In fact, it could expose proprietary business terms to the public, thereby harming businesses' ability to compete or transact in the marketplace. It is also operationally impractical for businesses to be able to link a particular data point to a particular consumer whose data was received under a particular contractual term. The costs that would be associated with such a process far exceed the benefit that would be provided to the consumer. The California legislature determined that businesses are not required to disclose the specific source of data to consumers in response to access requests when it structured the CCPA to require the disclosure of *categories of sources* of personal information only. Any requirement to return attestations from data sources or sample notices to consumers would render this CCPA term moot by having the practical effect of requiring businesses to disclose specific sources of personal information.

If the goal of Section 999.305(d) of the proposed regulations is to provide California consumers with additional notice of their opportunity to exercise rights under the CCPA, this aim can be accomplished in much less burdensome ways. The CA AG should clarify that businesses need not obtain examples of notices provided to consumers by data sources in order to engage in personal information sale under the CCPA and do not need to return the attestations they receive from data sources or the sample notices they may be required to maintain to consumers in response to access requests.

b. Clarify the Requirement to Obtain Parental Consent for Minors “in addition to” Verifiable Parental Consent Under the Children’s Online Privacy Protection Act (“COPPA”)

Per the proposed regulations, a business that has actual knowledge it collects or maintains the personal information of children under the age of thirteen must establish, document, and comply with a reasonable method for determining that a person affirmatively authorizing the sale of personal information about the child is the parent or guardian of the child.¹⁶ Such affirmative authorization must be “in addition to” any verifiable parental consent required under COPPA, according to the proposed rules.¹⁷ ANA asks the CA AG to clarify how this “additional” CCPA

¹⁶ Cal. Code Regs. tit. 11, § 999.330(a)(1) (proposed Oct. 11, 2019)

¹⁷ *Id.*

consent must function in practice by issuing a rule stating that a business may send one consent communication with separate check boxes for CCPA and COPPA-related consents.

In describing the requirement for parents or guardians of children under age thirteen to affirmatively consent to the sale of a child’s personal information, the proposed regulations list acceptable consent mechanisms that mirror the acceptable verifiable parental consent mechanisms that are set forth in the COPPA Rule.¹⁸ However, the proposed regulations explicitly state that any CCPA-related affirmative authorization from a parent or guardian to sell a child’s personal information must be *in addition to* any consents obtained under COPPA. It is therefore unclear how businesses must obtain such additional or separate consents. Moreover, it is unclear the extent to which COPPA could preempt the requirement to obtain affirmative authorization to sell personal information that is included in the CCPA.

The CA AG should permit a business to provide one consent mechanism that is acceptable under both the CCPA and COPPA to a parent or guardian that contains separate consent check boxes pertaining to the activities that require consent under each law. The proposed rules should not require a business to send two, completely separate consent communications or requests to a parent or guardian to obtain verifiable parental consent under COPPA and affirmative authorization pursuant to the CCPA. The “additional” consent requirement in the proposed rules also creates ambiguities when it comes to interpreting parents’ choices, as it is unclear what should happen if a consumer consents to personal information sale under the CCPA but rejects personal information collection, use, or disclosure under COPPA. ANA requests that the CA AG clarify this issue, preferably by stating that a business may send one consent request with separate check boxes for CCPA and COPPA-related consents.

III. Consumer Requests to Know and Delete

a. Ensure the Definition of “Request to Know” Aligns with the Text of the CCPA

The proposed regulations state that a “request to know” (*i.e.*, an access request) is “a consumer request that a business disclose personal information that it *has* about the consumer...”¹⁹ The definition includes a request for “specific pieces of personal information that a business *has* about the consumer.”²⁰ This provision departs from the text of the CCPA, which notes that a consumer has the right to request that a business disclose “[t]he categories of personal information it has *collected* about that consumer” and “[t]he specific pieces of personal information it has *collected* about that consumer.”²¹ ANA requests that, consistent with the text of the CCPA, the CA AG clarify that requests to know apply only to personal information *collected* about a consumer.

The CA AG should clarify that requests to know apply to personal information that a business has collected about a consumer. This update would bring the proposed regulations into conformity with the text of the CCPA. In its Initial Statement of Reasons describing the

¹⁸ *Id.* at § 999.330(a)(2); 16 C.F.R. § 312.5(b).

¹⁹ Cal. Code Regs. tit. 11, § 999.301(n) (proposed Oct. 11, 2019) (emphasis added).

²⁰ *Id.* at § 999.301(n)(1) (emphasis added).

²¹ Cal. Civ. Code § 1798.110(a)(1) (emphasis added).

proposed regulations, the CA AG noted its intent in providing a definition of “request to know.”²² The CA AG did not indicate a desire to alter the requirements of the CCPA in this description of its intent. Instead, the CA AG said it provided a definition of request to know to “allow... the regulations to group together the requirements businesses must follow,” suggesting the intent was to improve convenience and readability rather than substantively change the requirements of the law. The CA AG also stated that it provided a definition of request to know to offer further clarity and to avoid unnecessary confusion. As a result, it does not appear that the CA AG intended to change the meaning of the CCPA or create ambiguity by issuing this provision of the proposed regulations. ANA asks the CA AG to the extent practical to harmonize the language of the proposed rules with the text of the CCPA. This would help reduce confusion for businesses implementing the CCPA’s requirements. Therefore, ANA urges the CA AG to update the proposed rules’ definition of “request to know” so that requests for personal information apply to “personal information that a business has *collected* about the consumer” and “specific pieces of personal information that a business has *collected* about a consumer.” ANA submits this suggested clarification to the CA AG to help ensure that the regulations align with the text of the CCPA.

b. Clarify Required Methods for Submitting Requests to Know for Businesses that “Primarily Interact” with Customers at Retail Stores

The proposed regulations state that a business that operates a website but primarily interacts with customers in person at a retail location must offer three methods to submit requests to know: a toll-free number, an interactive webform accessible through the website, and a form that can be submitted in person at the retail location.²³ This directive is unclear and presents major challenges to businesses for two primary reasons.

First, the proposed regulation provides no guidance about how to determine the way a business “primarily” interacts with consumers. Today, very few businesses may “primarily” interact with consumers in retail locations, as most purchases and commercial interactions occur online. Second, requiring retail businesses to allow consumers to submit such requests in person through a physical form would create excessive burdens in terms of employee training and could cause customer service issues and disruptions to consumers through long lines at retail stores. In the retail industry, many employees are seasonal and may not have enough institutional knowledge or training to effectively and efficiently facilitate these in-person CCPA requests.

The CA AG should clarify that businesses that have websites but interact with customers in retail locations need to provide a toll-free number and a webform only for consumer requests and may direct consumers to such methods of submitting requests if they receive an inquiry about submitting CCPA requests in person at a retail store. The toll-free number and webform method of submitting requests would allow retail companies to cultivate employees with an expertise in managing CCPA requests received by phone or online and would allow for more well-trained individuals to provide accurate and helpful responses to consumer inquiries.

²² Office of the California Attorney General, *Initial Statement of Reasons for Proposed Adoption of California Consumer Privacy Act Regulations 6-7* (Oct. 2019) (hereinafter, “ISOR”), located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf>.

²³ Cal. Code Regs. tit. 11, § 999.312(c)(2) (proposed Oct. 11, 2019).

c. Ensure the Definition of “Request to Delete” Aligns with the Requirements Businesses Must Meet in Describing Such Requests

According to the section of the proposed regulations that addresses information a business must include in its privacy policy, a business must “[e]xplain that the consumer has a right to request the deletion of their personal information collected *or maintained by the business*.”²⁴ This provision is inconsistent with the proposed regulations’ definition of a “request to delete,” and it appears to require businesses to state in their privacy policies that consumers have a different right than the CCPA and proposed regulations afford them. We ask the CA AG to clarify that a business must provide a privacy policy disclosure regarding requests to delete that is consistent with the proposed regulations’ definition of the term and with the CCPA itself.

The proposed regulations state that a “request to delete” is “a consumer request that a business delete personal information about the consumer that the business has *collected from* the consumer....”²⁵ This definition matches the formulation of the deletion right in the CCPA itself, which states that “[a] consumer shall have the right to request that a business delete any personal information about the consumer which the business has *collected from* the consumer.”²⁶ The CA AG’s Initial Statement of Reasons for adopting draft CCPA regulations also mirrors this construction of the deletion right.²⁷ However, per the proposed regulations, a business must disclose in its privacy policy that a consumer has a right to request deletion of personal information maintained by the business.²⁸ This disclosure is not tied to personal information that was collected from a consumer. This mandated privacy policy disclosure clearly does not track with the language describing the right to delete in the proposed regulations or the CCPA itself.

Consistent with the CCPA and the CA AG’s definition of “request to delete” in the proposed regulations, the CA AG should clarify that a business must disclose that a consumer has a right to request the deletion of personal information about the consumer which the business has *collected from* the consumer in its privacy policy. This change would bring the proposed regulations in line with the text of the CCPA and would refrain from causing unnecessary confusion for businesses in their efforts to create mechanisms to comply with the law’s terms.

d. Remove the Requirement to “Permanently and Completely” Erase Personal Information

The proposed regulations state that a business must comply with a consumer’s request to delete personal information by de-identifying the personal information, aggregating the personal information, or “permanently and completely erasing” the personal information on its existing systems.²⁹ We ask the CA AG to remove the “permanently and completely erasing” language, because it represents a substantive requirement that is not grounded in the text of the CCPA,

²⁴ *Id.* at § 999.308(b)(2)(a) (emphasis added).

²⁵ *Id.* at § 999.301(o) (emphasis added).

²⁶ Cal. Civ. Code § 1798.105(a) (emphasis added).

²⁷ ISOR at 7.

²⁸ Cal. Code Regs. tit. 11, § 999.308(b)(2)(a) (proposed Oct. 11, 2019).

²⁹ *Id.* at § 999.313(d)(2).

does nothing to further the purposes of the law, imposes significant compliance challenges for businesses, and may conflict with other provisions of the proposed regulations.

The “permanently and completely erasing” language sets forth a requirement that goes far above and beyond what is required in the CCPA, which states that a consumer has “the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.”³⁰ In addition, the requirement creates compliance challenges for businesses, because businesses may use certain database systems or architectures that do not allow for “permanent and complete” deletion. Furthermore, the requirement to “permanently and completely” delete personal information could conflict with the proposed regulations’ recordkeeping requirements, which obligate businesses to “maintain records of consumer requests made pursuant to the CCPA and how the business responded to said requests for at least 24 months.”³¹ As such, the “permanently and completely erasing” language is unnecessarily limiting and challenging for businesses to effectuate, and we ask the CA AG to remove this language from the text of the proposed rules.

e. Clarify Businesses May Provide a General Contact Toll-Free Phone Number for Receiving Consumer CCPA Requests

The proposed rules require a business to provide a toll-free phone number as a method for receiving “requests to know” and note that a business may provide one for receiving requests to delete and opt out.³² The CA AG should clarify that a business may provide a toll-free general help or contact number to consumers to make CCPA requests and need not provide a CCPA-specific toll-free number. Requiring businesses to create a separate phone number for CCPA requests would create consumer confusion by forcing them to submit requests unrelated to the CCPA through one phone number and CCPA-related requests through another. It would also increase costs for businesses, which would have to maintain and staff a separate phone number for CCPA-related requests. As such, the CA AG should clarify that a business may provide its main consumer telephone number as the toll-free phone number through which it may receive consumer CCPA requests.

IV. Service Providers

a. Place Reasonable Limits on the Service Provider Requirement to Provide Business Contact Information Upon Receipt of a Request to Know

Per the proposed rules, a service provider that receives a request to know or a request to delete from a consumer must “inform the consumer that it should submit the request directly to the business on whose behalf the service provider processes the information and, when feasible, provide the consumer with contact information for that business.”³³ ANA asks the CA AG to clarify that a service provider does not need to provide a business’s contact information to a consumer if doing so could compromise the service provider’s competitive position in the

³⁰ Cal. Civ. Code § 1798.105(b).

³¹ Cal. Code Regs. tit. 11, § 999.317(b) (proposed Oct. 11, 2019).

³² *Id.* at §§ 999.312(a), (b); 999.315(a).

³³ *Id.* at § 999.314(d).

marketplace or abridge the confidentiality clauses the service provider agreed to in contracts with its business clients.

The proposed regulations' requirement that a service provider must provide a consumer with a business's contact information may be difficult if not impossible for service providers to execute. A service provider may, for example, maintain information about a consumer that came to the service provider from more than just one business. In situations such as these, the service provider may not be in a position to know which business's contact information to provide to the consumer upon receiving a request to know or a request to delete. Moreover, the obligation to provide business contact information to a consumer who submits a request to know to a service provider could have negative effects for business competition by enabling the service provider's competitors to submit requests to know to the service provider to gain confidential or proprietary information about the service provider's client list. Although the draft regulations state that a service provider only must provide contact information "when feasible," it is unclear whether service providers are obligated to provide such information when it might be technically feasible to do so but would violate confidentiality clauses in their contracts with their clients or otherwise expose them to risks to their competitive position in the marketplace. The CA AG should clarify that it is not feasible for a service provider to provide a business's contact information to a consumer if providing such information could violate the service provider's confidentiality agreements with its clients or expose the service provider's client list to a competitor.

b. Allow Service Providers to Use Personal Information to Improve Services

According to the draft rules, a service provider "shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose of providing services to another person or entity."³⁴ This provision could be read to prohibit service providers from using personal information to make general improvements to their services that would benefit consumers, the business that provided the personal information to the service provider in the first place, and other businesses. Although the proposed regulations note that a service provider can combine personal information received from one or more entities to which it is a service provider on behalf of such businesses to the extent necessary to detect data security incidents or protect against fraudulent or illegal activity, this allowance does not enable service providers to combine and use the personal information they receive from businesses to improve their products and services. The use of personal information to upgrade and enrich products and services is important to enable service providers to improve their offerings and provide better services to businesses, which ultimately benefits consumers. The CA AG should therefore revise the draft rules to clarify that service providers may use personal information to make general improvements to services.

V. Consumer Verification

a. Clarify How Businesses Must Respond to CCPA Requests When They Maintain Personal Information In A Manner that Is Not Associated With An Identifiable Person

³⁴ *Id.* at § 999.314(c).

The proposed regulations state that if a business maintains personal information in a manner that is not associated with an actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the non-name identifying information.³⁵ In addition, the proposed rules state that “[i]f a business maintains consumer information that is de-identified,” it is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request.³⁶ The proposed regulations do not clearly explain how businesses may reasonably engage in verification when they do not maintain personal information in a manner that is associated with a named actual person. ANA asks the CA AG to clarify that businesses that do not maintain data sufficient to verify a consumer’s identity are not required to collect additional data from the consumer to do so.

While the proposed regulations state that fact-based verification inquiries may be required when businesses maintain personal information in a manner that is not associated with a named actual person,³⁷ this provision of the proposed regulations forces businesses to act as detectives to verify a consumer who may come to the business by matching them to a non-identifying piece of information. Identifiers businesses may maintain such as cookie IDs and IP addresses, for example, are not sufficient to identify a consumer on an individual level, and identifying information provided by the consumer would do nothing to enable the business to verify the consumer’s identity. As a result, the proposed regulations’ discussion of a consumer providing a certain number of “data points” or “pieces of personal information” in order to allow a business to verify the consumer to the degree of certainty needed to effectuate a request may not be sufficient if the business maintains non-identifiable information such as identifiers.³⁸ Moreover, identifiers may cover entire households, libraries, shared devices, or other places, and they may therefore be linked to personal information from many individuals.

Consequently, it may be difficult if not impossible for a consumer to demonstrate they are the sole consumer associated with non-name identifying information held by a business. It is also unclear how businesses can conduct fact-based verification inquiries when the information they may need to verify an identity is not information the consumer may have readily available to them (*e.g.*, a cookie ID, mobile ad identifier, IP address, or other online identifier). The CA AG should clarify that if a business does not maintain data sufficient to verify a consumer’s identity, the business is not required to collect additional data to verify the consumer. In addition, this type of attempt at identification is likely to undermine consumer privacy rather than enhance it.

b. Clarify that Verification Inquiries to Consumers from Businesses Toll the 45-Day Time Period to Respond to Requests

The proposed regulations require businesses to establish, document, and comply with a reasonable method for verifying consumer requests.³⁹ The proposed rules also require

³⁵ *Id.* at § 999.325(e)(2).

³⁶ *Id.* at § 999.323(e).

³⁷ *Id.*

³⁸ *See id.* at §§ 999.325(b), (c).

³⁹ *Id.* at § 999.323(a).

businesses to respond to requests to know and requests to delete within 45 days.⁴⁰ Consistent with the proposed regulations' verification provisions, a business may require a consumer to submit information to verify his or her identity before responding to a request.⁴¹ The draft rules note that the 45-day time period to respond to requests to know and requests to delete "will begin on the day that the business receives the request, regardless of time required to verify the request."⁴²

The CA AG should clarify that when businesses ask for verifying information from a consumer, such an action tolls or pauses the 45-day time period the business has to respond to the consumer request and resumes only when the consumer responds with the requested verifying information. A similar clarification would be helpful related to the two-step process that is required to process online consumer requests to delete personal information.⁴³ The CA AG should clarify that a business's request for a second, confirming action validating that the consumer wants the personal information the business collected from the consumer deleted, which must be provided pursuant to the proposed regulations, tolls the 45-day time period for responding to a request until the consumer provides the confirmation. Businesses should not be penalized for the public's dilatory responses to requests for verification that are outside the control of a company.

Businesses cannot accurately facilitate CCPA requests without verifying the consumer who is the subject of the request. Without proper verification, businesses risk effectuating a consumer request against personal information that pertains to the wrong consumer, thereby failing to fulfill the wishes of the consumer who submitted the request and taking action that would affect personal information about a consumer that did not make the request. If businesses are required to respond to consumer requests to know and delete within 45 days of receiving them, regardless of the amount of time it takes to verify the consumer's requests, consumers would be at risk of businesses taking action on and making decisions about personal information that does not align with their choices. Accordingly, we encourage the CA AG to clarify that a business's request for verifying information or a request for a second, confirming action validating a request to delete tolls or pauses the 45-day period within which businesses must respond to consumer requests to know and delete.

c. Remove the Requirement that Unverified Requests to Delete Must Be Treated as Requests to Opt Out

The proposed rules state that if a business cannot verify the identity of a consumer submitting a request to delete, it must inform the requestor that their identity cannot be verified and instead treat the request as a request to opt out of personal information sale.⁴⁴ Per the proposed rules, requests to opt out of personal information sale need not be pursuant to verifiable consumer requests.⁴⁵ The requirement to transform unverifiable deletion requests into opt out requests threatens to harm consumers rather than protect their interests, and it represents an

⁴⁰ *Id.* at § 999.313(b).

⁴¹ *Id.* at §§ 999.323(b), (c).

⁴² *Id.*

⁴³ *Id.* at § 999.312(d).

⁴⁴ *Id.* at § 999.313(d)(1).

⁴⁵ *Id.* at § 999.315(h).

entirely new obligation that is not required by the CCPA itself and is outside of the scope of the law. The CA AG's proposed rule requiring businesses to pass along opt out requests to third parties to whom they have sold personal information in the prior 90 days would mean that a consumer's unverified deletion request could have a ripple effect throughout the ecosystem by removing personal information associated with that consumer from the entire online environment. This result may not align with the consumer's desires, particularly if the consumer thought he or she was submitting a deletion request to be effective solely on an individual business. Such an application may not reflect the consumer's preferences and denies them the ability to allow some businesses to sell personal information while restricting others from doing so. The CA AG should therefore clarify that consumers must affirmatively request that a business opt the consumer out from personal information sale before the business may treat a deletion request as an opt out request.

The right to delete information and the right to opt out from sale of personal information are two separate rights that achieve two separate results. Deletion removes the consumer's personal information from the systems of the business that is the subject of the request, while opt out requests have the potential to remove the consumer's information from being transferred by many businesses, thereby inhibiting consumers' ability to receive products, services, and loyalty programs they enjoy and have come to expect. Consumers should not be forced to opt out of personal information sale if a business cannot verify their request to delete. The requirement to transform unverifiable deletion requests into opt out requests may conflict with consumers preferences and places a substantive obligation on businesses that has no textual basis in the CCPA. In addition, it could lead to competitors undermining the system by requesting deletions, that while unverifiable, would force their competitors into unwarranted opt-outs. As such, we ask the CA AG to clarify that if a business cannot verify a consumer's deletion request, the consumer must specifically request that the business opt out the consumer from personal information sale before the business may take such an action.

VI. Privacy Policies

a. Clarify the Required Granularity of Privacy Policies

The proposed regulations state that “[f]or each category of personal information collected...” a business must provide the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties with whom the business shares personal information.⁴⁶ As such, the proposed regulations suggest businesses must state the sources, purposes, and categories of third parties with whom personal information is shared *for each category of personal information*. The CA AG should clarify that businesses do not need to make disclosures for each individual category of personal information collected and may instead provide disclosures with respect to all categories of personal information collected.

If businesses must make disclosures with respect to each category of personal information collected, privacy policies would be significantly longer and more complex, and less understandable for consumers, than they would be if the required disclosures could be made with

⁴⁶ *Id.* at § 999.308(b)(1)(d)(2).

respect to personal information generally. This would detract from the purpose of a robust consumer privacy notice, as it would induce notice fatigue and could discourage consumers from taking the time to read and understand the full privacy notice and its contents. Additionally, requiring granular disclosures for each category of personal information collected could impede businesses from satisfying the requirement that a privacy policy must “be written in a manner that provides consumers [with] a meaningful understanding of the categories listed.”⁴⁷ The CA AG should clarify that businesses may make required disclosures for personal information generally and do not need to make granular disclosures relevant to each category of personal information collected. Businesses should be able to provide consumers with privacy policies that logically disclose required information in a digestible and understandable format, as this approach would further the ultimate goal of robust consumer notice in a more effective way than requiring disclosures pertaining to each category of personal information collected.

b. Enable Flexibility for the Placement of Privacy Policies in Mobile Applications

ANA encourages the CA AG to update the draft rules to provide more flexibility for the placement of privacy policies in mobile applications. The draft rules currently require a business to place a privacy policy “on the download or landing page of a mobile application.”⁴⁸ A business should have the ability to meet the requirement to provide a privacy policy by doing so (1) in a digital distribution platform for computer software applications, such as an application store, *or* on the download or landing page of an application, *and* (2) by making the policy available from an within the application itself, for example, through the application’s settings menu.

Revising the proposed regulations to provide more flexibility for presenting privacy policies in the mobile space would align with industry codes of conduct and past publications from the CA AG’s office on privacy practices in the mobile environment.⁴⁹ For example, the CA AG’s 2013 report titled “Privacy On The Go: Recommendations for the Mobile Ecosystem” states that a business should “[m]ake the privacy policy conspicuously accessible to users and potential users... [and] [l]ink to the policy within the app (for example, on [the] controls/settings page).”⁵⁰ The report therefore contemplated flexible approaches to providing consumers with necessary disclosures and took the unique nature of mobile applications into account in formulating its recommendations. As a result, ANA asks the CA AG to update the proposed regulations so that a business may satisfy the requirement to provide a clear and conspicuous link to a privacy policy by making the privacy policy viewable from within an application store or the download or landing page of an application, and within the mobile application itself.

⁴⁷ *Id.*

⁴⁸ *Id.* at § 999.308(a)(3).

⁴⁹ See, e.g., DAA, Application of Self-Regulatory Principles to the Mobile Environment at 15, 17 (Jul. 2013), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/DAA_Mobile_Guidance.pdf; Kamala D. Harris, Attorney General, California Department of Justice, *Privacy on the Go: Recommendations for the Mobile Ecosystem* at 10 (Jan. 2013) (hereinafter, “Privacy on the Go”), located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf.

⁵⁰ Privacy on the Go at 10.

c. Clarify that Businesses Do Not Have to Make Statements About Minors In Privacy Policies Unless They Have Actual Knowledge They Collect Personal Information From Minors Under the Age of 16

Per the proposed rules, as part of a business's privacy policy, the business must "[s]tate whether or not the business sells the personal information of minors under 16 years of age without affirmative authorization."⁵¹ This obligation could require a business to make a positive statement about a practice in which it does not engage would be both inaccurate and misleading, and potentially harmful to the business. The CA AG should clarify that a business does not have to make such a statement in its privacy policy unless it has actual knowledge that it collects personal information from minors under the age of 16.

Laws in the United States specifying the contents of privacy policies have historically required businesses to make statements about practices in which they do engage.⁵² Businesses typically do not list actions they do not take in their privacy policies. Through the proposed regulations, the CA AG has imposed a new requirement on businesses that was not included in the text of the CCPA itself. A business would now be required to make an affirmative statement about a practice in which it may not engage. This requirement contrasts with longstanding practices and laws regulating privacy notices in the United States. Furthermore, this provision provides consumers with minimal if any benefit.

The requirement to make an affirmative statement in a privacy policy about whether a business sells personal information of minors without affirmative authorization may also force businesses to investigate the ages of their users. This potential indirect obligation of the CCPA may contravene the clear implementation guidance to the contrary that the Federal Trade Commission has provided to businesses surrounding COPPA compliance, as COPPA has been interpreted to not require businesses to investigate the ages of their users.⁵³ To better align with COPPA, only businesses that have actual knowledge that they collect personal information from minors under the age of 16 should have to make a statement regarding affirmative authorization for the sale of that personal information in their privacy policies. The CA AG should clarify that a business does not have to make a statement about its practices of obtaining affirmative authorization to sell personal information in its privacy policy unless it has actual knowledge it collects personal information from minors under the age of 16.

d. Clarify the Privacy Policy Disclosures a Business Must Provide to be Exempt from the Obligation to Provide Notice of the Right to Opt Out

According to the proposed regulations, a business is exempt from the requirement to provide a notice of the right to opt out if "(1) [i]t does not, and will not, sell personal information collected during the time period during which the notice of right to opt-out is not posted; and (2) [i]t states in its privacy policy that it does not and *will not* sell personal information."⁵⁴ ANA

⁵¹ Cal. Code Regs. tit. 11, § 999.308(b)(1)(e)(3) (proposed Oct. 11, 2019).

⁵² See, e.g., Cal. Bus. & Prof. Code §§ 22575-22579; Del. Code Ann. tit. 6, § 1205C; Nev. Rev. Stat. §§ 603A.310-360.

⁵³ See FTC, Complying with COPPA: Frequently Asked Questions, located at <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>.

⁵⁴ Cal. Code Regs. tit. 11, § 999.306(d)(2) (proposed Oct. 11, 2019) (emphasis added).

asks the CA AG to eliminate the requirement for businesses that do not sell personal information to state that they *will not* sell personal information in the future. This revision would benefit consumers by helping to reduce potential confusion about business practices if such practices change in the future.

Requiring a business to state that it will not sell personal information does not take into account the fact that business practices can and often do change over the course of time as offerings evolve and new services are added. Stating that a business will not sell personal information in a privacy policy could give consumers the false impression that a business will never change its practices in the future. The Federal Trade Commission's longstanding position on material changes to privacy policies acknowledges that businesses can change their data practices so long as such changes are communicated to consumers, the information collected is treated according to the terms of the policy that was in place at the time of information collection, and if a business wishes to treat previously collected information according to the terms of the new policy, it must obtain affirmative express consent from consumers before doing so.⁵⁵ The FTC has therefore provided a framework that recognizes business practices may change in ways that are not originally anticipated and offers a method for businesses to implement those changes moving forward. Requiring businesses to state that they will not sell personal information in privacy policies runs the risk of suggesting to consumers that businesses will never change their data practices, even as their offerings and services evolve.

Moreover, as discussed in Section VI(c) above, businesses do not typically make statements in privacy policies about practices in which they do not or will not engage. Laws regulating the contents of privacy policies have typically required businesses to disclose practices in which they do engage to consumers and have not forced them to make statements about practices in which they will not engage. As such, the CA AG should consider eliminating the requirement for businesses that do not sell personal information to state that they will not sell personal information in their privacy policies in order to be exempt from the need to provide a notice of the right to opt out of personal information sale.

e. Clarify the Disclosures Required of Businesses that Buy, Receive, Sell, or Share Personal Information of 4 Million or More Consumers

Pursuant to the proposed rules, “[a] business that alone or in combination, annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers” must make privacy policy disclosures about the number of distinct CCPA requests received, complied with in whole or in part, and denied during the prior calendar year.⁵⁶ The phrase “shares for commercial purposes” could be interpreted to include sharing personal information about a consumer with service providers, which would drastically increase the number of businesses that would be subject to this additional reporting requirement. The CA AG likely did not intend to include sharing personal information with service providers within the scope of the calculation for determining whether a business is subject to the extra reporting requirements for businesses that buy, receive, sell, or

⁵⁵ Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* at 57-60, (Dec. 2010), located at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

⁵⁶ Cal. Code Regs. tit. 11, § 999.317(g) (proposed Oct. 11, 2019).

share personal information of 4 million or more consumers. As a result, we ask the CA AG to clarify that sharing personal information about a consumer with a service provider does not count towards determining whether a business is subject to these additional reporting requirements.

VII. Other Required Notices

a. Affirm that Required Notices May Be Provided in a Privacy Policy

The proposed regulations impose new consumer notices that are not required by the text of the CCPA, and they do not clearly state whether such notices may be provided in a privacy policy. In terms of disclosures, the proposed rules require businesses to provide: (1) a notice at collection; (2) a notice of the right to opt out of the sale of personal information; and (3) a notice of financial incentive in addition to a privacy policy.⁵⁷ The CA AG should clarify that the notice at collection, notice of the right to opt out of the sale of personal information, and notice of financial incentive provided in a privacy policy accessible to consumers where required satisfies the proposed regulations' mandate to provide notice at collection, notice of the right to opt out of the sale of personal information, and notice of a financial incentive.

The proposed regulations do not clearly state whether these additional notices required by the proposed regulations may be provided in a privacy policy. A “notice of right to opt out” is defined as “the notice given by a business informing consumers of their right to opt-out of the sale of their personal information.”⁵⁸ The “notice of right to opt-out” must be provided on the Internet webpage to which the consumer is directed after clicking the “Do Not Sell My Personal Information” link, and must either include certain specific information or link to the section of the business’s privacy policy that contains such information.⁵⁹ Similarly, if a business offers a financial incentive or price of service difference online, the business may provide a “notice of financial incentive” by linking to the section of the business’s privacy policy that contains the required information.⁶⁰ A “notice of financial incentive” is “the notice given by a business explaining each financial incentive or price or service difference.” As a result, the notice of right to opt-out and notice of financial incentive contemplate use of the privacy policy to contain necessary disclosures, but they do not explicitly state whether the notice requirements may be satisfied by providing the required information through a privacy policy alone.

In addition, the “notice at collection,” which is defined as “the notice given by a business to a consumer at or before the time a business collects personal information from the consumer,” may be provided through a conspicuous link to the notice on the business’s website homepage, a mobile application download page, or on all webpages where personal information is collected.⁶¹ The explicitly listed methods for providing the notice at collection are typical methods by which businesses provide privacy policies. As a result, the proposed regulations suggest, but do not explicitly state, that a notice at collection may be provided in a privacy policy.

⁵⁷ *Id.* at §§ 999.305, 306, 307.

⁵⁸ *Id.* at § 999.301(j).

⁵⁹ *Id.* at § 999.306(b).

⁶⁰ *Id.* at § 999.307(a)(3).

⁶¹ *Id.* at § 999.305(a)(2)(e).

The CA AG should clarify that the notice at collection, notice of right to opt-out, and notice of financial incentive may be provided to consumers in a privacy policy, and if such notices are provided in a privacy policy that is made available to consumers where required, they do not need to be provided through any other means. Such a rule would enable business compliance with the CCPA and offer consumers a centralized place through which they may receive required business disclosures. Providing such notices within the privacy policy is consistent with consumer expectations. Consumers have come to expect such disclosures and information to be accessible from a privacy policy. Consumers would benefit from receiving all the necessary information through a single notice, and businesses would benefit from being able to focus privacy-related information in one unified disclosure.

b. Confirm that Notice at Collection Should Not Be Required in the Context of Particular Commonplace Consumer-Business Interactions

The CCPA states that a business that collects “a consumer’s personal information” shall, at or before the point of collection, inform consumers of the categories of personal information to be collected and the purposes for which the categories of personal information shall be used.⁶² The CA AG should clarify that notice at collection is not necessary in the context of certain commonplace and frequent interactions with a business through which consumers expect the business to collect personal information.

Consumers engage in certain interactions with businesses that should not necessitate a notice at collection, because in those interactions consumers often expect businesses to collect personal information. For example, taking a consumer’s payment card information at a cash register in a retail store should not trigger the need to provide a notice at collection. If businesses must provide a notice at collection before taking payment card information at a retail store, consumer shopping experiences could be hindered, and business transactions would take substantially longer to effectuate. Payment card information is often exchanged during retail transactions, and consumers expect businesses to collect this information in order to complete the transaction the consumer wants to effectuate. Another example of a consumer-business interaction that should not require a notice at collection is when a consumer contacts a business’s customer service office. If a consumer contacts a business’s customer service representative over the phone, the customer service representative should not be required to verbally read the consumer information that would satisfy the CCPA’s notice at collection requirement, because it is reasonable for a consumer to expect the business to collect certain personal information in the context of the customer service call.

Requiring businesses to provide a distinct notice associated with everyday and consumer-expected data collection that is necessary to facilitate purchases or respond to consumer inquiries would inhibit consumers’ ability to make purchases efficiently and interact with businesses without substantial interruptions. The CA AG should therefore clarify that businesses need not provide a notice at collection to consumers if the context of the consumer-business interaction is one under which the consumer should reasonably expect that the business is collecting personal information.

⁶² Cal. Civ. Code § 1798.100(b); Cal. Code Regs. tit. 11, § 999.305(a)(1) (proposed Oct. 11, 2019).

c. Grant Online Businesses that Do Not Maintain Personally Identifying Information Flexibility to Provide Effective Opt Out Mechanisms

According to the proposed regulations, a business must provide a webform to enable consumers to opt out of the sale of personal information.⁶³ If a business operates a website, the proposed regulations also state that it must provide a webform to consumers to submit requests to know.⁶⁴ The CA AG should clarify that online businesses that do not maintain information that can identify a consumer do not need to provide a webform, and may use another, equally effective method to enable consumers to submit a request to opt out, such as through email or other standard channels used for customer service.

The proposed regulations already recognize that methods for submitting consumer rights requests may need to be different depending on whether the data collection occurs offline or online. As such, similar flexibility should be provided for opt outs involving what has been traditionally referred to as non-personally identifying information. Webform requirements may work efficiently for opt outs or requests to know pertaining to personally identifiable information, such as a consumer's name, email address, or postal address. However, the webform requirements do not adequately address how a webform can facilitate a consumer opt out or request to know for businesses that do not maintain personally identifiable information (such as when such businesses maintain cookie IDs, mobile ad identifiers, IP addresses, and/or other online identifiers). The CA AG should clarify that online businesses that do not maintain personally identifying information do not need to provide a webform and may use another method, such as email or other common channels used for customer service, to enable a consumer to submit a request to opt out.

d. Clarify Discrepancies Between the Content of Required Notices and the Content of Privacy Policies

According to the proposed regulations, businesses must provide a notice at collection, which must specify “[a] list of the categories of personal information about consumers to be collected.”⁶⁵ However, the proposed regulations also state that in a privacy policy, a business must provide “the categories of consumers’ personal information the business has collected about consumers in the preceding 12 months.”⁶⁶ As such, the “notice at collection” requirement is forward-looking, and the privacy policy provision is backward-looking. The CA AG should clarify whether businesses must provide disclosures related to personal information they have collected in the past twelve months or whether they must provide forward-looking disclosures about what they intend to do in the future with collected personal information in required notices.

Requiring businesses to provide disclosures about information they will collect from consumers in addition to information they have already collected about consumers runs the risk of producing excessively long privacy notices that would not provide meaningful disclosures to consumers. The mandate hinders’ businesses ability to provide consumers with a reasonably readable and palatable privacy notice that is presented in a format they can understand.

⁶³ Cal. Code Regs. tit. 11, §§ 999.306(c)(2), 315(a) (proposed Oct. 11, 2019).

⁶⁴ *Id.* at § 999.312(a).

⁶⁵ *Id.* at § 999.305(b)(1).

⁶⁶ *Id.* at § 999.308(b)(1)(d)(1).

Furthermore, this discrepancy between the need to provide information about future practices and information about past practices fails to adequately clarify what information must be provided in required notices. If a business may make all CCPA-required disclosures in one privacy policy, it is not clear whether it must provide a section for categories of personal information to be collected in the future and a section for categories of personal information it collected in the past 12 months. We request that the CA AG clarify this provision by regulation.

VIII. Provisions of the Proposed Regulations that ANA Supports

a. Providing Flexibility For Businesses' Presentation of Opt Out Links to Consumers

The proposed regulations indicate that the CA AG may consider another opt out button or logo during its CCPA rulemaking process.⁶⁷ We support the CA AG's efforts to provide an additional acceptable way to present the opt out button or logo. In lieu of setting forth a specific, prescribed button or logo via regulation, we suggest that the CA AG allow businesses flexibility to decide on an appropriate button or logo, subject to certain guidelines.

The CA AG should require the opt out button or logo to clearly indicate to the consumer that clicking the button enables the consumer to opt out of the sale of personal information. Instead of adopting a third acceptable formulation for the opt out button or logo (in addition to "Do Not Sell My Personal Information" or "Do Not Sell My Info"), the CA AG should set forth reasonable criteria the button or logo must meet, such as clear, meaningful, prominent notice to the consumer of the ability to opt out, and allow businesses flexibility in choosing an acceptable way to implement the opt out button or logo. We ask the CA AG to enable a flexible acceptable method of providing consumers with the ability to opt out of the sale of personal information.

b. Prohibiting Certain Sensitive Specific Pieces of Information from Being Returned to a Consumer in Response to a Request to Know

Per the proposed rules, a business may not at any time disclose a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers.⁶⁸ ANA supports this provision, as many of the data elements that are forbidden from disclosure are elements that, when combined with a first initial or first name and last name, would constitute a data breach under California law if acquired by an unauthorized individual.⁶⁹

The proposed regulations helpfully foreclose the possibility that, in order to comply with the CCPA, a business would be forced to disclose certain particularly sensitive data elements to the wrong recipient, which would constitute a breach. Furthermore, this provision makes practical sense from a data security standpoint, as there are compelling public policy reasons to restrict this particularly sensitive information from disclosure. For example, disclosing such sensitive information could enable identity theft and other non-privacy enhancing consumer

⁶⁷ *Id.* at § 999.306(e)(1).

⁶⁸ *Id.* at § 999.313(c)(4).

⁶⁹ Cal. Civ. Code §§ 1798.82(g), (h).

effects, such as indirectly exposing private details about a consumer’s life. ANA supports the CA AG’s efforts to restrict certain data elements from disclosure all together, as this restriction is privacy protective for consumers and serves to help businesses comply with California law.

c. Adopting a Risk-Based Approach to Verifying Requests to Know and Delete

The proposed rules require a business to establish, document, and comply with a reasonable method for verifying that the person making a request to know or a request to delete is the consumer about whom the business has collected information.⁷⁰ The proposed rules also note that businesses may consider a number of factors to determine a reasonable verification method, such as: the type, sensitivity, and value of the personal information collected and maintained; the risk of harm to the consumer posed by unauthorized access or deletion; the likelihood that fraudulent or malicious actors would seek the personal information; whether the personal information to be provided to verify an identity is sufficiently robust to protect against fraudulent requests; the manner in which the business interacts with consumers; and available verification technologies.⁷¹ ANA supports this flexible, risk-based approach to verification presented in the proposed regulations. This non-prescriptive framework allows businesses to reasonably tailor their verification processes to the sensitivity of the data at issue and their own practices.

* * *

We thank the CA AG for the opportunity to submit comments on the proposed regulations interpreting the CCPA. We look forward to continuing our productive dialogue with the CA AG on this matter and the important issue of consumer privacy. Please do not hesitate to contact us with any questions you may have regarding these comments.

⁷⁰ Cal. Code Regs. tit. 11, § 999.323(a) (proposed Oct. 11, 2019).

⁷¹ *Id.* at § 999.323(b)(3).

Message

From: Kammerer, Susan [REDACTED]
Sent: 12/7/2019 12:05:31 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: APCA Comments - CA CCPA Regulations
Attachments: 19-12-06 CA CCPA Regulations - APCA Comments - Final.pdf

Please see attached.

Thank you,

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

Please Note - My Email address has changed effective January 21, 2019 to: [REDACTED]





December 6, 2019

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

VIA Electronic Mail: PrivacyRegulations@doj.ca.gov

To Whom It May Concern:

The American Property Casualty Insurance Association (APCIA) appreciates the opportunity to provide feedback on the proposed California Consumer Privacy Act Regulations (proposed regulations). APCIA is the preeminent national insurance industry trade association, representing property and casualty insurers doing business locally, nationally, and globally. Representing nearly 60 percent of the U.S. property casualty insurance market, APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers. APCIA represents the broadest cross-section of home, auto, and business insurers of all sizes, structures, and regions of any national trade association.

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

General Observations

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

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

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

Connecting the Business use with Personal Information

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

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

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

Requirement to obtain Affirmative Consent for New Uses of Information

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

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

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

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

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

CCPA Disclosure in the Privacy Policy

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

Right to Opt-Out

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

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

Privacy Notice

Privacy Policy Examples

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

Availability in Multiple Languages

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

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

Webpage Link for CA Specific Consumer Privacy Rights

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

Disclosure of the Verification Process

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

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

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

Notice of Improper Use of Minor's Data

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

Too Many Required Disclosures in the Privacy Policy

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

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

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

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

Responding to Requests to Know and Delete

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

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

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

Requests to Know

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

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

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

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

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

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

Moreover, there is a blanket requirement that if a business could not verify the identity of the requestor it must deny the request to delete and, instead, treat the request as one to opt-out. Our position is that the interest of consumers is poorly served by this provision. For instance, if an ex-spouse tries to request deletion of a current consumer's data, but his/her request cannot be verified, then in practice you are giving the ex-spouse the authority to automatically opt the current consumer out of anything. This appears contrary to the rights that the CCPA advocates for, such as individual control.

Requests to Delete

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

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

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

Service Provider

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

Authorized Agent

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

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

Methods for Submitting Requests

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

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

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

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

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

Requests to Opt-Out

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

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

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

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

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

Definitions

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

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

CCPA Scope

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

APCIA appreciates the opportunity to provide feedback. Please, let us know if you have any questions or would like additional information.

Respectfully submitted,

Message

From: [REDACTED]
on behalf of Katie Kennedy [REDACTED]
Sent: 12/6/2019 11:45:40 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Apple Inc Comments to the California Department of Justice re CCPA
Attachments: Apple Inc Comments to California Department of Justice re CCPA Regulations.pdf

To Whom It May Concern:

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

Please do not hesitate to reach out with any questions.

Thank you,

Katie

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



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

At Apple, we believe privacy is a fundamental human right. We purposely design our products and services to minimize our collection of user data. When we do collect personal information, we are transparent about it and take steps to provide users with choice and control. And we work to disassociate it from the user where possible. The customer is not our product, and our business model does not depend on collecting vast amounts of personal information to enrich targeted profiles on individual consumers marketed to advertisers.

We are proud of our deep commitment to protecting consumer privacy. However, we also recognize that privacy needs to be protected by safeguards that go beyond the commitments of individual companies. Laws and regulations are needed to ensure that individuals can understand how their personal information is used and trust that their privacy will be respected, regardless of the values or business model of the particular company that is processing their data.

As a technology company continuously pushing the bounds of innovation, we understand the immensely important role that user data plays in providing valuable services for consumers. But respect for user privacy and the provision of innovative, data-driven services are not mutually exclusive; you can have great user experiences *and* great privacy. To achieve this, we need a thoughtful privacy law that takes a comprehensive view of the interests at stake and appropriately balances important consumer privacy considerations with the benefits that individuals can derive from transparent and respectful use of their data. To be effective, this law must not only deter harmful uses of personal information, but also encourage businesses to rethink their collection and use of personal information by incentivizing the creation and deployment of privacy-preserving architectures and technologies – including, for example, on-device processing.

We applaud the California Attorney General's office for the work it has done in collecting pre-rulemaking comments and drafting regulations for the California Consumer Privacy Act. We respectfully offer the following comments on certain key issues in the proposed regulations where the Attorney General has the power to make revisions that could clarify ambiguities, encourage privacy-protective and consumer-friendly practices, and mitigate the risk of unintended negative consequences.

As discussed in more detail below, we encourage the Attorney General to clarify the meaning of the "household" definition and limit disclosures of "household" data that may undermine consumer privacy. We also encourage the Attorney General to promote the use of consumer-friendly online CCPA rights request portals by removing unnecessary barriers to the provision of such portals, recognize the importance of encouraging innovation in proper authentication and verification practices, and clarify the role of service providers in the rights request process.

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

Apple
One Apple Park Way
Cupertino, CA 95014



I. The current definition of “household” legislates affiliations among persons and risks violating constitutionally protected privacy rights. The Attorney General should clarify the definition of “household” to help prevent such violations.

Given the CCPA’s unprecedented privacy protections for “household” data, it is important that the definition of “household” be precisely crafted in order to ensure that consumer personal information remains protected from unintentional disclosures and bad actors. Data about public or commonly accessible devices can yield significant amounts of information about people, including, in some cases, potentially sensitive data. Unfortunately, the proposed regulations’ sweeping approach to “households” creates a significant risk that consumers may suffer privacy intrusions both from unrelated and unknown persons *and* from members of their (actual) household.

The proposal to define a “household” around “a person or group of people occupying a single dwelling,” Regulations § 999.301(h), will likely result in unrelated or unaffiliated people being grouped into a single “household.” This broadly scoped definition lacks context or distinction between different types of dwellings, meaning that entire college dorms, retirement homes, apartment buildings, condominiums, or any other multi-family building could potentially be treated as a single “household” under the CCPA. Such an outcome would lead to unintended disclosures of data and, as a result, perversely cause the CCPA to undermine consumers’ privacy. Additionally, the definition’s use of the word “occupying”¹ and the failure to require that the occupants maintain any permanent or extended connection to the dwelling could allow temporary guests to be treated as members of the household. For example, a guest of a family who visits on occasion (*e.g.*, a cousin, family friend) may use the family’s Wi-Fi a few times every year. Under the broad definition of “household,” this pattern of activity could potentially allow a business to conclude that the guest also “occupies” the family’s dwelling and is therefore part of the household and entitled to access the “household” data. This same problem will be present in the short-term rental context, where a number of unrelated persons who occupy the same dwelling at different points over the course of a year may all be considered to be part of the same “household.”

¹ The word “occupy” can be interpreted to cover a guest’s temporary stay in a location. *See, e.g.*, Oxford English Dictionary Online, <https://www.oed.com/view/Entry/130189?redirectedFrom=occupy#eid> (giving as a definition of the verb “occupy” “to be situated, stationed, or seated at or in, to be at or in (a place, position, etc.)”). Certain California laws also treat the word “occupant” as being interchangeable with “guest.” *See, e.g.*, Cal. Health & Safety Code § 18862.30 (“‘Occupant’ and ‘resident’ shall be interchangeable and shall include ‘occupant,’ ‘resident,’ ‘tenant,’ or ‘guest’”). Additionally, while the word “occupant” is sometimes used in California law to refer to persons who live in a dwelling, the definitions of the word in these contexts often do not require a particularly close connection between the persons living in the dwelling. *See, e.g.*, Cal. Code Regs. tit. 17, § 56901 (defining “occupant” as “any individual living in the facility, including consumers and non-consumers, the owner/operator and his/her family members, and live-in staff.”); Cal. Civ. Code § 1946.8 (defining “occupant” as “any person residing in a dwelling unit with the tenant. . . includ[ing] lodgers”).



In addition to its broad scope, the proposed “household” definition also fails to require a close or intentional connection between the members of a “household.” This absence of limiting conditions may lead to violations of the CCPA and consumers’ constitutionally protected right to privacy. For example, unrelated consumers who are grouped in the same broadly defined “household” (e.g., roommates, people who reside in separate units within a multi-unit apartment building) may gain information about other members of their “household.” Such privacy violations may lead to a range of negative consequences, such as, embarrassment, fraud, identity theft, and even physical harm. For example, a household member who is simply interested in learning about the household data that pertains to their own activities may unintentionally obtain data related to other members of the household. The consequences may be more severe if a bad actor seeks to use household data for malicious purposes (e.g., obtaining information about the activities of other members of a “household” for the purpose of stalking another resident of a multi-unit apartment building).

The risks of the harms described above will disproportionately affect economically disadvantaged Californians. While some Californians may reside in “households” with persons whom they have chosen to affiliate, others have less control over their living situations and will not be able to easily relocate to a different “household” to avoid the risks of privacy violations.

Even in the case of closely related consumers who reside in the same household (e.g., spouses, adult children residing with their parents), the broad “household” concept may allow such consumers to violate each other’s privacy in undesirable and unexpected ways. For example, spouses may have separate devices (e.g., computers, mobile phones) and have a reasonable expectation that their spouse will not have access to data related to their non-shared devices. However, a request for the household’s data could yield information about the activities of their shared devices and even non-shared devices if the business views such devices as being tied to the household and not any particular consumer. Such an outcome could effectively force some consumers to partially forgo their privacy and data autonomy merely because they choose to live with other people. In some cases, these privacy violations could even create significant risks of physical harm. For example, an abusive spouse in a two-person household may submit access requests to nearby domestic abuse support centers and family law practices in order to determine whether someone from their household viewed their websites or contacted them (e.g., requesting data that may have been collected about a household device navigating a law firm’s website), and, in some cases, even obtain copies of the communications made from their household.

The CCPA and the draft regulations do not currently include adequate safeguards to protect against the risks noted above. For example, the draft regulations allow businesses to respond to non-account-based requests for household data with aggregate household data. However, access to aggregate household PI still creates significant risks to consumers. For example, aggregate data about a household’s interaction with various websites and services would allow any member of that household to gain insight on the interests and activities of other members of that household. If combined with other information the household member may have (e.g., knowledge about one’s neighbors or roommates), some of this aggregate information could possibly be tied back to particular members of the “household,” thereby effectively revealing



those persons' personal information. In some cases, this information could be used in harmful ways, such as the stalking and domestic abuse scenarios outlined above.

Although the CCPA includes a broad exception that allows for the denial of requests that would "adversely affect the rights and freedoms of other consumers," CCPA § 198.145(l), this provision is not sufficient to protect consumers against the risk of harm created by the proposed regulations' broad definition of household. For example, it puts the burden on individual businesses to determine whether their provision of household personal information in response to a verified request will create risk to consumers, and different businesses may reasonably come to different conclusions. In many cases, businesses will simply not have enough information about the context of the request to know whether such risks exist.

To help mitigate significant risks created by the inclusion of the "household" concept in the CCPA, the definition of "household" should be narrowed to ensure that the benefit of granting consumers access to household information is adequately balanced against the risks that such access may create. At a minimum, "households" should be limited to consumers who: (1) reside at the same address; (2) share a common device or service provided by the business; and (3) are identified by the business by reference to a permanent unique identifier, shared account, or group or family account, if such account type is made available by the business. The combination of these three elements is a more accurate threshold for whether persons actually share a "household" relationship and desire to be viewed as a single, related entity by a business than the existing test of "occupying a single dwelling." Requiring household members to "reside" at the same address would reflect the intent to exclude guests. Requiring that household members share a common device or service may increase the likelihood that the relevant consumers actually view themselves as part of a common household. When two users share a device or account, they are also more likely to understand that other users of the device or account may have access to the information stored on that device or account. Finally, requiring businesses to look to a shared identifier, such as a permanent unique identifier or shared account, may increase the likelihood that the relevant consumers actually view themselves as sharing a household relationship. For example, under this definition, two people who reside at the same multi-unit apartment building and maintain separate accounts with an Internet service provider would not be treated as a single "household." This would be an improvement from the existing definition, which could be interpreted to treat these people as a single household simply because they both occupy the same "dwelling."

II. The regulations should prohibit businesses from disclosing aggregate household data in response to requests made outside of password-protected accounts.

As discussed above, the current definition of "household" is overly broad and creates a significant risk of privacy violations and other harms for consumers. In addition to the changes suggested above, the Attorney General should seek to mitigate these risks further by removing the provision that allows businesses to provide aggregate household data in response to requests made outside of password-protected accounts.



The disclosure of aggregate household data can still provide a great deal of insight about the members of a “household.” This is particularly the case in smaller households. For example, a request from one resident of a two-person household would effectively disclose the personal information of the other household member, as the requestor could deduce how the aggregate data differed from their own data. Despite this risk of harm, the proposed regulations currently allow aggregate data to be provided in response to a request that is not made via a password-protected account. While such requests must still be verified pursuant to section 999.325 of the regulations, such a process would allow one member of the household to submit a verifiable request to obtain aggregate data that pertains to all members of the household. Given the potentially sensitive nature of some aggregate household personal information and the risk of harm posed by its unauthorized disclosure to other members of the “household,” this provision should be removed.

III. The Attorney General should remove certain proposed restrictions on the use of online portals to promote secure and efficient responses to consumer rights requests.

Apple supports the Attorney General’s decision to make self-service portals an acceptable method for allowing consumers to access, view, and receive a copy of their personal information. However, there is a risk that the proposed requirement that such portals “fully disclose[] the personal information that the consumer is entitled to under the CCPA,” Regulations § 999.313(c)(7), may deter businesses from using such portals and thereby deny consumers a convenient and secure means of exercising their rights.

While much of the personal information that consumers are entitled to under the CCPA will likely be producible in file formats and sizes that are deliverable through an online portal, there may be situations where this is not the case. For example, it may be more efficient to provide personal information from certain databases directly to the consumer via email instead of first sending that data to the online portal. It may also not always be feasible to deliver files of certain sizes or formats via the online portal. Provided that a business is transparent about how the consumer will receive their personal information in response to an access request, there is no harm to the consumer from a business’s use of more than one medium of delivery. However, the risk of being found noncompliant with the unnecessarily strict proposed language may deter some businesses from offering otherwise consumer-friendly and secure portals if they cannot guarantee that their portal will be a feasible means of delivery for all information in all instances.

To encourage the use of portals, the Attorney General should remove the requirement that they fully disclose all information required by the CCPA. If such a change were adopted, the regulations would still encourage the use of secure self-service portals, while recognizing that, in some instances, the most efficient and secure way of delivering consumer information will be a combination of portal and non-portal means. Such an approach would be consistent with the EU’s General Data Protection Regulation (GDPR), which encourages the use of portals to fulfill the access right (“[w]here possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal



data”), but does not expressly require that all personal data be provided via the portal. GDPR, Recital 63.

IV. The verification requirements must be flexible enough to allow businesses to adapt in response to future threats and protect consumers by always requiring that businesses verify identities to a “reasonably high degree of certainty.”

To protect consumer privacy, it is essential that the regulations require robust, yet flexible verification standards, so that bad actors cannot take advantage of published processes to steal and exploit consumers’ personal information. At Apple, our experience with protecting consumer data has taught us that bad actors are constantly developing new strategies, and companies need innovative and dynamic strategies to counter these efforts. Including specific verification procedures in the regulations may cause businesses to become reliant on the prescribed processes, even when the prescribed processes may not be sufficient to protect consumers’ personal information from attack. Such an outcome would be harmful to consumers, as the prescribed procedures will likely be ineffective in certain contexts today and are even more likely to become obsolete in the future.

Currently, the proposed regulations describe two specific processes for verifying a request to a reasonable degree of certainty (matching at least two pieces of information) and a reasonably high degree of certainty (matching three pieces of personal information and obtaining a signed declaration). Regulations § 999.323(b). There are many instances in which these processes may not provide for meaningful verification. For example, an increasing availability of compromised payment and identity data have led to increasing e-commerce fraud across the online ecosystem. Some bad actors can easily identify valid billing addresses and certain identity data to pair with compromised accounts to meet the proposed verification methods and violate consumers’ privacy rights. As another example, the FTC has warned about the threat of SIM swap scams, which may defeat security systems that rely on telephone numbers alone as a means of authentication. And many of the most common security questions used to secure online accounts can be answered with a search of public records. Each of these examples demonstrates that many bad actors could likely provide two or three pieces of data that match data held by a business, rendering the prescribed processes ineffective. Additionally, the required signed declaration for “reasonably high degree of certainty” verifications seems unlikely to serve as a meaningful obstacle to fraudulent requests. Bad actors routinely falsify documents, and many businesses may not have a requestor’s authentic signature on file or be able to accurately identify fraudulent signatures.

If the Attorney General adopts the prescriptive matching procedures, businesses and courts will almost certainly gravitate towards viewing them as the standard for determining whether a business has a reasonable verification process. Due to the flaws with these approaches, such an outcome may allow bad actors to frequently use the CCPA process to gain unauthorized access to consumer personal information. These risks will only increase in the future, as bad actors who study the published regulations will no doubt work to develop new techniques for bypassing the two/three data point and signed declaration requirements.



To combat the ever-evolving strategies of bad actors, businesses need to (and should be encouraged to) continually seek out and develop innovative and dynamic approaches to securing consumers' personal information. At Apple, we have implemented a wide range of tools and processes to protect our users and our systems from bad actors, including two-factor authentication. The security tools and processes that we use have changed over time to counter evolving threats, and they will continue to evolve in the future. Instead of cementing prescriptive verification procedures into law, the regulations should aim to encourage additional, evolving approaches to verification, along with robust minimum standards that prioritize consumer privacy.

To support strong minimum standards for identity verification, ongoing enhancements to consumer verification procedures, and deny bad actors inside knowledge of businesses' verification techniques, the Attorney General should revise the proposed regulations to require a reasonably high degree of certainty before disclosing consumer information and remove the specific descriptions of the data point matching verification techniques.

Further, as the right to privacy is fundamental and belongs to the individual, a business should not be required to respond to any request to exercise a privacy right unless it can verify the identity of the requestor. Anything less than that would obligate businesses to take risks with privacy rights and greatly increase the risk that a business grant one person's rights to another. And, attempts to have alternative criteria for different circumstances would leave companies open to an undermining of standards. Additionally, socially-engineered efforts to exploit the differences in verification standards could lead not only to exploited privacy rights but could also be the first step in a bad actor's quest to gain knowledge of certain personal information and leverage that knowledge to gain access to other, more sensitive, personal information. There are no tiers of fundamental rights, we do not believe there should be tiers of acceptable verification.

V. The Attorney General should clarify that service providers shall respond to consumer requests solely by directing the consumer to contact the relevant business(es) on whose behalf the service provider is working.

To promote the accurate and efficient fulfillment of consumer rights requests, the regulations should be revised to clarify that service providers shall respond to consumer requests solely by directing the consumer to contact the businesses on whose behalf the service providers collect personal information. The proposed regulations are not entirely clear regarding the role of service providers in responding to consumer requests. The draft regulations imply that service providers may act on consumer requests (*i.e.*, if a service provider receives a request, but does not fulfill the request, it shall "explain the basis for the denial"). Regulations § 999.314(d). However, the same section also provides that a service provider shall "inform the consumer that it should submit the request directly to the business on whose behalf the service provider processes the information and, when feasible, provide the consumer with contact information for that business." This sentence implies that the business, and not the service provider, is the entity that should receive and act on rights requests. Therefore, the proposed regulations seem



to allow a service provider to either evaluate and act on consumer requests or direct the consumer to the appropriate underlying business. Such a system is prone to causing confusion among consumers and businesses and may increase the likelihood of mistakes during the consumer rights request process.

As the entity that “determines the purposes and means of processing consumers’ personal information,” CCPA § 1798.140(c), the “business” should have sole responsibility for evaluating and acting on consumer rights requests. The business is best positioned to know what information it has about a given consumer and how such information is being used. Such information is critical for evaluating a consumer request and ensuring that the privacy interests of the CCPA and the other public interests and policy concerns are properly respected. A service provider that attempts to respond to a request with an incomplete picture of how the consumer’s information is used is also more likely to provide an incomplete and potentially incorrect response to the rights request (e.g., a service provider may not be aware that certain personal information is relevant to an ongoing investigation and therefore fail to apply the proper exceptions to a deletion request).

Clearly establishing the “business” as the single point of contact for CCPA requests will also help reduce consumer confusion. Under the current regulations, consumers may be confused about whether they have to submit CCPA requests to a business, its service providers, or all of these parties. Such an approach would also align the CCPA with the GDPR, which places the responsibility for responding to data subject requests with the “controller” (i.e., the entity that determines the purposes and means of processing personal data). GDPR, Art.12-22.

Revising the regulations to clarify the limited role of service providers in responding to consumer requests would be consistent with the CCPA’s transparency goals, more fully respect the variety of stakeholder and policy interests that may be impacted by CCPA requests, and promote the efficient fulfillment of consumer requests.

Message

From: Tobin, Timothy P. [REDACTED]
Sent: 12/6/2019 11:49:39 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: Auto Alliance Comments on the Proposed California Consumer Privacy Act Regulations
Attachments: Alliance CCPA NPRM Comments 20191204_SB_2.pdf

To Whom it May Concern:

Please find attached comments on the CCPA by the Alliance of Automobile Manufacturers (the "Auto Alliance").

Regards,

Timothy Tobin

Partner

Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004

Tel: [REDACTED]
Direct: [REDACTED]
Fax: [REDACTED]
Email: [REDACTED]
Blog: www.hldataprotection.com
www.hoganlovells.com

Please consider the environment before printing this e-mail.

About Hogan Lovells

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

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



December 6, 2019

California Office of the Attorney General
ATTN: Privacy Regulations Coordinator
300 S. Spring Street, First Floor
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

RE: Comments of the Alliance of Automobile Manufacturers on the California Attorney General’s Proposed California Consumer Privacy Act Regulations

To Whom It May Concern:

The Alliance of Automobile Manufacturers (“Alliance”) welcomes the opportunity to provide these comments (“Comments”) to the Attorney General’s Office regarding the Proposed California Consumer Privacy Act Regulations.

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. 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.

Automakers have long recognized the potential privacy considerations raised by collecting data in association with connected vehicle technologies and services. And automakers have taken proactive steps to protect consumer privacy. In 2014, the Alliance, the Association of Global Automakers (a trade association representing U.S. operations of certain international vehicle manufacturers and original equipment suppliers), and their respective members issued the Privacy Principles for Vehicle Technologies and Services (“Principles”).¹ The Principles were groundbreaking. The Alliance’s members have all committed to meet or exceed the commitments contained in the Principles when offering innovative vehicle technologies and services.

The Alliance and its members appreciate the careful work that the Office of the Attorney General has undertaken in drafting the proposed regulations. In particular, the Alliance welcomes the following aspects of the proposed regulations:

- Clarifying that businesses need not provide consumers with specific pieces of personal information in response to access requests if the disclosure of the information creates a substantial, articulable, and unreasonable risk to the security of that personal information, the

¹ Consumer Privacy Protection Principles (2014) [hereinafter “Principles”], available at https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf.



- consumer's account with the business, or the security of the business's systems or networks. As reflected in the comments below, however, the Alliance does request that the Attorney General clarify that disclosure should not be required where there is a substantial, articulable, and unreasonable risk to the safety or security of consumers, and not just their personal information.
- Clarifying that businesses shall not disclose certain types of sensitive information in response to a consumer's request to know. The Alliance requests, though, that the Attorney General issue regulations permitting businesses to not disclose personal information in response to a request to know where such disclosure poses a significant risk to consumers, and not just to the information itself.
- Permitting businesses to offer granular options for sale opt-out and deletion requests, so long as the options to opt-out of all sales or delete all information are presented more prominently than any other option.
- Permitting businesses to provide aggregate household information in response to a request to know household information where the requestor does not have a password-protected account. The Alliance believes that requests to know for shared devices should be afforded the same treatment as they raise the same privacy concerns as households.

The remainder of this submission contains requests for additional modifications to the proposed regulations, including those referenced above. We present first those requests that are of particular relevance to the Alliance and its members and follow with requests of general relevance:

Requests and Comments of Particular Relevance to the Alliance and Its Members

- Permitting automakers to retain vehicle-related information for purposes of analyzing and addressing safety, quality, performance, efficiency, or security issues after receiving a request to delete;
- Permitting reasonable, beneficial data sharing among manufacturers, suppliers, and dealers given the close relationship the parties have in serving consumers;
- Permitting businesses to share personal information with providers of emergency response services even where sales opt-outs have been registered;
- Providing reasonable options for businesses to comply with notice at collection requirements in the context of devices that may be resold or used by multiple individuals when the business that collects information from the devices does not know of the sale or use of the device by multiple individuals;
- Permitting businesses to disclose only aggregated information related to shared devices unless all users submit verified requests; and
- Permitting businesses to not disclose information pursuant to a request to know if the disclosure exposes consumers or others to safety or security risks.

Requests and Comments of General Relevance

- Clarifying that with appropriate notice at the point of collection, a consumer's provision of personal information to a business involved in a clearly disclosed, jointly offered service constitutes an intentional disclosure under Cal. Civil Code §1798.140(t)(2)(A);



- Deferring action on the requirements and standards for user-enabled privacy controls pending the outcome of the proposed California Privacy Rights Act Initiative that would address this issue;
- Requiring explicit consent for new uses of personal information only if the change in practice is material;
- Clarifying that businesses may comply with notice at collection requirements when not collecting personal information from consumers by obtaining examples of consumer notices and a single attestation from data sources, rather than obtaining examples and attestations for each consumer;
- Permitting businesses to require authorized agents to use the same verification process that consumers would have to undergo if submitting requests on their own behalf;
- Removing from the proposed regulations the requirement that businesses receiving sales opt-out requests notify all third parties that received personal information via sales in the 90-day period prior to the opt-out that they may not further sell the information;
- Clarifying that businesses are permitted, but not required, to use signed declarations when verifying consumer requests;
- Permitting businesses to present in their privacy policies information about the sources, use purposes, and disclosures associated with all personal information collected by the business, rather than specifying by category, so long as the disclosure reasonably helps consumers understand processing activities;
- Clarifying that each right to know request (e.g., request to obtain access to specific pieces of personal information and request to learn about the categories of personal information collected about the particular consumer) counts toward the number of requests that a business must respond to within a 12-month period;
- Requiring businesses to disclose information about the sale of personal information related to minors only if businesses have actual knowledge that they collect such information;
- Permitting businesses to display the Do Not Sell My Personal Information link only on the main page of a website and in the privacy policy, rather than requiring the link on every page, which could lead consumers to believe that they must opt-out on every page they visit.
- Clarifying that businesses may, at their discretion, use fact-finding to verify a consumer request, where personal information is maintained in a format not associated with a named individual; and
- Permitting businesses to not disclose proprietary or trade secret information in response to a consumer's request to know.

The Alliance appreciates the Attorney General's consideration of these requests and the efforts the Attorney General is undertaking to develop the regulations. Please feel free to contact us if you have any questions or would like to discuss any aspect of these comments.

REQUESTS AND COMMENTS OF PARTICULAR RELEVANCE TO THE ALLIANCE AND ITS MEMBERS

ISSUE 1: Permit Automakers to Retain and Use Vehicle-Related Information Tied to VIN Only for Safety, Quality, Performance, Efficiency, or Security After Receiving a Request to Delete

Automakers often rely on Vehicle Identification Numbers (“VINs”) to link vehicle-related information for purposes of analyzing and addressing safety, quality, performance, efficiency, and security issues. To be able to track how vehicles perform over time for these purposes, including, for example, in different weather conditions and climates, automakers collect data on vehicles by VINs. This VIN-related, longitudinal information is essential to further improve the nation’s transportation and mobility services and infrastructure. Although the benefits of such data rely on the use of VINs, other identifiers typically are not necessary. The Alliance therefore requests that the Attorney General adopt one of the proposals below to enable automakers to retain vehicle data tied to VINs for purposes of analyzing and addressing vehicle safety, quality, performance, efficiency, or security issues.

PROPOSAL 1

Issue interpretive guidance clarifying that vehicle-related data stored in association with Vehicle Identification Numbers and no other identifiers (such as name, account number, postal address, email address, telephone number, or SIM card number) is not considered consumer personal information.

PROPOSAL 2

Issue interpretive guidance clarifying that information that cannot be linked to a particular consumer without the use of additional identifiers is “deidentified” so long as the business maintaining the information stores information that could be used to identify the information separately from the deidentified information and so long as the business complies with the requirements in Cal. Civ. Code § 1798.140(h).

PROPOSAL 3

§ 999.313 Responding to Requests to Know and Requests to Delete

(d)

...

(8) The collection and internal use of personal information for analysis related to safety, quality, performance, efficiency, or security by a business or service provider constitutes “solely internal uses that reasonably aligned with the expectations of the consumer based on the consumer’s relationship with the business” under Civil Code §1798.105(d)(7) and therefore shall not be subject to a request to delete, as long as this collection and use is disclosed to consumers.

ISSUE 2: Exempt Reasonable, Beneficial Data Sharing Between Suppliers, Dealers, and Manufacturers

The CCPA exempts from sale opt-out requirements the sharing of vehicle and ownership information for purposes of effectuating “a vehicle repair covered by a vehicle warranty or a recall” if the

information is not used for any other purpose. However, vehicle manufacturers, auto dealers, and suppliers routinely share information for reasonable, non-warranty, and non-recall purposes that benefit consumers. For example:

- Dealerships may rely on manufacturer data to evaluate past, non-warranty repairs. Franchisor-franchisee sharing arrangements generally, and especially in the vehicle sales context, are efficient and consistent with consumer expectations. The sharing of information allows consumers to receive consistent services from dealers by leveraging the relationships that the dealers have with the vehicle manufacturer.
- Suppliers and manufacturers may exchange vehicle-level data to assess safety, performance, and security-related issues.

Consumers may not recognize that by asking manufacturers, dealers, or suppliers to not sell their personal information, the sharing of information between these parties will be disrupted in ways that directly affect the consumers. When traveling, consumers may be surprised to learn that an out-of-town dealer is unable to obtain past service records. Or when consumers move, automakers may not be allowed to let consumers know of the local dealers that can now service their vehicles. Consumers may not recognize that a sales opt-out may prevent suppliers and manufacturers from analyzing vehicle-performance and efficiency issues.

The sharing of information between legally distinct, unaffiliated businesses that work closely together to provide transportation and mobility services promises great benefits to consumers, who may not even recognize that such sharing, which can be among entities that use a common brand, constitutes a sale.

The Alliance therefore requests that the Attorney General clarify that such data sharing practices are not subject to the sales opt-out.

PROPOSAL 1

The Attorney General's office could issue interpretive guidance clarifying that where sharing is consistent with reasonable, informed consumer expectations and benefits consumers with regard to motor vehicle safety, security, repair, performance, or efficiency, such sharing would not be considered a "sale."

PROPOSAL 2

Adopt the following regulation

§ 999.315 Requests to Opt-Out

...

(i) A request to opt-out does not apply when information is exchanged between parties whose commercial conduct is related to the degree that informed consumers would reasonably expect the parties to share information for the purposes of benefitting the consumer with regard to safety, security, repair, performance, or efficiency issues.

PROPOSAL 3

Adopt the following definition:

§ 999.301 Definitions

“Sell,” “selling,” “sale,” or “sold,” does not include a transfer of information between parties whose commercial conduct is related to the degree that informed consumers would reasonably expect the parties to share information for the purposes of benefitting the consumer with regard to safety, security, repair, performance, or efficiency issues.

ISSUE 3: Permit Businesses to Share Personal Information with Providers of Emergency Response Services Even Where Sales Opt-Outs May Apply

Many businesses, including automakers, provide emergency response services to consumers. In emergency situations, automakers may provide these services to consumers even if they have not subscribed to or have previously opted-out of the services. Some emergency and roadside assistance services may be provided by third-party, for-profit entities that retain and use personal information for their own purposes. For example, an emergency roadside assistance provider may be an independent mechanic that wishes to establish and maintain an independent relationship with the consumer. In some cases, an accident may automatically trigger a communication from a vehicle to an emergency provider. Even though this may be a direct disclosure from the vehicle to the provider and might not involve a transfer of personal information to the automaker and then the provider, the CCPA’s definition of sale includes “making available” personal information to another entity. Accordingly, when automakers share personal information with such emergency and roadside assistance providers or make it available to them through an automatic process from the vehicle, the disclosures may constitute “sales” under CCPA. If consumers have opted-out of sales, that could prevent automakers from disclosing personal information as necessary to support the delivery of emergency services.

The Alliance therefore requests that the Attorney General permits businesses, in response to a consumer’s request for emergency or roadside assistance services, or in response to automated crash or similar notifications, share personal information with providers of such emergency or roadside assistance services.

PROPOSAL

Provide interpretive guidance that an automaker may share personal information with emergency responders or roadside assistance providers or make it available from the vehicle in emergency situations regardless of whether the consumer associated with the personal information has requested that the automaker not sell the personal information.

ISSUE 4: Modify Notice at Collection Requirements to Support Reasonable Compliance by Businesses that Manufacture Devices Reasonably Subject to Resale or Use by Non-Owners

The CCPA requires businesses to provide consumers with notice, at or before data collection, of the categories of personal information to be collected and the purposes for which the information will be used. The draft regulations add a number of obligations to this requirement, including making the notice visible or accessible where consumers will see it before any personal information is collected; using formats that draw consumer attention, including on smaller screens; and making the notice accessible to consumers with disabilities.

These requirements may present challenges for resold devices, such as certain connected vehicles, that lack displays or have displays that cannot be remotely updated. Even with displays that can be remotely updated, an automaker, for example, may have no knowledge of a vehicle resale and therefore may not be able to provide notice to the new owner. If businesses have no knowledge that a device has been resold and the device has no interface via which to present a privacy notice, businesses may be unable to guarantee that subsequent owners receive notice at or before collection of information from the sold device.

The regulations should permit notice at collection options that support reasonable compliance by businesses that collect information from devices that may change owners without notice.

Similarly, devices such as vehicles that have multiple users may collect personal information from different users. The regulations should clarify that where initial notice is provided to a registered user or account holder, the notice is sufficient with respect to non-registered users that the account holder permits to use the vehicle, device, or service.

PROPOSAL

§ 999.305 Notice at Collection of Personal Information

...

(e) A business that collects personal information via a device that is reasonably expected to change owners should take reasonable steps to provide notice at collection to subsequent purchasers of that device. The business will be deemed to have taken reasonable steps if:

(1) Notice is provided to the new owner via email, device updates, or upon device reset or reactivation; or

(2) The business posts a privacy policy on its website, if reasonable notice cannot be provided by the methods above.

(f) Notice to the owner of a device or account-holder of a service at collection constitutes notice at collection as to other users of the device or service.

ISSUE 5: Permit Businesses to Disclose only Aggregated Information Related to Shared Devices Unless All Users Submit Verified Requests

The Attorney General's draft regulations include provisions designed to address the potential privacy issues associated with requests to access or delete household information. The draft regulations propose that where a consumer does not have a password-protected account with a business, businesses may respond to requests to know related to household information by providing aggregate information. Businesses may choose to honor requests to delete or obtain access to specific pieces of information when all household members jointly issue such requests, subject to verification.

The privacy risks posed by household information also apply in the context of shared devices. Requiring compliance with the access or deletion request of a single individual with respect to a shared device could harm the privacy interests of the other individuals who use the same device. For example, a co-owner of a vehicle could request access to precise geolocation information and therefore see the other co-owner's travel history, or could delete all personal information associated with a vehicle, which request the other co-owner of the vehicle would not have agreed to. The

Alliance thus requests the Attorney General adopt provisions extending the provisions for household information to information collected from shared devices.

PROPOSAL 1

§ 999.318. Requests to Access or Delete Household or Shared Device Information

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

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

PROPOSAL 2

§ 999.319. Requests to Access or Delete Shared Device Information

(a) A business may respond to a request to know personal information relating to a device intended for use by multiple users by providing aggregate information, subject to verification requirements set forth in Article 4.

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

ISSUE 6: Businesses Should Not Be Required to Disclose Information that Exposes Consumers or Others to Safety or Security Risks

The draft regulations clarify that businesses need not provide consumers with specific pieces of personal information in response to access requests if the disclosure of the information creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks. The Alliance welcomes these exceptions to the right to know, and the benefits to security which will result.

However, the right to know poses risks not only to the security of personal information, consumer accounts, and business systems or networks, but also to consumers themselves or other individuals (e.g., where the information disclosed may relate to more than one individual and may be misused by the recipient against another individual to whom the data also relates). For example, many vehicles are driven by more than one individual, including family members or friends. Automakers have no way of knowing whether or how frequently a non-owner drives a vehicle. The disclosure of the precise location history of a vehicle can create stalking or harassment risks, endangering individual or public safety. Specifically, if a business disclosed to the owner of a vehicle the precise location history of that vehicle on grounds that the information is reasonably linked to the owner by

virtue of ownership, that could enable an abusive owner to track and harm an estranged spouse, domestic partner, or others whose traveling patterns are revealed to the owner. In some cases, no level of verification could assure an automaker that an individual has not let another individual drive his or her vehicle.

The Alliance therefore requests that the Attorney General extend the exceptions to the right to know to include exceptions for individuals' safety or security. Such a change would be consistent with Cal. Civil Code § 1798.145(m), which states that "[t]he rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers."

PROPOSAL

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

...

(3) A business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, ~~or~~ the security of the business's systems or networks, **or the safety or security of the requesting consumer or other individuals.**

REQUESTS AND COMMENTS OF GENERAL RELEVANCE

ISSUE 7: With Notice, Allow the Sharing of Personal Information with Joint Offering Partners Even Where Sales Opt-Outs May Apply

Jointly offered goods or services create significant efficiencies and benefit consumers by enabling businesses to offer and provide consumers a product or service they might not otherwise be able to obtain. Jointly offered goods or services frequently require for recordkeeping, servicing and other reasons that both distinct businesses collect the personal information and process it for their own respective purposes in providing the joint offering. In other words, each entity is not necessarily a service provider to the other. However, for some jointly offered goods or services, consumers may provide their personal information to only one of the partners, though it is appropriate and expected that the receiving business would share the personal information with the other business.

Especially if consumers are informed at the outset of receiving a jointly offered good or service that their personal information will be shared with a joint offering partner, the activity should not be controversial. As long as there is effective notice and a consumer decides to move forward with entering into a relationship involving a jointly offered good or service, it is reasonable to consider the consumer to be intentionally disclosing their personal information to both partners.

For these reasons, we request that the California Attorney General clarify that with appropriate notice at the point of collection, a consumer's provision of personal information to a business involved in a clearly indicated jointly offered service equates to an intentional disclosure under Cal. Civil Code §1798.140(t)(2)(A).

PROPOSAL

§ 999.315. Requests to Opt-Out

...

- (i) In response to a request to opt-out, a business need not cease sharing information with a third party that receives personal information from the business in association with the provision of a jointly-offered service to the consumer, provided that the identity and participation of the joint offering partner was clearly disclosed to the consumer before the consumer elected to receive the jointly-offered service.

ISSUE 8: Remove User-Enabled Privacy Control Requirements or Make Them Consistent with the California Privacy Rights Act Initiative

The draft regulations would require businesses that collect personal information from consumers online to treat “user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism,” as a request to opt-out. The provision does not clarify what sort of settings or controls should be treated as valid opt-out signals, nor would it allow any period for development and implementation of a technical standard. The Alliance understands that enabling consumer-friendly preference mechanisms can enhance privacy protections. But for such mechanisms to be effective and understandable, there must be standards or a consensus regarding what signals are valid and how signals should be interpreted.

The lack of clarity here is particularly problematic for connected vehicles and other devices that collect information “online” but do not have standard interfaces. It is not clear what would constitute a user-based privacy signal in the connected vehicle ecosystem. Technologically savvy consumers could alter vehicle systems to trigger the transmission of snippets of code whenever data was collected, intending the code to signal an opt-out request. If manufacturers do not know that code is being transmitted or how to interpret the code, the code will not be respected as an opt-out signal. Moreover, requiring vehicles to respond to the random wireless transmission of code to vehicles raises significant cybersecurity concerns. For security reasons, vehicles may not be able to ingest and process any code transmitted to it.

The proposed regulation establishes an all-or-nothing approach to privacy signals that limits consumer choice—consumers may very well wish to restrict sales to some businesses but not others, or restrict sales to data brokers, while permitting third party tags to collect information on websites in order to receive more relevant ads or personalized content.

Moreover, the proposed regulations would mandate activities that would be optional under the California Privacy Rights Act initiative (“CPRA”) that is likely to be voted on and approved in the 2020 election. The CPRA would require businesses either to implement a do not sell signal or to post a “Do Not Sell My Personal Information” link or button and honor do not sell requests through that link or button. And the CPRA would instruct a Data Protection Authority to conduct a rulemaking to flesh out how the automated controls would work.

Given the likelihood of the CPRA taking effect, it is not reasonable for CCPA regulations to require compliance with a not yet elaborated “do not sell” controls framework that is likely to be replaced in a short period of time.

For all these reasons, the Alliance requests that the Attorney General remove from the final rule the requirement that businesses must comply with “user enabled privacy signals” and revisit this issues only if the CPRA Initiative that has been filed with the Attorney General is not approved by the voters in November of 2020.

PROPOSAL

§ 999.315. Requests to Opt-Out

...

~~(c) In response to a request to opt-out, a business need not cease sharing information with a third party that receives personal information from the business in association with the provision of a jointly offered service to the consumer, provided that the identity and participation of the joint offering partner was clearly disclosed to the consumer before the consumer elected to receive the jointly offered service.~~

...

(g) A consumer may use an authorized agent to submit a request to opt-out on the consumer’s behalf if the consumer provides the authorized agent written permission to do so. A business may deny a request from an authorized agent that does not submit proof that they have been authorized by the consumer to act on the consumer’s behalf. ~~User-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.~~

ISSUE 9: Explicit Consent Should Be Required Only for Uses of Previously Collected Information that Are Incompatible with Purposes Disclosed at Original Collection

The draft regulations require businesses to notify and obtain explicit consent from consumers before using personal information for purposes not disclosed in notices at collection. The Alliance and its members agree that businesses should be transparent in their data practices and process information in ways that respect the context in which the information was collected. That is why Alliance’s members have committed to obtain affirmative consent before using certain information in ways that are materially different than what was disclosed at the time of collection. However, the mere fact that a purpose was not disclosed at the point of collection does not mean that the purpose is inconsistent with or materially different from the purposes disclosed at collection.

For example, manufacturers may collect driver behavior information collected for a range of purposes, such as enabling consumers analyze their own driving behaviors. Consumers may expect that manufacturers will use such information to improve vehicle safety, security, and performance, even if every iteration of such purpose is not expressly disclosed in a notice at collection. Moreover, obtaining opt-in consent to any privacy policy change regarding a purpose, even if minor in scope, is burdensome. It also risks consumers not receive the benefit of a new or different purpose that is not such a significant change.

The Alliance therefore requests that the Attorney General follow FTC policy and require explicit consent for new data practices only if the new practices materially differ than those disclosed at the

point of collection.² A material difference would be one that is “likely to affect the consumer’s conduct or decision with regard to a product or service.”³ If a new data processing purpose would not be likely to change the conduct of reasonable consumers, businesses should not be required to obtain consent.

PROPOSAL 1

§ 999.305 Notice at Collection of Personal Information

(a) Purpose and General Principles

...

(3) A business shall not use a consumer’s personal information for any purpose **other than materially different from or incompatible with** those disclosed in the notice at collection. If the business intends to use a consumer’s personal information for a **materially new purpose or a purpose that is not compatible with the purposes was not** previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.

PROPOSAL 2

§ 999.305(a) Notice at Collection of Personal Information

(a) Purpose and General Principles

...

(3) A business shall use a consumer’s personal information for the purposes disclosed in the notice at collection. A business shall not use a consumer’s personal information for a purpose incompatible with the stated purpose at the time of collection without explicit consent.

ISSUE 10: Clarify that Signed Attestations Are Required Per Data Source, Not Per Consumer

The draft regulations include provisions that are designed to support businesses in ensuring that consumers receive notices at collection where the businesses did not collect personal information from the consumers. The regulations provide two options for businesses that do not collect personal information directly from consumers: (1) they can contact the consumer directly to provide notice and the opportunity to opt-out; or (2) they can contact the source of the information to confirm that the source provided adequate notice at collection to the consumer and obtain signed attestations from the source describing how notice was given and an example of the notice.

The draft regulations do not specify whether businesses must obtain signed attestations for each source or for each consumer. Requiring businesses to obtain and store signed attestations on a per consumer basis would lead to substantial data transfer and storage requirements with little benefit. If the attestations and example notices are identical, then a single, representative example would suffice, so long as businesses received confirmation initially from the source that the example was

² *Id.* at viii.

³ FTC, FTC Policy Statement on Deception 1 (1983), available at https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

accurate and representative of those provided to all consumers (or to all consumers in a given context). The Alliance therefore requests that the Attorney General clarify that attestations are required per source of information.

PROPOSAL

§ 999.305 Notice at Collection of Personal Information

...

(d)

...

(2) Contact the source of the personal information to:

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

b. Obtain signed attestations from the source describing how the source **gave gives** the notice at collection and including an example of the notice **or notices the source uses to provide such notice**. Attestations **from each source of information** shall be retained by the business for at least two years and made available to the consumer upon request.

Businesses need not obtain separate attestations for each consumer unless there are material differences in the notices provided to consumers.

ISSUE 11: Businesses Can Require Authorized Agents to Use the Same Verification Processes as Consumers

The CCPA allows consumers to authorize other individuals to opt-out of sales and to submit verified requests for access or deletion of personal information on their behalf. Businesses must take reasonable steps to verify requests. However, establishing unique procedures to verify authorized agents may prove burdensome on businesses and requestors. While it should not be easier for authorized agents to submit requests than it would be for consumers to issue requests on their own, it may not always be reasonable to require authorized agents to undergo processes that are more burdensome than those offered to consumers themselves. Though, in some cases requiring authorized agents to undergo additional verification procedures may be reasonable.

Authorized agents presumably have access to the same information that consumers would have to verify identities. Thus, a reasonable option for verifying requests submitted by authorized agents, at least in some circumstances, would be for businesses to require authorized agents to undergo the same verification as the consumers for whom they act. Authorized agents could “stand in the shoes of the consumer” and provide the same data points that would be requested of the consumer.

The Alliance therefore requests the Attorney General to clarify that businesses may require authorized agents to verify requests via the same processes provided to consumers.

PROPOSAL

§ 999.308 Privacy Policy

...

(5) Authorized Agent

a. Explain how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf, **which may include requiring that the authorized agent provide the same information to the business that the consumer would need to provide if the consumer were making the request on the consumer's own behalf.**

ISSUE 12: Remove Flow-Down Obligation for Opt-Out Requests

The CCPA grants consumers the right to opt-out of future sales of their personal information. Under the draft regulations, a business that receives an opt-out request is required not only to cease selling personal information, but also to notify all third parties to which the business sold the consumer's personal information in the 90 days prior to the consumer's opt-out request that the consumer has opted out, instructing the recipients to not further sell the information.

This look-back requirement goes beyond the requirements set forth in the CCPA. And it may not reflect consumer wishes. A consumer may have specific concerns with a certain business' practices but may have no issue with the practices of the businesses that receive personal information from the initial business. In fact, the consumer may want the receiving business to continue selling personal information due to the benefits received from that business and the associated data sharing which may differ from the consumer's concerns with the business to which the consumer made the sale opt-out request.

PROPOSAL

§ 999.315 Requests to Opt-Out

~~(f) A business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the consumer's request that the consumer has exercised their right to opt-out and instruct them not to further sell the information. The business shall notify the consumer when this has been completed.~~

ISSUE 13: Clarify That Signed Declarations Are Permitted but Not Required for "Reasonably High" Verification of Consumer Rights Requests

The draft regulations provide guidance on how businesses may verify the identity of a consumer before responding to a consumer's access or deletion request. The regulations state that verification to a "reasonably high degree of certainty *may include* matching three pieces of personal information provided by the consumer with personal information maintained by the business" together with a consumer's signed declaration of identity.⁴ The regulation then goes on to state that such declarations must be maintained as part of a business' record-keeping obligations.

⁴ § 999.325(c) (emphasis added).

Although the proposed regulatory language suggests that verification “may include” signed declarations, the final sentence of § 999.325(c) could be interpreted as requiring signed declarations from consumers. Although signed declarations may be warranted in some circumstances, some businesses may be able to verify the identity of a consumer to a reasonably high degree of certainty without such declarations—such as where consumers maintain secure, password-protected accounts.

The Alliance requests clarification that the signed declaration is an optional measure for verification, at the discretion of the business.

PROPOSAL

§ 999.325 Verification for Non-Accountholders

...

(c) A business’s compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. **If businesses elect to rely on signed declarations, Businesses they shall** maintain all signed declarations as part of their record-keeping obligations.

ISSUE 14: Eliminate the Requirement that Businesses Provide the Sources, Purposes, and Sharing Activity for Each Category of Information for Privacy Policy and Access Requests

The CCPA requires businesses to provide consumers in their online privacy policies and in response to access requests, information regarding the categories of personal information collected, categories of sources for the information, purposes for collecting or selling the information, and categories of third parties with whom the business shares the information. The draft regulations specify that in online privacy policies and in response to access requests, these descriptions of sources, purposes, and sharing should be provided for each category of personal information. This requirement would result in privacy policies that are lengthier and more granular than those required by the CCPA, which permits providing three descriptions, one for all sources, one for all purposes, and one for all third parties.

The regulatory requirements may therefore lead to notices that overwhelm consumers and are in tension with the proposed regulatory requirement that privacy policies be “presented in a way that is easy to read and understandable to the average consumer.”

For businesses that rely on the same sources, seek to achieve the same purposes, and engage in common disclosures for all categories of personal information processed, these granular privacy notice requirements will yield little consumer benefit and only serve to make privacy policies longer and less likely to be read by consumers than today. Accordingly, the requirement actually harms consumers. It would be simpler and more transparent for such businesses to provide information about how they process all personal information.

The Alliance therefore asks the Attorney General to modify the disclosure regulation, requiring businesses to provide meaningful information to consumers.

PROPOSAL

§ 999.305 Notice at Collection of Personal Information

...

(b)(2) ~~For each category of personal information, A list of the business or commercial purpose(s) for which it the personal information will be used in a manner reasonably designed to help consumers understand how the business will process personal information.~~

§ 999.308 Privacy Policy

...

(b)(1)(d)(1) ~~For each category of personal information collected, p~~Provide the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties with whom the business shares personal information. The notice shall be written in a manner that provides consumers a meaningful understanding of the categories listed **and the ways in which the business processes personal information.**

§ 999.313 Responding to Requests to Know and Requests to Delete

...

(c)(10) In responding to a verified request to know categories of personal information, the business shall ~~disclose provide for the each identified category of personal information it has collected about the consumer:~~

- a. The categories of sources from which the personal information was collected;
- b. The business or commercial purpose for which it collected the personal information;
- c. The categories of third parties to whom the business sold or disclosed the category of personal information for a business purpose; and
- d. The business or commercial purpose for which it sold or disclosed the category of personal information.

ISSUE 15: Clarify Limitations on Right to Know Requests

The CCPA provides that businesses shall not be required to provide personal information to a consumer more than twice in a 12-month period. Requests to know may take the form of a request for the “specific pieces of personal information” the business has collected about the consumer, or for the “categories of personal information, categories of sources, and/or categories of third parties.” It is unclear whether each type of request would count toward the two-request limit or whether both

types of request, together, count as one request. The Alliance therefore requests that the Attorney General clarify that any single instance of a right to know request counts toward the total number of such requests that a business must honor within any 12-month period.

PROPOSAL

§ 999.313 Responding to Requests to Know and Requests to Delete

...

(c)(11) A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner that provides consumers a meaningful understanding of the categories listed.

(12) A business shall not be required to respond to a consumer's right to know request more than twice in a 12-month period, regardless of whether such right to know requests are for "specific pieces" of personal information or for "categories" of personal information.

ISSUE 16: Require Businesses to Make Statements About Sales of Personal Information Related to Minors Only If Businesses Have Actual Knowledge that They Collect Such Information

The draft regulations apply an "actual knowledge" standard to requirements relating to affirmative authorizations for sale of personal information of children under the age of 16. This "actual knowledge" standard is consistent with existing federal law under the Children's Online Privacy Protection Act. The Alliance requests that this "actual knowledge" standard apply also to the requirements regarding disclosures in privacy notices about whether businesses business sell personal information related to minors. Businesses should not be required to make statements regarding the processing of such information if they do not have actual knowledge that they hold such information.

PROPOSAL

§ 999.308 Privacy Policy

(b)(1)(e)(3) If a business has actual knowledge that it collects or maintains the personal information of minors under 16 years of age, Sstate whether or not the business sells the personal information of minors under 16 years of age without affirmative authorization.

ISSUE 17: Clarify that Placement of "Do Not Sell My Info" Link Only on the Main Page of a Website Meets "Homepage" Requirement

The CCPA requires that a link titled "Do Not Sell My Personal Information" be provided on a business's Internet homepage. The CCPA further defines "homepage" to include "any internet web page where personal information is collected." Thus, the CCPA appears to require that the Do Not Sell button appear on every webpage that collects personal information. Given the breadth of the definition of personal information and typical automated data collection, this for most businesses means each and every webpage, rendering the concept of a homepage meaningless.

Given current business practices, consumers have become accustomed to looking to the footer of a website's main page to find the Terms of Use and Privacy Statement and other legal information, and similarly in the "Settings" link or menu on a mobile app. The Alliance therefore requests that the California Attorney General exercise discretion and allow for the placement of the Do Not Sell link on a website's main page, or on a mobile app's "Settings" or menu page, to satisfy the posting to "homepage" requirement. Placement on every page of a website could be distracting and could create the impression that consumers must opt-out each time the button appears.

PROPOSAL

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

...

(b)(1) A business shall post the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link on the website's **main page homepage** or the download or landing page of a mobile application.

§ 999.315 Requests to Opt-Out

(a) A business shall provide two or more designated methods for submitting requests to opt-out, including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," or "Do Not Sell My Info," on the **main page of the** business's website or **the Settings or menu of a** mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information.

ISSUE 18: Clarify Consumer Rights Request Verification Requirements When Personal Information Is Maintained Without Association with Named Persons

The draft regulations provide that if a business maintains personal information in a manner not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with that information. The regulations contemplate that this "may require the business to conduct a fact-based verification process." This provision is helpful in the automotive context, where manufacturers may retain information associated with a VIN but not a named individual. Vehicle manufacturers may be able to verify that a certain consumer is currently associated with a VIN. But they may not be able to determine whether that consumer is associated with all of the information associated with the VIN. Vehicles change owners and are operated by multiple consumers. So, a VIN may be associated with multiple consumers.

It is not clear from the draft regulations the degree to which manufacturers would be required to perform fact-finding to confirm the consumer request. As noted above, associating the consumer

with the personal information may be challenging. The Alliance therefore requests that the Attorney General clarify that businesses have reasonable discretion to conduct fact-finding.

PROPOSAL

§ 999.325 Verification for Non-Accountholders

...

(e)(2) If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the non-name identifying information. ~~This may require~~ **The business may, in its discretion, take reasonable steps** to conduct a fact-based verification process that considers the factors set forth in section 999.323(b)(3).

ISSUE 19: Exempt Proprietary Information and Trade Secrets from Mandatory Disclosure in Response to a Request to Know

Today's vehicles deploy a variety of sensors and other technologies that collect information relating to vehicle safety, performance, efficiency, and security. Automakers devote substantial resources to determine what combination of sensors, what frequency of data collection, and what combination of information will best address those issues.

Under the CCPA, consumers have the right to request that businesses disclose the specific pieces of personal information that businesses have collected. For automakers, and other businesses, disclosing all of the specific pieces of personal information, particularly if linkages between or uses of sensor data are revealed, would expose proprietary or trade secret information. The Alliance therefore requests that the Attorney General adopt one of the proposals below to prevent businesses from being forced to disclose their proprietary or trade-secret information.

PROPOSAL 1

Issue interpretive guidance clarifying that information that reveals proprietary information or information protected by trade secret or intellectual property rights does not constitute personal information subject to the CCPA.

PROPOSAL 2

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

...

(c) Responding to Requests to Know

...

(12) A business shall not be required to disclose information that would reveal proprietary information or trade secrets in response to a request to know.



Thank you for your consideration,



Jessica L. Simmons
Assistant General Counsel



Message

From: Steve Kirkham [REDACTED]
Sent: 12/6/2019 5:59:00 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Eric Levine [REDACTED]
Subject: Berbix Inc.'s Comments on the Proposed Regulations for CCPA
Attachments: berbix-ccpa-comments-dec2019.pdf

Hi there,

Please find our comments on the proposed regulations for CCPA in the attached PDF. Should you have any questions or prefer another format, please let us know.

Regards,
Steve Kirkham
Co-Founder, Berbix Inc.



2338 Market Street
San Francisco, CA 94114

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

Email: PrivacyRegulations@doj.ca.gov

December 5, 2019

Dear Mr. Becerra,

We're Steve Kirkham and Eric Levine, the co-founders of Berbix, an identity verification company headquartered in San Francisco, California (<https://www.berbix.com/>). Prior to founding Berbix, we led the proactive Trust & Safety efforts at Airbnb.

Berbix serves companies who need identity verification for a broad range of purposes (for example, data subject request verification, age verification, fraud reduction, or compliance with regulatory requirements). Our Software-as-a-Service product enables businesses to seamlessly collect and instantly validate photo IDs, driver licenses, and passports of their customers. Moreover, we offer a selfie match and liveness check feature which makes it possible to deterministically detect whether a person is who they say they are and whether they are in front of their device in real-time.

We are writing to submit comments regarding the Text of Proposed Regulations for the California Consumer Privacy Act that your office published on October 11, 2019. In particular, we'd like to offer some suggestions relating to (i) rules regarding verification (§§ 999.323 through 999.325), (ii) the role of authorized agents (§ 999.326 and § 999.315), and (iii) the enumerated methods for providing parental consent to the sale of a child's information (§ 999.330 (a)(2)). These suggestions revolve around the idea that your regulatory framework should leverage the existing government-issued identification document infrastructure for the purposes of verifying consumers' identity when they make data requests under CCPA, and are based on our experience fighting fraud and abuse at both Berbix and Airbnb.

We believe that, should your office follow our suggestions, the resulting regulatory framework would improve the ability of Californians to exercise their rights, while simultaneously limiting the ability of bad actors to fraudulently usurp Californians' rights. Moreover, the clarifications that we're suggesting would facilitate compliance with CCPA for businesses and for the third-party identity verification services that serve them. While our company, Berbix, could potentially benefit from some of our suggestions, it is our strong conviction that our own personal information, and that of all other California residents protected by CCPA, would be better safeguarded if you were to adopt our suggestions. Our comments follow, starting at page 3 of this letter.

We're available to provide further information to your office if we can make ourselves useful in any way, and are eagerly looking forward to the entry into force of CCPA on January 1st, 2020.

Best regards,

Steve Kirkham

Steve Kirkham
Co-Founder, Berbix Inc.

Eric Levine

Eric Levine
Co-Founder, Berbix Inc.

Berbix Inc.'s Comments on the Proposed Regulations for CCPA

(i) Rules regarding verification (§§ 999.323 through 999.325)

The Rules Regarding Verification in Article 4 of your Proposed Regulations should be amended to ensure that the requirements for identity verification effectively delineate the need to authenticate the consumer who is submitting a request from the need to tie that authenticated consumer with records held by the business. In addition, the Proposed Regulations should be amended to make it easier for businesses to rely on third-party identity verification services, who should be habilitated to perform an adequate level of identity verification, for example, by verifying a person's identity through the use of a government-issued identity document.

As they stand, §§ 999.323 through 999.325 do not effectively delineate the need to authenticate the consumer who is submitting a request from the need to tie that authenticated consumer with records held by the business. In the proposed regulations, these two distinct concerns appear to be at times merged together, so that business may be able to comply with your regulations merely by matching a few data points with information provided by an individual. While such a method may be adequate in cases where the business does not maintain information in a manner "associated with a named actual person" (§ 999.325 (e)(2)), it unnecessarily creates an important vector for fraud in all other cases.

Research has shown that when companies use weak identity verification mechanisms for verifying the identity of consumers submitting data access requests, it is extremely easy for even moderately skilled bad actors to exfiltrate data or cause it to be deleted.¹ In addition, bad actors can leverage data obtained in a first flight of fraudulent requests to be able to exfiltrate more data in subsequent requests to other businesses, as they may in the process have acquired more information to "match" against.² Moreover, with the prevalence of large-scale data breaches, the information that businesses may want to use for matching to an individual's identity might already be readily available to bad actors.

By properly distinguishing the task of verifying a consumer's identity with that of identifying the data that a business has about a consumer, and by reinforcing the role of third-party identity verification services, your regulatory framework could be improved to minimize fraud while simultaneously preventing businesses responding to Californians' requests from directly collecting sensitive information from them.

We suggest you make the following changes to the Proposed Regulations:

¹ See in a GDPR context, "GDPArrrr: Using Privacy Laws to Steal Identities", Black Hat Conference 2019, <https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf>

² See note 1.

- With respect to the procedures that can be used for verification, third-party identity verification services should only be subject to the restrictions that are relevant to them (§ 999.323 (c)). In particular, third party verification services should explicitly be authorized to request additional information from consumers for purposes of verification. However, such services would only be authorized to disclose to the business the set of information that the business would be able to collect if it wasn't using a third-party identity verification services (i.e. the information necessary to tie records to a given verifiable consumer request).
- Relying on a password-protected account for verification should explicitly be designated as insufficient for requests pertaining to sensitive data (§ 999.324 (a)). Indeed, consumers often reuse the same passwords and are often allowed by businesses to use simple passwords. Given how common data breaches are, it could be trivial for a third-party to guess a consumer's password and make CCPA requests on their behalf. Rather, requests pertaining to sensitive data should be subject to the higher requirements of § 999.325. While such a requirement may increase the burden of verification for consumers, it ensures that their information is adequately safeguarded, and that third-parties cannot improperly access their data or cause it to be deleted.
- Finally, the text of the Proposed Regulations should more granularly distinguish between the task of verifying the identity of a consumer, and the task of identifying the information that the business has which relates to a consumer (in particular at § 999.325). In addition, we strongly recommend that you remove the recommendation for the use of a signed declaration under penalty of perjury as an adequate modality for verification in cases where a higher bar is required in § 999.325 (c), as such a requirement is not only unlikely to deter bad actors, but could also be very easily circumvented by such bad actors willing to forge such a declaration, particularly when requests to know can be submitted over the Internet. Rather, you should encourage businesses to rely on the verification of a government-issued identification document, as such documents are effectively a "gold standard" method of identification, especially when matched with a live picture of the document holder.

The Text of the Proposed Regulations could be amended as follows:

§ 999.323. General Rules Regarding Verification

[...]

(c) A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may

request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, and for security or fraud-prevention purposes. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 999.317. If the business is using a third-party identity verification service, that third-party identity verification service may request additional information from the consumer for purposes of verification, but shall share with the business only the information necessary for the business to locate the information that the business has about the consumer.

[...]

§ 999.324. Verification for Password-Protected Accounts

(a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 999.323. The business shall also require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data. The use of a password-protected account shall not be sufficient for requests pertaining to sensitive or valuable personal information, which shall warrant a more stringent verification process complying with the requirements of section 999.325.

[...]

§ 999.325. Verification for Non-Accountholders or for Requests Pertaining to Sensitive or Valuable Personal Information

(a) If a consumer does not have or cannot access a password-protected account with the business, or if the consumer's request pertains to sensitive or valuable personal information, the business shall comply with subsections (b) through (g) of this section, in addition to section 999.323.

(b) A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data points extracted from a government-issued identification document provided by the consumer with data points maintained by the business, which the business has determined to be reliable for the purpose of verifying the consumer.

(c) A business's compliance with a request to know specific pieces of personal information

requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may include matching at least three pieces of personal information extracted from a government-issued identification document provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with the matching of a picture of the consumer's face taken at the moment of the submission of the consumer's request with the picture found on the consumer's government-issued identity document ~~a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. Businesses shall maintain all signed declarations as part of their record-keeping obligations.~~

(d) A business's compliance with a request to delete may require that the business verify the identity of the consumer to a reasonable degree or a reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion. For example, the deletion of family photographs and documents may require a reasonably high degree of certainty, while the deletion of browsing history may require a reasonable degree of certainty. A business shall act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with the regulations set forth in Article 4.

(e) Illustrative scenarios follow:

(1) If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide ~~evidence that matches the personal information maintained by the business, a copy of a government-issued identification document.~~ For example, if the business maintains the consumer's name ~~and credit card number~~, the business may require the consumer to ~~provide the credit card's security code and identifying a recent purchase made with the credit card to verify their identity to reasonable degree of certainty~~ compare the name of the consumer as it appears on the consumer's identity document with the name in records maintained by the business, and compare a picture of the consumer collected for verification purposes with the picture appearing on the consumer's government-issued identity document.

[...]

(ii) The role of authorized agents (§ 999.326 and § 999.315)

We suggest that your office changes § 999.326 (a)(2) to remove the ability for businesses to require that consumers using an authorized agent verify their own identity directly with the business in cases where a password-protected account is not a sufficient or available means of verifying a consumer's identity. We also suggest subjecting authorized agents to rigorous security and data privacy obligations (§ 999.326 (d)). Moreover, we suggest that your office explicitly clarifies that a permission obtained through electronic means shall be a satisfactory means for an authorized agent to obtain permission to act on a consumer's behalf (§ 999.326 (a)(1) and § 999.315).

The Proposed Regulations include the ability for businesses to force consumers using an authorized agent in their requests to know and requests to delete to verify their identity directly with the businesses whom they seek to exercise their rights with. This could effectively decrease consumers' ability to exercise their rights when a password-protected account is not an adequate or available means of verifying their identity with a business. In addition to the risks enumerated in our suggestions relating to §§ 999.323 through 999.325 ((i), above), this means that consumers may have to verify their identity with dozens, if not hundreds of different entities, with varying levels of privacy and security controls if they desire to control the way their information is handled.

Rather, in such cases, consumers should be able to verify their identity with an authorized agent, who would then be able to certify or otherwise attest to the business, electronically or in writing, that they have verified the consumer's identity in accordance with § 999.323. The authorized agent would be authorized to reveal to the business only the information that is strictly necessary for the business to satisfy the consumer's request.

Authorized agents should be a cornerstone of consumers' ability to exercise their rights under CCPA, thereby realizing the objective stated in your Initial Statement of Reasons of setting the ground for innovation and the development of new technology in this area. Authorized agents could be required to register with your office, and should be subjected to risk-appropriate requirements with respect to data protection and security measures that exceed the more general requirements of § 999.324 (d) (for example, the obtention of a SOC 2 report issued by an independent third-party auditor). Moreover, they should be strictly limited in the use they could make of consumers' information for any purpose other than verification or fraud prevention. Subject to such requirements, authorized agents could be an effective means through which you could ensure that Californians can effectively exert their rights under CCPA, while minimizing the risk of fraud committed by bad actors.

The Text of the Proposed Regulations could be amended as follows:

§ 999.326. Authorized Agent

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, the business may require that the consumer:

(1) Provide the authorized agent written or electronic permission to do so; and

(2) Verify their own identity directly with the business in cases where section 999.324 is applicable to the request submitted by the authorized agent on the consumer's behalf.

(b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4000 to 4465.

(c) A business may deny a request from an agent that does not submit proof that they have been authorized by the consumer to act on their behalf.

(d) Authorized agents shall implement and maintain a data protection program comprising risk-appropriate controls with respect to data privacy and security measures, and shall not use information collected from or about consumers while acting on consumers' behalf for any purpose other than verification or fraud prevention purposes.

§ 999.315. Requests to Opt-Out

[...]

(g) A consumer may use an authorized agent to submit a request to opt-out on the consumer's behalf if the consumer provides the authorized agent written **or electronic** permission to do so. A business may deny a request from an authorized agent that does not submit proof that they have been authorized by the consumer to act on the consumer's behalf. User-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.

[...]

(iii) The role of authorized agents with respect to requests to opt-out of the sale of information (§ 999.315)

§ 999.315. Requests to Opt-Out

[...]

(g) A consumer may use an authorized agent to submit a request to opt-out on the consumer's behalf if the consumer provides the authorized agent written **or electronic** permission to do so. A business may deny a request from an authorized agent that does not submit proof that they have been authorized by the consumer to act on the consumer's behalf. User-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.

(h) A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request. The business shall inform the requesting party that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent.

(iii) The enumerated methods for providing parental consent to the sale of a child's information (§ 999.330 (a)(2))

We suggest that you supplement the non-exhaustive list of methods for providing parental consent to the sale of a child's information (§ 999.330 (a)(2)) to include "Face Match to Verified Photo Identification", a method approved by the FTC in the context of COPPA.

The approach taken in the Proposed Regulations is to transpose the requirements elaborated by the FTC in the context of COPPA to the parental consent mechanism of CCPA. However, the enumeration of reasonably calculated methods in § 999.330 (a)(2) appears to be a direct copy of 16 CFR § 312.5, which doesn't reflect additional methods that the FTC has deemed sufficient to satisfy the COPPA parental consent requirements under the FTC's Rule Safe Harbor program (16 CFR § 312.5 (b)(3)).

In 2015, in an effort to reflect technological evolutions since the COPPA Rule was first drafted, the FTC approved an additional method for verifying parental consent, described by the FTC as "Face Match to Verified Photo Identification". That method is one by which a picture of the identification document of the parent is collected through a website or an app, along with a picture of the parent's face, the latter of which is scanned to ensure that the picture is one of a live person (and not a picture of a picture) and is matched to the face displayed on the photo identification using facial recognition technology.^{3,4} This method was deemed by the FTC to be superior to other methods approved in the COPPA Rule itself. Indeed, in its thorough review of the technology, the FTC noted:

The [Face Match to Verified Photo Identification] method is very similar to an existing [verifiable parental consent] method already in the Rule, which calls for verifying a parent's identity "by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete." The proposed method does not involve checking the government-issued identification against databases of such information, but, as noted above, does involve verification of the

³ "FTC Grants Approval for New COPPA Verifiable Parental Consent Method", November 19, 2015, <https://www.ftc.gov/news-events/press-releases/2015/11/ftc-grants-approval-new-coppa-verifiable-parental-consent-method>.

⁴ To the best of our knowledge, there is only one other method that was similarly approved by the FTC, Knowledge-Based Identification (<https://www.ftc.gov/news-events/press-releases/2013/12/ftc-grants-approval-new-coppa-verifiable-parental-consent-method>). However, this method was approved in 2013, and as noted in a 2019 report by the U.S. Government Accountability Office, "data stolen in recent breaches, such as the 2017 Equifax breach, could be used fraudulently to respond to knowledge-based verification questions. The risk that an attacker could obtain and use an individual's personal information to answer knowledge-based verification questions and impersonate that individual led the National Institute of Standards and Technology (NIST) to issue guidance in 2017 that effectively prohibits agencies from using knowledge-based verification for sensitive applications". See "Federal Agencies Need to Strengthen Online Identity Verification Processes", June 14, 2019, <https://www.gao.gov/products/GAO-19-288>.

identification document to ensure its authenticity. **The proposed method is more rigorous than the existing approved method in that it involves the use of facial recognition technology to check that the individual to whom the identification was issued is the same individual who is interacting with the system at that moment.** Both methods involve prompt deletion of the identification information collected from the parent.⁵ [our emphasis]

The addition of “Face Match to Verified Photo Identification” method to the enumeration in § 999.330 (a)(2) would reduce uncertainty for businesses that are evaluating how to comply with CCPA and encourage their reliance on the more robust means of verifying a parent’s identity that recent technological advances have enabled.

The Text of the Proposed Regulations could be amended as follows:

§ 999.330. Minors Under 13 Years of Age

[...]

(a) (2) Methods that are reasonably calculated to ensure that the person providing consent is the child’s parent or guardian include:

- a. Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;
- b. Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;
- c. Having a parent or guardian call a toll-free telephone number staffed by trained personnel;
- d. Having a parent or guardian connect to trained personnel via video-conference;
- e. Having a parent or guardian communicate in person with trained personnel; and

⁵ “Commission Letter Approving Application Filed by Jest8 Limited (Trading As Riyo) For Approval of A Proposed Verifiable Parental Consent Method Under the Children’s Online Privacy Protection Rule”, November 19, 2015, <https://www.ftc.gov/public-statements/2015/11/commission-letter-approving-application-filed-jest8-limited-trading-riyo>.

f. Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information, where the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.

g. Verifying a parent or guardian's identity by checking a form of government-issued identification and using facial recognition technology to check that the individual to whom the identification was issued is the same individual who is interacting with the business, where the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.

[...]



December 6, 2019

Via Electronic Mail

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

Re: Notice of Proposed Rulemaking – California Consumer Privacy Act

Dear Privacy Regulations Coordinator:

The Bank Policy Institute (BPI)¹ appreciates the opportunity to submit comments on the Attorney General's proposed regulations under the California Consumer Privacy Act.² BPI member banks are dedicated to protecting customer data, and they have adopted robust privacy and information security programs with administrative, technical, and physical safeguards designed to achieve that important goal. These programs are designed pursuant to and consistent with the requirements of state, federal and foreign laws, notably the federal Gramm-Leach-Bliley Act (GLBA)³ and its implementing regulations. Therefore, BPI member banks already adhere to notice and disclosure requirements, protect the security and confidentiality of customer information, protect against anticipated threats or hazards to the security or integrity of customer information, and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to customers.⁴ These programs are tailored to the size, complexity, activity, and overall risk profile of a bank, as contemplated under federal law.⁵

¹ The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost two million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

² Cal. Civ. Code § 1798.100 *et seq.*

³ 15 U.S.C. § 6801 *et seq.*

⁴ As noted by President Clinton in signing the GLBA into law, the GLBA requires banks to "clearly disclose their privacy policies to customers up front...consumers will have an absolute right to know if their financial institution intends to share or sell their personal financial data, either within the corporate family or with an unaffiliated third-party [and]...will have the right to "opt out" of such information sharing with unaffiliated third parties...[and] allows privacy protection to be included in regular bank examinations...[and] grants regulators full authority to issue privacy rules and to use the full range of their enforcement powers in case of violations." William J. Clinton, Statement on Signing the Gramm-Leach-Bliley Act, November 1999. Available at web.archive.org/web/20160322081604/http://www.presidency.ucsb.edu/ws/?pid=56922; accessed Nov. 20, 2019.

⁵ See, e.g., Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 30, app. B (2018).

I. Executive Summary

Given the CCPA's January 1, 2020 effective date and the separate, statutorily required, regulatory effort it is important that the Attorney General endeavor to harmonize any new requirements with the structure established by the CCPA itself. This harmonization is critical, both to allow businesses adequate time to test and implement strong compliance policies and processes and to help consumers understand their rights and responsibilities. Clarity and consistency are vital to achieving the CCPA's goal of putting consumers in control of their privacy online.

It is also crucial that the Attorney General recognize and align regulatory efforts with the long-standing and effective frameworks that banks have built over decades, under federal standards, to protect the privacy and security of consumer data. Banks already employ extensive programs in these areas, which differ from those utilized by other sectors of the economy. The regulations should take these programs into account and ensure that consumer protections are not unintentionally weakened by companies' CCPA compliance efforts.

In Part II of this letter, we propose amendments to the draft regulations to address such issues. In Part III, we describe two provisions of the regulations that, while not substantively problematic, would benefit from further clarification.

II. Proposed Amendments

- A. The effective date of the regulations should be at least six months after the final regulations are published, to account for the imposition of requirements that go beyond the statute, and the Attorney General should not undertake enforcement actions for conduct that occurs before January 1, 2021.**

As explained throughout these comments, the CCPA is a highly complex statute that requires businesses to invest significant time and resources in compliance. The proposed regulations, even if modified as recommended in this letter, will add additional implementation expectations to that effort, and it will take time for businesses to design, test, and implement compliant systems and processes. Many of these burdens are not contemplated by the CCPA itself, and so businesses have had less than two months to evaluate the implementation requirements of the proposed regulations, much less to invest substantial resources into compliance, given the uncertain nature of any final and binding rules. Thus, the Attorney General should provide a transitional implementation period to allow firms to establish and test compliance procedures that reflect the final regulations. Requiring businesses to compress this timeline unreasonably is likely to lead to mistakes and omissions that ultimately do not benefit consumers or the goals of the CCPA.

Section 11343.4(b)(2) of the California Government Code permits agencies to prescribe an effective date for regulations different from the default date unless the statute requires otherwise. The CCPA does not prescribe the effective date for the Attorney General's regulations, only for the CCPA itself. The Attorney General therefore has the authority to prescribe a later effective date for the regulations.

Even if the regulations are presumed to be enforceable on the same date as the statute, Section 1798.185(c) of the CCPA can reasonably be read to state that enforcement shall not begin until "six months after [1] the publication of the final regulations issued pursuant to this section or [2] July 1, 2020, whichever is sooner." That is, enforcement could be interpreted to be permitted either on January 1, 2021 or six months after the regulations are finalized, whichever is sooner. This reading is consistent with principles of fair notice and harmonizes with the legislature's clearly indicated intent to give businesses a reasonable amount of time (six months) to come into compliance with the Attorney General's regulations, which are not required to be finalized until July 1, 2020. Furthermore, it is common practice to allow such a period to give businesses a chance to interpret and implement regulations. Reading the statute to allow enforcement of the regulations on the very day they are made effective would be unjust.

The CCPA does not require the Attorney General to begin enforcement as soon as he is permitted to do so but instead leaves the commencement of enforcement efforts to the Attorney General's discretion. Thus, even if the Attorney General is statutorily empowered to begin enforcement of the final regulations on July 1, 2020, BPI would recommend that he refrain until January 1, 2021 in order to give businesses adequate time to develop compliance systems and processes, adequately test these procedures, and implement them. Doing so would better serve the interests of consumers by decreasing the risks of identity theft and security breaches that could result from hastily implemented compliance measures.

Finally, any "look back" requirements and enforcement activity should commence upon the implementation date of the CCPA regulations. Federal agencies have taken a similar approach with respect to data subject to "look back" periods in order to provide adequate time to institutions to effectively implement regulatory expectations.⁶

- B. The requirement in § 999.313(d)(1) that if a business cannot verify the identity of a requestor seeking deletion it shall instead treat the request as a request to opt out of sales does not comport with the text of the CCPA or a reasonable inference of consumer intent and should be removed.**

The CCPA treats the right to delete and the right to opt out of the sale of personal information as separate, placing them in distinct sections of the statute and subjecting them to distinct sets of exceptions. There does not seem to be any legal basis to convert a request to an unrequested, unrelated action because the requestor's identity could not be verified.

Additionally, without knowing who the consumer is, a business may not be able to fulfill the opt-out request or may have to opt out individuals who may not be the actual requestor, such as those who happen to share the same name. This would counter the intent of the statute to give consumers controls over their personal information, which is unreasonable and ill-advised.

If a request to delete cannot be verified, the only required action should be to inform the requestor of that fact; we therefore recommend that the attending opt-out expectations be removed. The business is separately required to provide the requisite notices and opportunities for the consumer to opt out of the sale of their information if they wish to do so.

- C. Section 999.323(c)'s statement that businesses shall "generally avoid" requesting additional information from the consumer for the purpose of verification is at odds with the need to ensure verification and should be removed.**

The CCPA's references to the verification of consumer requests serve as a protection of consumers' interests in the integrity and security of their personal information. It is not possible for businesses to determine with certainty at the outset what information and procedures will be necessary to verify a consumer's identity in all cases. This is particularly true because banks will be required to respond to requests from non-customers under the CCPA, and they often will not know at the outset what information they may have on such individuals that could be used for verification purposes. Discouraging businesses from asking for additional information when it is needed for reasonable verification efforts will only harm consumers and increase the likelihood of fraudulent requests. Despite efforts in the proposed regulations to decrease the value to fraudsters of submitting right-to-know requests, there is still a significant risk of disclosure of personal information to a bad actor or from the deletion of a consumer's

⁶ For example, in 2016, the Financial Crimes Enforcement Network chose not to require identification of beneficial owners on a "look back" basis prior to the May 11, 2018 implementation date of its Customer Due Diligence rule, as it felt it would be "unduly burdensome" due to the "significant changes to processes and systems that [covered institutions were] required to implement" under the rule. See 81 Fed. Reg. 29,404 (May 11, 2016).

personal information against their wishes. In order to reduce these risks, the Attorney General should encourage businesses to take all reasonable steps to verify a consumer's identity before responding to a request.

BPI members and other banks have rigorous procedures in place to comply with Know Your Customer (KYC) requirements⁷ that are well-suited to the verification required by the CCPA. It would better serve consumers' interests for banks to provide the full amount of protection these procedures offer, instead of watering them down for CCPA compliance purposes.

Furthermore, although the Attorney General's Statement of Reasons indicates that this provision is meant to "protect consumers by prohibiting businesses from using verification as an excuse to collect and use personal information for other means," the statute, as well as the proposed regulations, have established other safeguards to prevent such behavior. Section 1798.130(a)(7) of the CCPA requires businesses to "[u]se any personal information collected from the consumer in connection with the business' verification of the consumer's request solely for the purposes of verification." The second sentence of § 999.323(c) further requires that any additional information collected be used only for verification, security, or fraud-prevention purposes. Given these prohibitions, the potential harms to consumer privacy from weakened verification methods outweigh reduced risk of misuse by businesses that this regulatory language might accomplish. We therefore recommend that this language be removed from the final rule.

D. The requirement in § 999.325 that businesses provide two types of right-to-know requests with two different levels of authentication scrutiny would impose burdensome implementation requirements that go beyond the statute and do not benefit consumers.

Requiring multiple verification tiers for right to know requests, as the draft regulations contemplate, has no foundation in the statute and would not benefit consumers. Providing information even about the categories of personal information collected without adequate identity verification can pose security risks. A financial institution generally does not disclose whether a consumer has an account with it unless it is able to verify the consumer's identity. This is because bad actors can use information about the institution or other institutions with which a consumer has accounts to commit identity fraud. By providing individuals with information about data that has been collected on a consumer without verifying their identity to a high level of confidence, businesses run a significant risk of aiding identity thieves in their attempts to harm consumers.

If a business chooses to have multiple tiers of verification based on the sensitivity of the data and the level of risk, that should be permitted, but it should not be a requirement placed on all entities. The Initial Statement of Reasons does not specify why this differentiation is "reasonably necessary" to protect consumer privacy, nor does it address the concern that such an approach could actually result in identity theft. The regulations should instead encourage businesses to take all reasonably necessary steps—including use of existing KYC procedures, if they exist—to verify a consumer's identity before responding to a request. This aligns with the guidelines established by § 999.323(b)(3) of the draft regulations.

Relatedly, BPI requests that the Attorney General clarify that the requirement in §§ 999.308(b)(1)(c)-(b)(2)(c) and § 999.313(a) that a business describe the process used to verify consumer requests, including any information the consumer must provide, may be satisfied with a description at a high level of generality. Requiring more detailed descriptions of verification processes could aid bad actors in their efforts to exploit the system for fraudulent purposes. This is particularly true for banks, where information gathered about an individual's accounts with one institution is often used by identity thieves to attempt to gain access to accounts or to create new accounts at other institutions.

⁷ Although the term "KYC" is not used in regulations, it is generally used in industry and regulator parlance to refer to institutions' obligations to collect, analyze, and use information about their customers to comply with various anti-money laundering and sanctions requirements that require financial institutions to understand, to some extent, the nature and identities of the parties with whom or on whose behalf they are conducting financial transactions.

- E. Requiring publication of metrics regarding responses to consumer requests in a business's privacy policy, as § 999.317(g) would, will not benefit consumers, but could increase the risk of identity fraud. These metrics should instead be provided upon request to the AG.**

The metrics described by § 999.317(g) are intended to gauge a company's compliance with the CCPA. Since the statute is enforced by the Attorney General and not by the consumers for whom a privacy policy is drafted, it would be more appropriate for businesses to be required to provide them to the Attorney General upon request. Placing them in the privacy policy would only serve to increase the length and complexity of a document that is intended to be digestible by consumers, without providing them any useful information about how their personal information is collected or used. In addition, the posting of metrics provides additional information for fraudsters looking to attack companies with fraudulent requests. For example, businesses with metrics showing a high rate of fulfilling requests are likely to become victims of fraudulent requests, where fraudsters may avoid a business with metrics showing a high percentage of access request denials. Finally, such an approach is in line with Section 11346.3(a) of the California Administrative Procedure Act, which states that an agency must consider the impact on California businesses and avoid imposing "unnecessary or unreasonable regulations or reporting, recordkeeping, or compliance requirements."

- F. The requirement in § 999.313(d)(4) that a business must specify the manner in which it has deleted information is burdensome, confusing, and unnecessary, and it should be removed.**

In a large business, the process of responding to a request to delete personal information will be complicated, likely involving many systems and business units. Some data elements may be deleted outright, while others are deidentified, or otherwise modified to place them outside the scope of the CCPA's definition of personal information. Providing a detailed description of this process would be burdensome and, rather than providing "greater transparency about the business's practices in deleting personal information" as the Initial Statement of Reasons contemplates, would in fact create confusion for consumers. For example, consumers may not appreciate the differences between deletion, deidentification, and aggregation. Businesses should instead be permitted to simply inform a consumer that their personal information has been deleted, or to inform them of the reasons it has not been deleted, as provided by § 999.313(d)(6) of the proposed regulations.

- G. Section 999.305(d)'s requirement that a business obtain attestations of compliance from third-party collectors if the business does not directly collect information from a consumer is confusing and lacks statutory basis.**

Under § 999.305(d), a business is not required to provide initial notice if it is not directly collecting personal information from the consumer. However, this provision requires that businesses ensure that the party that provided (sourced) the data gave the consumer the initial notice mandated by the CCPA. It also requires that businesses retain a "signed attestation" by that party to confirm the third party's adherence with the initial-notice requirement.

This requirement is problematic because it places the burden on the business receiving data to confirm that all parties who are sourcing data are complying with their CCPA notice obligations. The requirement has no basis in the text of the CCPA. Third parties who provide data should be the ones maintaining any documentation of their compliance with their notice obligations, in line with the provisions set forth in Civil Code section 1798.115(d).

- H. The requirement in §§ 999.305(b)(2), 999.308(b)(1)d.2, and 999.313(c)(10) that information be presented category by category rather than in the aggregate—contrary to how the language of the CCPA is reasonably read—will result in consumer confusion and should be removed.**

Given the level of detail that the proposed regulations would require in these sections, consumers are likely to be overwhelmed by the quantity of information, without providing a more meaningful understanding of a business's

data practices. There are 11 CCPA categories of personal information, a proposed minimum of three source types, and seven third-party types, along with an uncertain number of uses or purposes of collection, all of which businesses would be required to describe both in a privacy notice and in customized responses to access requests. Under the draft regulations' approach of requiring this information to be described "category by category," which goes beyond a reasonable interpretation of the statute's requirements, this could require many additional pages to communicate the various permutations of these pieces of information. Even for a business of moderate complexity, for example, a notice could run to more than 20 pages. This would be overwhelming to consumers, and it is unclear if and how this information could be presented on a small screen, as the draft regulations require.

These provisions would impose a large administrative burden on businesses of all sizes, without meaningfully adding to consumers' understanding—and, in fact, quite possibly detracting from it. Therefore, we recommend that it be limited, as it is under the statute, to personal information that is sold.

I. Section 999.306(d)(2) appears to require that a business that begins selling personal information obtains opt-in consent from every consumer who the business has previously interacted with. This would be extremely burdensome and lacks statutory basis.

If a business that has not previously sold personal information decides to begin doing so—or if an aggressive interpretation of the CCPA's definition of "sale" is adopted that encompasses practices a business did not believe were included—§ 999.306(d)(1) prohibits it from selling information collected during the period when it did not post a notice of right to opt-out. This limitation is sufficient to provide the protection for consumers intended by the CCPA's right to opt out from sale. Consumers who interact with a business that does not sell their information have not thereby expressed any affirmative desire to opt out of the sale of their information, and it would be in tension with the statutory framework to treat them differently from other consumers.

Additionally, it may be very difficult or impossible for a business to implement this provision. Determining all consumers whose personal information may have been previously collected and contacting them to obtain consent may not be possible, depending on the information a business maintains. Instead, businesses should be prohibited from selling information that was collected without the proper notices in place, and they should be required to adhere to the practices disclosed at the time of collection for that data going forward (unless opt-in consent is obtained), but they should not be restricted from changing their practices and providing the same CCPA rights as any other business in relation to data collected in the future. BPI would recommend that businesses be required to give consumers a reasonable period of time to opt out after the requisite notices are provided, as is required, for example, by the GLBA.⁸

J. The 12-month lookback in the regulations and the statute should not be enforced in relation to conduct occurring before the effective date of the CCPA.

As of January 1, 2020, when the CCPA is effective, businesses will be required to make various disclosures about their practices for the past 12 months regarding collection, use, and sale of personal information. However, since the CCPA's definitions, particularly those of "sale" and "personal information" differ significantly from definitions in other statutes, some businesses may have difficulty ascertaining the precise set of data points they collected or transfers they engaged in that would fit these definitions. Accordingly, BPI would recommend that the Attorney General not bring enforcement actions based on disclosures of conduct occurring before the effective date of the CCPA, as long as businesses make reasonable efforts to give consumers an understanding of their practices.

⁸ See 16 CFR § 680.24.

K. Section 999.325(e)(2)'s instruction that businesses use a "fact-based verification process" for information not associated with a particular consumer should be removed.

For personal information that is not associated with a "named actual person," businesses are advised in § 999.325(e)(2) to conduct a "fact-based verification process" to allow a consumer to show that they are the only person associated with the personal information. This provision appears to require businesses to reidentify or link information that is not maintained in a manner that would be considered personal information, in contradiction of the CCPA.⁹ BPI requests that this provision be removed, or that the Attorney General clarify that the provision is a recommendation rather than a requirement and that it does not require re-linking of non-personal information. Additionally, if the provision is retained, BPI requests that the Attorney General clarify the meaning of the term "fact-based verification process."

III. Requests for Clarification

A. The regulations should clarify that consumers should not be able to skirt the rules of discovery during litigation by exercising rights under the CCPA.

The regulations should consider—and affirmatively prevent—the ability of a consumer to initiate a CCPA access or deletion request in lieu of discovery in a court matter. If not prevented, individuals would be able to circumvent established legal discovery rules under the false pretense of exercising a state-law privacy right. BPI requests that the Attorney General clarify that Section 1798.145(a)(4) of the CCPA, which states that the law shall not restrict a business's ability to "[e]xercise or defend legal claims" prevents this sort of avoidance of discovery rules.

B. The regulations should clarify that § 999.306(d)(2) does not restrict a business from changing its practices to begin selling personal information, if proper notice is given and opt-out mechanisms are provided.

Section 999.306(d)(2) requires that, for a business to be exempt from providing a notice of right to opt-out, it must "state in its privacy policy that it does not **and will not** sell personal information" (emphasis added). On its face, this would appear to restrict a business that does not sell information (and that therefore does not provide a notice of right to opt-out) from ever changing this practice. However, § 999.306(d)(1) plainly contemplates that the business only must refrain from selling information collected during the time period during which the notice of right to opt-out is not provided. BPI requests that the Attorney General clarify that § 999.306(d)(2) merely requires a business to state that it will not sell personal information collected during the time period during which the notice of right to opt-out is not provided.

The Bank Policy Institute appreciates the opportunity to submit comments concerning the Attorney General's draft regulations. If you have any questions, please contact the undersigned by phone at [REDACTED] or by email at [REDACTED].

Respectfully submitted,



Angelena Bradfield
Senior Vice President, AML/BSA, Sanctions & Privacy
Bank Policy Institute

⁹ See Cal. Civ. Code § 1798.100(e).

Message

From: Meghan Pensyl [REDACTED]
Sent: 12/6/2019 8:04:02 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Kate Goodloe [REDACTED]
Subject: BSA Comments on Proposed CCPA Regulations
Attachments: 2019.12.6 - BSA comments on CCPA AG Regulations - FINAL.pdf

To whom it may concern:

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

Many thanks.

Best,
Meghan





December 6, 2019

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

RE: Proposed Text of Regulations to Implement the California Consumer Privacy Act

Dear Attorney General Becerra:

BSA | The Software Alliance appreciates the opportunity to submit comments on proposed regulations to implement the California Consumer Privacy Act (“CCPA”).

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

BSA submits these comments to address the unique role of service providers, which create the products and services that other businesses rely on. Service providers have important obligations to safeguard the privacy of data they process and maintain. The CCPA recognizes this role, including by requiring service providers to act on behalf of businesses and at their direction. A broad reading of the draft regulations risks upsetting the business-service provider relationship set out in statute. We urge three revisions to the draft regulations to avoid that result:

- *First*, to ensure that service providers can meet the specific requests of their customers, the regulations should expressly state that a service provider may use personal information received from a business or consumer to serve another entity—*when a business or consumer directs it to do so*.
- *Second*, and for the same reason, the regulations should also expressly state that a service provider may combine information received from one or more businesses,

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

when doing so is needed to provide and maintain the services and related services provided to those businesses.

- *Third, the regulations should clarify that a service provider should only respond to consumer requests sent to it by a business—to help avoid the privacy and security risks associated with requiring service providers to respond directly to consumers, with whom they generally lack a direct relationship.*

These changes will together help to ensure the business-service provider relationship established by the CCPA is not inadvertently altered by the draft regulations.

I. The Unique Role of Service Providers.

As enterprise software companies, BSA members develop and deliver the technology products and services on which other businesses rely. In this role, they generally act as service providers under the CCPA.² Service providers are critical in today's economy, as more companies across a range of industries become technology companies—and depend on service providers for the tools and services that fuel their growth. Software is the backbone of shipping and transportation logistics. It enables financial transactions all over the world. And it drives the growth of new technologies like artificial intelligence (“AI”), which have helped companies of all sizes enter new markets and compete on a global scale.

Businesses entrust some of their most sensitive data—including personal information—with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations. Indeed, many businesses depend on BSA members to help them better protect privacy. For example, our members offer cloud computing services that allow customers to compartmentalize datasets, which can prevent a breach in one location from impacting a full dataset. Other BSA members provide privacy-enhancing technologies that use, for example, data masking, which help companies to reduce the sensitivity of data they hold, and thereby reduce privacy and security threats.

II. The Difference Between “Businesses” and “Service Providers” Under the CCPA.

The CCPA recognizes the distinct role of service providers. While the statute focuses primarily on businesses, which “determine[] the purposes and means of the processing of consumers' personal information”³ it recognizes that businesses may engage service providers to

² Of course, when BSA members collect data for their own business purposes, they take on responsibility for complying with the provisions of the CCPA that apply to “businesses” that “determine[] the purposes and means of the processing of consumers' personal information.” For instance, a company that operates principally as a service provider will nonetheless be treated as a business when it collects data for the purposes of providing services directly to consumers. While these comments focus on issues relevant to service providers, we recognize there are a number of issues important to companies acting as “businesses” under the CCPA that are likewise important to BSA. Those include providing more clarity on how businesses can comply with requests to delete, including ensuring a reasonable timeline for deletion of personal information in backup systems, supporting use of security measures like multi-factor authentication in connection with user verification, and providing additional guidance on how businesses are to honor opt-out requests in connection with consumer browser plugins or privacy settings.

³ See Cal. Civil Code § 1798.140(d).

“process[] information on behalf of a business.”⁴ The CCPA requires service providers to enter into written contracts with businesses they serve, limiting how the service provider can retain, use, and disclose personal information provided to them by a business.⁵

The CCPA also assigns businesses and service providers different obligations, in line with their different roles in handling consumers’ data. Since businesses decide why and how to collect a consumer’s personal information, they must provide consumers certain rights, including the ability to opt-out of sales of their information. Businesses must therefore direct service providers to help implement certain rights, including the right to delete personal information.⁶ But service providers do not decide why a consumer’s information is collected or used. Rather, they process the personal information on behalf of a business, pursuant to their written contract.

Distinguishing between businesses and service providers is important from a privacy perspective, because adopting this type of role-based responsibility improves privacy protection. Indeed, the distinction is pervasive in the privacy ecosystem. For example, the EU’s General Data Protection Regulation (“GDPR”) applies to “controllers” that determine the means and purpose for which consumers’ data is collected (similar to businesses under the CCPA), and “processors” that process data on their behalf (similar to service providers under the CCPA). Voluntary frameworks that promote data privacy and cross-border transfers also reflect the distinct roles that different types of companies have in handling consumers’ data.⁷

III. The Draft Regulations Should be Clarified to Avoid Altering the Business-Service Provider Relationship Established in the CCPA.

The draft regulations should not be read to upset the business-service provider relationship created by the text of the CCPA. We encourage three revisions to avoid that result.

A. Service Providers’ Role in Processing Personal Information

Our first two recommendations focus on the portions of the draft regulations addressing how service providers process data provided to them by a business.

Text of Proposed Regulations. Section 999.314(c) states that a service provider “shall not use personal information received either from a person or entity it services or from a consumer’s direct interaction with the service provider for the purpose of providing services to another person or entity.” However, “[a] service provider may . . . combine personal information received from one or more entities . . . on behalf of such businesses, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.”

Negative Consequences of Reading Proposed Regulations Broadly. If this provision were read broadly, it would risk upsetting the business-service provider relationship created in the CCPA.

⁴ See Cal. Civil Code § 1798.140(v).

⁵ *Id.*

⁶ See Cal. Civil Code § 1798.105(d).

⁷ For example, privacy laws in Hong Kong, Malaysia, and Argentina distinguish between “data users” that control the collection or use of data and companies that only process data on behalf of others. In Mexico, the Philippines, and Switzerland, privacy laws adopt the “controller” and “processor” terminology. Likewise, the APEC Cross Border Privacy Rules, which the US Department of Commerce has strongly supported and promoted, apply only to controllers and are complemented by the APEC Privacy Recognition for Processors, which help companies that process data demonstrate adherence to privacy obligations and help controllers identify qualified and accountable processors.

Under the statute, if a business asks a service provider to use personal information to serve multiple businesses, or to combine that information with other data sets, the service provider is obligated to do so. The draft regulations should not be read so broadly to prevent that result.

If Section 999.314(c) were read to prevent these actions, it would have several negative consequences:

- *First*, it would risk placing new obligations on service providers that are inconsistent with their role under the CCPA. In particular, if the draft regulations were read to require a service provider to refuse to process data when a business specifically asks for the data to be provided to multiple businesses, it would effectively require the service provider to decide when it can and cannot process information. Yet the CCPA makes businesses—not service providers—responsible for those decisions.

By definition, a business “determines the purposes and means of the processing of consumers’ personal information.”⁸ Service providers have no such authority, which is fundamental to the distinction between businesses and service providers under the statute. Moreover, the CCPA prescribes specific contractual and other requirements that entities must observe if they wish to establish and maintain a business-service provider relationship.⁹ The draft regulations should not be read to upset this careful balance.

- *Second*, it would risk limiting the ability of businesses to combine information in ways that benefit consumers. Indeed, businesses may ask service providers to combine information with other data sets, or to serve multiple businesses, for a range of purposes that benefit consumers and support responsible innovation—without monetizing consumers’ data or using it for advertising. These include:
 - *Serving businesses that enter into a joint venture.* When two businesses want a service provider to act on their behalf, the CCPA allows the service provider to do so, as long as a written contract is in place. Similarly, a business may choose to engage two service providers, and direct them to share data on its behalf. The draft regulations should not be read to prohibit such arrangements.
 - *Providing and improving services.* Businesses may direct service providers to use personal information they disclose to the service provider to improve services offered to multiple businesses. For example, a service provider may use personal information provided by one business to improve an algorithm that powers a service provided to multiple businesses, even without combining the underlying data. Similarly, a business may direct a service provider to combine metadata that is personal information under the CCPA from its

⁸ See Cal. Civ. Code § 1798.140(c)(1).

⁹ See generally Cal. Civ. Code §§ 1798.140(v), (d) and (f) (defining “service provider,” “business purpose,” and “commercial purpose,” respectively). A broad reading of the draft regulations would limit the actions of service providers in new ways, not contained in the statutory text of CCPA. Even under the broadest grant of rulemaking authority in the CCPA, see Cal. Civ. Code § 1798.185(b), that broad reading of subdivision 999.314(c) would not “fill in the details” of the statutory scheme, See *Ford Dealers Ass’n v. Dep’t of Motor Vehicles*, 32 Cal. 3d 347, 362-63 (1982). The broad reading would also conflict with the CCPA’s consent requirements, which subjects certain actions to opt-out consent and others to opt-in consent. Reading subdivision 999.314(c) broadly to disallow these actions would also ignore the role of consent in the statutory scheme, and create a ban on processing to which no consent could be given.

- business and from other businesses to better provide a service, such as to prepare to handle peak traffic times across geographies.
- *Facilitating research.* Service providers can help entities conducting scientific research by combining multiple sets of data, at the direction of those entities and in line with privacy safeguards they have established. The resulting data could then be used to serve each of the participating entities.
 - *Providing benchmarking services to both consumers and businesses.* These services can provide context to a consumer or business seeking to understand how it fits into broader trends. For example, a consumer may want to opt-in to a program that allows her health care provider to use a service provider to combine her information with other data sets, to better understand potential health risk factors. While such a service would depend on the service provider's ability to combine several sets of personal information in order to identify those risk factors, it may limit the information shared with consumers to aggregated or de-identified information about how that consumer fits into these broader trends. Similarly, businesses may use benchmarking services to understand industry trends in hiring and human resources management, and to identify areas in which they may need to invest additional resources.
 - *Developing and testing AI systems.* AI systems are trained with large volumes of data. Their accuracy—and benefits—depend on access to large amounts of high-quality data, which service providers may process at the direction of businesses. For example, cities are optimizing medical emergency response processes using AI-based systems, enabling them to more strategically position personnel and reduce both response times and the overall number of emergency trips. The draft regulations should not prohibit service providers from using or combining information for such purposes, at the direction of a business.
 - *Supporting open data initiatives.* More broadly, there is increasing recognition among governments and companies of the benefits of sharing data—subject to appropriate privacy protections. For example, in January the United States enacted the OPEN Government Data Act, which makes non-sensitive government data more readily available so that they can be leveraged to improve the delivery of public services and enhance the development of AI.¹⁰ Companies have also supported voluntary information-sharing arrangements, including seeking to develop common terms so that companies that want to share data can more readily do so.¹¹

Proposed Revision to Regulations. To ensure the draft regulations are not read so broadly as to prohibit service providers from processing personal information at the direction of and on behalf of businesses—we suggest adding the italicized language to Section 999.314(c):

"A service provider shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for

¹⁰ See Public Law No. 115-435, Title II (Jan. 14, 2019).

¹¹ See Microsoft, The Open Use of Data Agreement, available at <https://github.com/microsoft/Open-Use-of-Data-Agreement>; The Linux Foundation Projects, Community Data License Agreement, available at <https://cdla.io/>.

the purpose of providing services to another person or entity, *except at the direction and on behalf of the business providing the personal information*. A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity, or for purposes compatible with providing the services.”

B. Role of Service Providers in Responding to Consumer Requests

Our third recommendation addresses the role service providers play in responding to consumer requests under the CCPA.

Text of Proposed Regulations. Section 999.314(d) states: “If a service provider receives a request to know or a request to delete from a consumer regarding personal information that the service provider collects, maintains, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial. The service provider shall also inform the consumer that it should submit the request directly to the business on whose behalf the service provider processes the information and, when feasible, provide the consumer with contact information for that business.”

Negative Consequences of Proposed Regulations. This provision also risks upsetting the business-service provider relationship established in the CCPA. In particular, Section 999.314(d) could be read to require service providers to evaluate and respond to consumer requests to know or delete personal information—an obligation not placed on them by the CCPA.

Under the text of the CCPA, service providers merely play a supporting role in executing deletion requests on behalf of businesses.¹² Notably, the statute requires *businesses* to delete personal information pursuant to a verifiable consumer request and to “direct any service providers” to do the same.¹³ The statute thus anticipates that service providers act *at the direction of businesses*—and not at the direction of consumers, with whom they lack a direct relationship. The connection between right to know requests and service providers is even more attenuated; the text of the law does not refer explicitly to service providers in connection with the right to know.¹⁴ As a result, “neither the CCPA nor the regulations require service providers to comply with such requests.”¹⁵

This arrangement is for good reason. Requiring service providers to respond directly to consumer requests invites a host of security and privacy risks, which arise because service providers generally do not interact with consumers. In the ordinary course, a service provider may not maintain information about the consumers its business customers serve—and thus would not ordinarily review records containing their names, services provided, or other information needed to respond to a request. Service providers should not be encouraged to seek out that information, if they would not otherwise have access to it. For example, a service provider that works with multiple businesses may not be able to identify the business relevant to a consumer’s request without combing through personal information it provides on a host of businesses, to identify the relevant one. That result should be avoided, because it would invade consumers’ privacy, not protect it. Likewise, service providers may not have sufficient

¹² See Cal. Civ. Code §§ 1798.105(c), (d).

¹³ See Cal. Civ. Code § 1798.105(c).

¹⁴ See generally Cal. Civ. Code §§ 1798.100 and 1798.110.

¹⁵ *Initial Statement of Reasons*, at 22-23.

information to verify a consumer's request, and thus could create security risks in responding directly to a consumer without verifying her identity.

Instead, the CCPA recognizes that businesses should respond to consumer requests—since they have the most complete understanding of what data they control about a particular consumer. Section 999.314(d) should be revised to ensure it does not alter this process.

Proposed Revision. We suggest revising Section 999.314(d) to more clearly reflect the existing statutory scheme, by deleting the language in strikethrough below and adding the language in italics.

~~"If a service provider receives a request to know or a request to delete from a consumer regarding personal information that the service provider collects, maintains, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial. The service provider shall also~~ *then the service provider shall* inform the consumer that it should submit the request directly to the business ~~on whose behalf the service provider processes the information, and when feasible, provide the consumer with contact information for that business.~~ *with which the consumer interacted."*

* * *

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

Sincerely,



Kate Goodloe
Director, Policy
BSA | The Software Alliance

Message

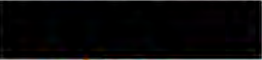
From: Moises Rosales [REDACTED]
Sent: 12/7/2019 12:31:27 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Anna Buck [REDACTED]
Subject: C.A.R.'s Comments on the Proposed CCPA Regulations
Attachments: C.A.R. - Comments on Proposed CCPA Regulations.pdf
Importance: High

To Whom It May Concern,

Attached please find C.A.R.'s comments on the proposed CCPA regulations.

Thank you.

MOISES ROSALES
ADMINISTRATIVE ASSISTANT
CALIFORNIA ASSOCIATION OF REALTORS®
1121 L STREET, SUITE 600
SACRAMENTO, CA 95814



Help your clients keep their homes & insurance coverage.
[Download the shareable materials today!](#)



CALIFORNIA ASSOCIATION OF REALTORS®

December 6, 2019

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

RE: California Consumer Privacy Act Proposed Regulations

Dear Attorney General Becerra:

Thank you for the opportunity to provide comments regarding the proposed California Consumer Privacy Act (CCPA) regulations. The California Association of REALTORS® (C.A.R.) seeks to be a valuable contributor in the development of these regulations so that the uniqueness of the real estate industry, and specifically the real estate transaction process, is considered. We also feel it is critical that the regulatory scheme consider some of the issues unique to our trade and we hope we can be of assistance to those working to craft the regulations associated with this landmark law.

Business practices for handling requests made pursuant to the CCPA

In the real estate industry, information held in the aggregate can nonetheless prove incredibly useful for both the principals and the professionals engaged in the homebuying and selling process. According to the proposed regulations, requests for deletion may be completed by deidentifying or aggregating the consumer's personal information ("PI"). It would be useful to our industry if more guidance was given on what steps should be taken to properly deidentify or aggregate information in order to properly comply with this part of the law.

Furthermore, another area of concern to the real estate industry is the fact that real estate transactions involve at a minimum two separate and unrelated households and the documents related to the transactions include PI of multiple consumers; at the least, documents will have PI of both the buyer and the seller, and in many cases may have PI of multiple consumers on the buyer and seller side respectively. It is feasible that a CCPA business by responding to one consumer's request could negatively impact another consumer's CCPA rights or require more burdensome compliance for the business. For example, in the real estate context a buyer might request disclosure from a REALTOR® that could require the disclosure of PI that also qualifies as the seller's PI. Similarly, a seller may request deletion of PI that also qualifies as a buyer's PI where the buyer wishes the REALTOR® business to continue to retain the PI. Additional guidance on how to properly process and respond to requests for information that involve multiple unrelated households and/or consumers would be helpful.



REALTOR® is a federally registered collective membership mark which identifies a real estate professional who is a Member of the NATIONAL ASSOCIATION OF REALTORS® and subscribes to its strict Code of Ethics.



Personal Information of Minors

Real estate transactions are likely to deal with the PI of families, which may very well include minors. Under the current law, if a business has actual knowledge that a minor's PI is collected, there needs to be an opt-in. Moreover, under CCPA as currently drafted, there is no scope for an implied opt-in, such as when two parents of minors provide their own PI to a REALTOR® in the course of a real estate transaction where the parents' PI also qualifies as the PI of the minors. Thus, when a business collects the parents' PI that would also qualify as their children's PI, like the family of two parents and their minor children suggested above, does the presence of minors subject all of the PI to opt-in requirements, both as household PI and as individual PI that relates to both adult and children? This would seem to pose an unintended but nevertheless unduly burdensome impact on business; therefore, we would request further guidance on how to handle this common scenario.

Anti-Discrimination

Under the CCPA, businesses may not discriminate against consumers for exercising their rights under the law. This is a laudable goal and in line with our State's long history of leading the way with regard to ensuring that all Californians are treated equally in the eyes of the law. However, there are circumstances under which the exercise of a CCPA right unavoidably will lead to a different level of service.

For example, one of the many benefits of listing a property with a licensed real estate agent or broker is that the property is listed on the Multiple Listing Service ("MLS") after a listing agreement is signed. If a consumer exercises his or right to opt out of any sharing of PI, the listing either cannot be completed or will be incomplete. Our industry currently gives consumers the right to do so irrespective of the CCPA, but we warn that this can restrict the ability of a listing agent to effectively market the seller's property and could mean a seller doesn't receive as high a sales price as if they had listed on the MLS. But under the CCPA, a consumer could complain that they were discriminated against for exercising their opt-out rights to not have their PI shared with the MLS, resulting in a lower sales price, despite the clear warnings that our members give as industry-standard. The regulations should be clarified so that not providing a service that cannot be offered due to the exercise of a CCPA right is not considered discriminatory.

Conclusion

C.A.R. thanks the Office of the Attorney General for their work on these regulations and looks forward to a collaborative relationship in building a regulatory framework that both protects consumer privacy and ensures that the real estate market continues to function in a healthy manner. If you or a member of your staff have any questions or comments, please do not hesitate to contact me at [REDACTED] or [REDACTED]

Sincerely,



Anna Buck
Legislative Advocate

Message

From: Andre Cotten [REDACTED]
Sent: 12/6/2019 8:51:06 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: CA AG NPR concerning the CCPA: Consumer Bankers Association Comment
Attachments: California AG NPR concerning the CCPA - Consumer Bankers Comment .pdf

Hi—

Please find the Consumer Bankers Association's comment attached.

Best,

ANDRE' B. COTTEN, ESQ.

Assistant Vice President, Regulatory Counsel
Consumer Bankers Association
1225 Eye Street, NW, #550 | Washington, DC 20005
[REDACTED]

***CBA LIVE 2020**

San Diego, CA | March 23-25



December 6, 2019

VIA ELECTRONIC SUBMISSION

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

Re: Notice of Proposed Rulemaking Regarding the California Consumer Privacy Act

Dear Mr. Becerra:

The Consumer Bankers Association¹ (“CBA” or “the Association”) appreciates the opportunity to offer our views on the California Attorney General’s (“the Attorney General” or “the AG”) Notice of Proposed Rulemaking (the “Proposed Rule” or the “Draft Regulations”) concerning California’s regulatory approach to the California Consumer Privacy Act (the “Act” or “the CCPA”).

CBA appreciates the Attorney General’s efforts to provide guidance to businesses on how to comply with the CCPA and to clarify the Act’s requirements through proposed regulations. Most importantly, CBA’s member banks share the Attorney General’s goal of protecting the privacy of consumers. However, we have significant concerns about the proposed regulations as drafted by the Attorney General. Below, we have identified our most pressing issues and offered the Attorney General solutions to consider in the next phase of the rule writing process.

I. The Attorney General’s Right to Opt-Out of Sale Guidance is Insufficient to Address Practical Business Concerns.

CBA urges the Attorney General to provide more certainty about the right to opt-out of sales of personal information. From a review of the draft regulations, it seems a bank, or any covered entity, may present the choice to opt-out of certain sales, so long as a global option to opt-out of the sale of all personal information is more prominently presented than other choices. Note, this option assumes a global option is feasible. From a practical perspective, it is likely a business may possess varying data elements about a single consumer through different relationships with the consumer, which may not be linked.

Moreover, the proposed regulations require a bank, or covered entity, which collects personal information from consumers online to “treat user-enabled privacy controls, such as browser plugin or privacy setting or another mechanism, which communicates or signal the consumer’s choice to opt-out of

¹ The Consumer Bankers Association is the only national trade association focused exclusively on retail banking. Established in 1919, the Association is now a leading voice in the banking industry and Washington, representing members who employ nearly two million Americans, extend roughly \$3 trillion in consumer loans, and provide \$270 billion in small business loans.

the sale as a valid request” to opt-out of sale of personal information “for that browser or device, or, if known, for that consumer.” This raises a number of operational complexities and issues since neither the statute nor the proposed regulations condition this opt-out method being a well-established or widely used standard to communicate requests to opt out of sale of personal information.

II. Provide Covered Entities with a Safe Harbor When Verifying Consumer Requests.

The CCPA establishes a series of rights which are contingent upon the receipt and authentication of a “verifiable consumer request.” In order to comply with a consumer’s request to exercise his or her rights under the CCPA, the “business shall promptly take steps to determine whether the request is a verifiable consumer request.”

CBA appreciates the Attorney General for providing helpful guidance related to verification requests. Generally, the proposed regulations direct banks to use a more rigorous verification process when dealing with more sensitive information. The proposed regulations also take it a step further by directing banks not to release sensitive information without being highly certain about the identity of the individual requesting the information. The proposed regulations also provide prescriptive steps of what to do in cases where an identity cannot be verified.

As the Attorney General is aware, banks collect personal information as part of routine transactions to facilitate consumer requests. Even with the proposed rules, furnishing personal information to customers purporting to exercise their rights under the CCPA, in response to a verifiable consumer request, may result in unintended risk and harm to the consumer, including misuse of personal information to perpetuate fraud and identity theft. As a potential solution, the Attorney General should establish a safe harbor from liability to assure banks, and other covered entities, that rejecting a suspicious right of access request in good faith will not later result in a violation.

Moreover, CBA implores the Attorney General to look to the implementation issues encountered by the General Data Protection Regulation (GDPR) in its next stage of rule writing. According to a study published by Blackhat USA 2019 (“the Study”)², the Study demonstrates how legal ambiguity surrounding the “right of access” process may be used by social engineers to facilitate fraud. The Study’s experimental findings also demonstrate many organizations fail to adequately verify the originating identity of right of access requests. As a result, social engineers can abuse right of access requests as a scalable attack mechanism for acquiring deeply sensitive information about individuals.

The Attorney General’s proposed regulations do not seem to consider the prevalence and petulance of social engineers. Without a safe harbor from liability, banks may be hesitant to reject the legitimacy of consumer requests for fear of potential enforcement actions. Thus, the Attorney General’s oversight would allow more potential gateways for social engineers to exploit legal and policy loopholes.

As the CCPA is set to apply to various industries, CBA also encourages the Attorney General to better consider a business’ size and complexity, the nature and scope of its business activities, and the sensitivity of any personal information at issue. In alternative, the Attorney General may consider

² <https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf>

utilizing principles such as those found in existing authentication guidance issued by the Federal Financial Institutions Examination Council.

III. The CCPA as Proposed is Potentially Harmful for Consumers' Information.

Building on the previous discussion, CBA encourages the Attorney General to finalize a rule which does not put consumers at any additional risk of fraud or identity theft. The proposed regulations impose new disclosure obligations beyond those enumerated in the statute.

In particular, the proposed disclosures require banks, and other covered entities, to specify a potentially concerning level of detail about certain privacy practices. For example, the draft would require a business to address the following new disclosures:

- Describe the process the bank will use to verify the consumer request, including any information the consumer must provide;
- Explain how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf; and
- For each category of personal information collected, provide the categories of sources from which the information was collected, the business or commercial purposes(s) for which the information was collected, and the categories of third parties with whom the business shares personal information.

As previously mentioned, banks are constantly having to safeguard and mitigate against potential and real fraud. The CCPA as proposed seems to be another apparent path for fraudsters to attempt to infiltrate the banking system and harm real consumers.

IV. The CCPA Should Protect the Intellectual Property Rights of Covered Entities.

As the proposed rules are currently written, CBA believes the CCPA may infringe on the intellectual property rights of our member banks. Pursuant to § 1798.185(a)(3), the CCPA grants the Attorney General 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."

Furthermore, we urge the Attorney General to include a rule to establish an exception from the CCPA for intellectual property or for data which, if disclosed, would have an adverse effect on the rights or freedoms of others. The CCPA should not apply to information which is protected intellectual property of a bank, or any other covered entity, including information subject to copyright, patent, service mark and/or trade secret protections. A bank also should be required to disclose any information which is subject to intellectual property protections, including any formula, pattern, compilation, program, device, method, technique or process developed to process or analyze personal information, or any information derived from such process or analysis.

The Attorney General should consider duplicating the EU's GDPR approach to intellectual property. The GDPR places reasonable limitations on its enumerated consumer privacy rights. It provides both an intellectual property exclusion and the avoidance of infringement on the rights of others. CBA believes its

member banks, and other covered entities, deserve the same protections if a bank is presented with a scenario where its attempt to comply with a consumer's request may put it in the position of violating the rights of others or placing it in jeopardy with its competitors.

V. The Definition of "Sell" is too Broad and Unnecessarily Burdensome.

The CCPA includes definition for "sell" as follows:

"(t)(1) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration. (2) For purposes of this title, a business does not sell personal information when: (A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party. (B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.

(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met: (i) The business has provided notice that information being used or shared in its terms and conditions consistent with § 1798.135. (ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose. (D) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with § 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with § 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with § 17200) of Part 2 of Division 7 of the Business and Professions Code)."

CBA urges the Attorney General to provide more clarification about the covered activities in its definition of "sell." The definition as written is too general and too open-ended. There are a myriad of activities which would possibly fall within the CCPA's current definition of sale, which see beyond the scope of the law's actual public policy concerns. For example, cookies embedded on a bank's website could currently be construed to be covered under the current definition of "sell." As an additional practical complexity posed by the CCPA, it is also unclear how a bank's interactions with the Google

search engine or via an ad placed on Facebook would be treated under the current definition. There is also a lack of clarity about what constitutes valuable consideration under the CCPA.

Note, banks, and other covered financial institutions, are also unsure about the scope of the CCPA's Gramm-Leach-Bliley exception. The Attorney General should draft rules to provided banks, and other covered entities, with the clarity needed to comply with this comprehensive privacy law.

VI. Transfers of Personal Information to Service Providers is Not a Sale.

Banks, and other financial institutions, transfer personal information to service providers to maximize the consumer experience by providing products and services. These transfers are not sales as contemplated in the CCPA, and the final regulations should clarify this distinction for service providers. Section 999.314 proposes a covered entity which otherwise meets the definition of a service provider is a service provider even if it collects personal information directly from consumers at the request of a business.

Note, the proposed rules also state a service provider which also meets the definition of a business must comply with the CCPA for any personal information it collects or sells outside of its role as a service provider. CBA supports this proposed clarification regarding service providers, and we urge the Attorney General to consider further clarifications. A final rule with additional clarity is essential to ensure banks, and other financial institutions, can transfer personal information to a service provider to benefit the bank's customers without the transfer being deemed a sale of personal information pursuant to the CCPA.

VII. Provide More Clarity Concerning the "Right to Cure."

Section 1798.155(b) states, in part, a "[bank] shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance." To begin, the Attorney General's regulations did not propose any rules to codify this provision of the CCPA. CBA urges the Attorney General to establish specific criteria for what is necessary in order for a bank, or other covered entity, to successfully "cure" a violation.

The Attorney General should provide more detailed guidance. For example, there may be a circumstance where a cure cannot unwind the effects of a violation, guidance is needed as to other means in which the bank, other covered entity, could cure, or mitigate against, the violation through implementation of enhanced business practices.

VIII. The "Lookback" Period Should Begin January 1, 2020.

As the proposed rules are currently written, the CCPA appears to apply retroactively by requiring businesses to provide information subject to a consumer's request covering the time period prior to the Act's effective date and prior to the publication of implementing regulations. CBA believes rulemaking should clarify the 12-month lookback period provided for in § 1798.130 applies from the effective date of

the CCPA, which is January 1, 2020. This change would preclude its application to activities occurring prior to the effective date.

IX. Establish an Effective Date for Final Rules to Allow Covered Entities Adequate Time to Comply.

The Attorney General should exercise its discretionary authority to set an effective date of 18 months after the final rules are issued. CBA believes this extension is essential so banks, and other covered entities, can properly comply. Banks will need sufficient time to review and implement direction from the Attorney General's final regulations, which may require changes to implementation plans which were based in good faith on the statutory language, prior to regulations being adopted.

For example, the final regulations will require banks, and other covered entities, to change their verification processes due to the CCPA's prescriptive requirements, e.g. "double" authentication for deletion, declaration signed under penalty of perjury, etc. These potential changes and clarifications will require development work, testing and validation, and employee training. Truncating these necessary steps into a potentially short time frame, e.g. 1 month, may create the undue operation risk of either not properly verifying a valid request or disclosing information to the incorrect person. These types of risks are anti-consumer and preventable.

Currently, the CCPA's deadline for the Attorney General's rulemaking is July 1, 2020, six months after the law's January 1 effective date. Pursuant to the CCPA, the Attorney General could technically begin enforcement of the CCPA on July 1, 2020, which is the same day the final rules could be published. This would be an unreasonable request for covered entities. CBA supports the goal of consumer privacy protection, however, the CCPA is complex and in part, unclear. Banks, and other covered entities, will need sufficient time to come into full compliance to ensure they implement the full privacy protections as intended by the legislature to ultimately benefit consumers.

X. Establish an Enforcement Date of No Earlier than July 1, 2020.

CBA urges the Attorney General to preclude any enforcement action based on conduct or omission occurring on or after the enforcement date. The CCPA provides in §1798.185(c), the "Attorney General shall not bring an enforcement action under this title until six months after the publication of the final rule issued pursuant to this section or July 1, 2020, whichever is sooner." For example, if the enforcement date is July 1, 2020, because it is earlier than the six-month anniversary of final regulations, the AG should clarify any enforcement will be based only on conduct or omissions occurring July 1, 2020 or later and not conduct or omissions occurring on or after the CCPA effective date, January 1, 2020.

CBA appreciates the opportunity to comment on the Notice of Proposed Rulemaking, and we plan to continue to engage the California Office of the Attorney General as the rulemaking process continues and to ensure our member banks have the necessary guidance to comply with the tenants of the final rule. Please feel free to contact André Cotten for further discussion regarding our comments at

██████████ or ██████████

Sincerely,

A handwritten signature in cursive script, appearing to read "Andre B. Cotte".

Assistant Vice President, Regulatory Counsel
Consumer Bankers Association

Message

From: Von Borstel, Megan (Perkins Coie) [REDACTED]
Sent: 12/7/2019 12:42:24 AM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
CC: Shelton Leipzig, Dominique (Perkins Coie) [REDACTED]
Subject: California Chamber Comments Regarding AG's Proposed CCPA Regulations
Attachments: California Chamber of Commerce Comments Regarding Attorney General's Proposed CCPA Regulations December 6 2019.pdf

Office of the Attorney General: Privacy Unit,

On behalf of the California Chamber of Commerce, we wish to thank the Office of the Attorney General for the opportunity to make comments to the Attorney General's draft regulations for the CCPA. Attached are the California Chamber's comments, titled "California Chamber of Commerce Comments Regarding Attorney General's Proposed CCPA Regulations December 6, 2019." Please do not hesitate to contact me with any questions.

Thank you,

Dominique Shelton Leipzig | Perkins Coie LLP
PARTNER PRIVACY & SECURITY
CO-CHAIR AD TECH PRIVACY & DATA MANAGEMENT
1888 Century Park East Suite 1700
Los Angeles, CA 90067-1721
[REDACTED]

Megan Von Borstel | Perkins Coie LLP
ASSOCIATE | she/her/hers
131 S. Dearborn Street Suite 1700
Chicago, IL 60603-5559
[REDACTED]

NOTICE: This communication may contain privileged or other confidential information. If you have received it in error, please advise the sender by reply email and immediately delete the message and any attachments without copying or disclosing the contents. Thank you.



California Chamber of Commerce Comments Regarding Attorney General’s Proposed CCPA Regulations December 6, 2019

JENNIFER BARRERA

EXECUTIVE VICE PRESIDENT



DOMINIQUE SHELTON LEIPZIG

PARTNER



MEGAN VON BORSTEL

ASSOCIATE



Executive Summary

The California Chamber of Commerce (“CalChamber”) submits the comments herein to the California Attorney General’s (“AG”) office regarding the AG’s proposed regulations for the California Consumer Privacy Act (“CCPA”).

Each comment is presented separately in three parts: (a) the header which identifies the proposed regulation; (b) issue headers that synthesize the issue or concern with the proposed regulation; and (c) subparts that identify (i) the proposed regulation, (ii) problem with proposed regulation, and (iii) recommended change(s) in the language to solve or mitigate CalChamber’s related concern(s). Specific language is proposed in Exhibit “A” in a redlined version of the proposed regulations.

As indicated in Exhibit A, we request that the enforcement date of the regulations be delayed until January 1, 2021 to allow time for companies to update their practices to comply. Companies have already spent millions to update their practices for the CCPA itself. It would be burdensome, costly, and in some instances, impossible to change administrative and technical processes for regulations that are not yet final.

As individual groups are raising a variety of discrete issues with the proposed regulations, this is not a collectively exhaustive list; rather, this report is intended to reflect key issues for the CalChamber at large.

JENNIFER BARRERA

EXECUTIVE VICE PRESIDENT



DOMINIQUE SHELTON LEIPZIG

PARTNER



MEGAN VON BORSTEL

ASSOCIATE



Biographies



JENNIFER BARRERA | EXECUTIVE VICE PRESIDENT | CAL CHAMBER

<https://advocacy.calchamber.com/bios/jennifer-barrera>

Jennifer Barrera oversees the development and implementation of policy and strategy as executive vice president and represents the California Chamber of Commerce on legal reform issues.

She led CalChamber advocacy on labor and employment and taxation from September 2010 through the end of 2017. As senior policy advocate in 2017, Barrera worked with the executive vice president in developing policy strategy. She was named senior vice president, policy, for 2018 and promoted to executive vice president as of January 1, 2019.

In addition, she advises the business compliance activities of the CalChamber on interpreting changes in employment law.

From May 2003 until joining the CalChamber staff, she worked at a statewide law firm that specializes in labor/employment defense, now Carothers, DiSane & Freudenberger, LLP. She represented employers in both state and federal court on a variety of issues, including wage and hour disputes, discrimination, harassment, retaliation, breach of contract, and wrongful termination.

She also advised both small and large businesses on compliance issues, presented seminars on various employment-related topics, and regularly authored articles in human resources publications.

Barrera earned a B.A. in English from California State University, Bakersfield, and a J.D. with high honors from California Western School of Law.



DOMINIQUE SHELTON LEIPZIG | PARTNER | LOS ANGELES, CA

www.perkinscoie.com/DSheltonLeipzig/

Privacy and cybersecurity attorney Dominique Shelton co-chairs the firm's Ad Tech Privacy & Data Management group. She provides strategic privacy and cyber-preparedness compliance counseling, and defends, counsels and represents companies on privacy, global data security compliance, data breaches and investigations with an eye towards helping clients avoid litigation. Dominique frequently conducts trainings for senior leadership, corporate boards and audit committees regarding risk identification and mitigation in the areas of privacy and cyber.

She leads companies in legal assessments of privacy, data security, cyber preparedness and compliance with such regulations as the California Consumer Protection Act (CCPA), California Confidentiality of Medical Information Act (CMIA), the Video Privacy Protection Act (VPPA), the Children's Online Privacy Protection Act (COPPA) and the NIST Cybersecurity Framework.

Dominique has significant experience leading investigations related to data and forensic breaches. She has steered investigations for a range of companies, including for national retailers, financial institutions, health and wellness enterprises, media companies and others.

Dominique also advises companies on global privacy and data security, particularly on EU General Data Protection Regulation (GDPR). Her background includes advising on European, Asian and South American privacy and security compliance projects for U.S.-based and overseas companies. In addition, she counsels on strategies for related legal compliance and vendor management in cross-border transfers.

Dominique is the author of two books titled *Implementing the CCPA- a Global Guide for Business* (Sept. 2019, IAPP); and *Transform* (Mar. 2019)



MEGAN VON BORSTEL | ASSOCIATE | CHICAGO, IL

www.perkinscoie.com/megan-von-borstel

Megan Von Borstel has experience with privacy counseling and data breach response. She counsels clients on compliance efforts with state, federal, and international privacy laws and regulations, including the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). Megan is also familiar with the Stored Communications Act, the Biometric Information Protection Act, and various other state and federal statutes.

Megan earned her J.D. at Washington University School of Law, where she served as editor-in-chief for the *Washington University Jurisprudence Review*, received the Judge Amandus Brackman Moot Court Award, and volunteered at the law school's appellate and children's rights clinics. Megan also served as a judicial extern for the Honorable Shirley Padmore Mensah, U.S. Magistrate Judge for the U.S. District Court of Eastern Missouri.

TABLE OF CONTENTS

	Page
I. SECTION 999.315 REQUESTS TO OPT-OUT—CHAMBER PROPOSED CHANGES.....	1
A. ISSUE: BUSINESSES NEED THE OPTION NOT TO TREAT BROWSER PLUG-INS OR SETTINGS AS OPT-OUT REQUESTS, AND INSTEAD HAVE THE CHOICE TO PROVIDE AN OPT-OUT BUTTON.	1
1. Proposed Regulation: 999.315(c); 999.315(g).....	1
2. Problem with Proposed Regulation:	1
3. Recommended Change:	1
B. ISSUE: PROPOSED REGULATIONS GIVE BROWSERS SIGNIFICANT DISCRETION TO EXERCISE AGAINST BUSINESSES THAT BROWSERS MAY BE IN COMPETITION WITH AND WHOSE “SALES” THEY ARE BLOCKING.	1
1. Proposed Regulation: §999.315(a); 999.315(c).....	1
2. Problem with Proposed Regulation:	1
3. Recommended Change:	2
C. ISSUE: PROPOSED REGULATION’S REQUIREMENT TO SHARE OPT-OUT REQUESTS WITH THIRD PARTIES EXCEEDS STATUTORY REQUIREMENTS.....	2
1. Proposed Regulation: §999.315(f).....	2
2. Problem with Proposed Regulation:	2
3. Recommended Change:	3
D. ISSUE: VERIFICATION OR AUTHENTICATION OF CONSUMERS SUBMITTING OPT-OUT REQUESTS SHOULD NOT BE PREVENTED OR LIMITED.	3
1. Proposed Regulation: §999.315(h)	3
2. Problem with Proposed Regulation:	3
3. Recommended Change:	3
E. ISSUE: RESPONSE TO REQUEST TO OPT-OUT ONLY SHOULD APPLY TO BUSINESS THAT SELL PERSONAL INFORMATION AND MORE TIME TO RESPOND IS NECESSARY.....	3
1. Proposed Regulation: §§999.315(d); 999.315(e).....	3
2. Problem with Proposed Regulation:	3
3. Recommended Change:	3

TABLE OF CONTENTS

(continued)

	Page
II. SECTION 999.307 NOTICE OF FINANCIAL INCENTIVE–CHAMBER PROPOSED CHANGES	4
A. ISSUE: DATA DOES NOT HAVE INDEPENDENT VALUE	4
1. Proposed Regulation: §999.307; 999.337	4
2. Problem with Proposed Regulation:	4
3. Recommended Change:	4
B. ISSUE: REGULATION CREATES ONEROUS DISCLOSURE REQUIREMENTS	4
1. Proposed Regulation: §999.307(a); 999.307(a)(3); 999.307(b)(2); 999.307(b)(5)	4
2. Problem with Proposed Regulation:	4
3. Recommended Change:	4
III. SECTION 999.313 RESPONDING TO REQUESTS TO KNOW AND REQUESTS TO DELETE–CHAMBER PROPOSED CHANGES	5
A. ISSUE: UNVERIFIABLE REQUESTS TO DELETE SHOULD NOT BE REQUIRED TO BE TREATED AS OPT-OUTS BECAUSE IT CHANGES THE CONSUMER’S INTENT, INCREASES COSTS, AND EXACERBATES DIFFICULTIES WITH DELETING DATA FROM ARCHIVES OR BACKUPS	5
1. Proposed Regulation: §999.313(d)	5
2. Problem with Proposed Regulation:	5
3. Recommended Change:	6
B. ISSUE: ENSURE BUSINESSES HAVE ENOUGH TIME AND FLEXIBILITY TO RESPOND TO REQUESTS UNDER STATUTORY TIMEFRAME	7
1. Proposed Regulation: §999.313(a); 999.313(b)	7
2. Problem with Proposed Regulation:	7
3. Recommended Change:	7
C. ISSUE: PROPOSED REGULATION REQUIREMENTS HEIGHTEN BURDENS ON BUSINESS AND EXCEED STATUTORY LANGUAGE	7
1. Proposed Regulation: §999.313	7
2. Problem with Proposed Regulation:	7
3. Recommended Change:	8

TABLE OF CONTENTS

(continued)

	Page
D. ISSUE: REGULATION SHOULD CLARIFY THAT A BUSINESS’S OBLIGATION TO COMPLY WITH A CONSUMER REQUEST IS LIMITED TO ITS ABILITY TO IDENTIFY RESPONSIVE MATERIALS USING COMMERCIALY REASONABLE EFFORTS.	8
1. Proposed Regulation: §999.313(c); 999.313(d).....	8
2. Problem with Proposed Regulation:	8
3. Recommended Change:	9
E. ISSUE: REGULATION SHOULD CONSIDER HOW RESPONDING TO REQUESTS COULD JEOPARDIZE OTHER CUSTOMERS’ SECURITY AS WELL.....	9
1. Proposed Regulation: §999.313(c)(3); <i>see also</i> 999.313(d); 999.323.....	9
2. Problem with Proposed Regulation:	9
3. Recommended Change:	9
F. ISSUE: REGULATION DOES NOT ADDRESS REQUESTS SEEKING PORTABILITY OF INFORMATION WHERE DISCLOSURE OF CONSUMER’S PERSONAL INFORMATION IS NECESSARY TO SUPPORT PORTABILITY.....	9
1. Proposed Regulation: §999.313(c)(4).....	9
2. Problem with Proposed Regulation:	9
3. Recommended Change:	9
G. ISSUE: NOTIFYING CONSUMER OF REASON FOR REQUEST DENIAL MAY INTERFERE WITH LAW ENFORCEMENT INVESTIGATION, HINDER BUSINESS OPERATIONS, AND IS CONTRARY TO THE PURPOSE OF AN EXEMPTION.....	10
1. Proposed Regulation: §999.313(c)(5).....	10
2. Problem with Proposed Regulation:	10
3. Recommended Change:	10
H. ISSUE: INDIVIDUALIZED RESPONSES TO CATEGORIES OF SOURCES OR THIRD PARTIES IS TOO BURDENSOME FOR BUSINESSES.....	10
1. Proposed Regulation: §999.313(c)(9)-(10).....	10
2. Problem with Proposed Regulation:	10
3. Recommended Change:	11

TABLE OF CONTENTS

(continued)

	Page
IV. SECTION 999.314 SERVICE PROVIDERS–CHAMBER PROPOSED CHANGES.....	11
A. ISSUE: PROPOSED REGULATIONS’ LIMITATIONS ON SERVICE PROVIDERS’ PERMISSIBLE USES OF DATA CONTRADICTS THE STATUTORY DEFINITION OF “BUSINESS PURPOSE” AND “SERVICE PROVIDER.”	11
1. Proposed Regulation: §999.314(c).....	11
2. Problems with Proposed Regulation:.....	11
3. Recommended Change:	12
B. ISSUE: PROPOSED REGULATION CREATES ADDITIONAL BURDENS FOR BUSINESS THAT EXCEED STATUTORY LANGUAGE.	12
1. Proposed Regulation: §999.314(d)	12
2. Problem with Proposed Regulation:	12
3. Recommended Change:	13
V. SECTION 999.301 DEFINITIONS–CHAMBER PROPOSED CHANGES.....	13
A. ISSUE: DEFINITION OF RIGHT TO KNOW CONFLICTS WITH REQUIREMENTS FOR HOW TO RESPOND TO RIGHT TO KNOW.	13
1. Proposed Regulation: §§999.301(n); 999.313(c)(10)	13
2. Problem with Proposed Regulation:	13
3. Recommended Change:	13
B. ISSUE: DEFINITION OF RIGHT TO KNOW CREATES INFEASIBLE REQUIREMENTS FOR RESPONDING TO INDIVIDUAL CONSUMER REQUESTS.	13
1. Proposed Regulation: §999.301(n).	13
2. Problem with Proposed Regulation:	13
3. Recommended Change:	13
C. THE SCOPE OF THE DEFINITION OF “PRICE OR SERVICE DIFFERENCE” COULD PREVENT BUSINESS WITH SERVICE PROVIDERS.	14
1. Proposed Regulation: §999.301(l)	14
2. Problem with Proposed Regulation:	14
3. Recommended Change:	14

TABLE OF CONTENTS

(continued)

	Page
D. ISSUE: DEFINITION OF “AFFIRMATIVE AUTHORIZATION” REQUIREMENT FOR TWO-STEP PROCESS TO OPT-IN IS OVERLY BURDENSOME FOR CONSUMERS AND BUSINESS.	14
1. Proposed Regulation: §999.301(a).....	14
2. Problem with Proposed Regulation:	14
3. Recommended Change:	14
E. ISSUE: PROPOSED REGULATIONS NEED TO PROVIDE CLARIFICATION REGARDING DEFINITION OF DIRECT NOTICE TO CONSUMERS.....	14
1. Proposed Regulation: §999.301; <i>see also</i> §§999.305(a)(3); 999.305(d)(1); 999.306(d)(2).....	14
2. Problem with Proposed Regulation:	14
3. Recommended Change:	14
VI. SECTION 999.300 TITLE AND SCOPE—CHAMBER PROPOSED CHANGES	15
A. ISSUE: THE REGULATIONS SHOULD CLARIFY THE CCPA’S JURISDICTIONAL SCOPE AND EFFECTIVE DATE.	15
1. Proposed Regulation: §999.300.....	15
2. Problem with Proposed Regulation:	15
3. Recommended Change:	15
VII. SECTION 999.305 NOTICE AT COLLECTION OF PERSONAL INFORMATION—CHAMBER PROPOSED CHANGES	15
A. ISSUE: PROPOSED REGULATION REQUIREMENTS FOR EACH CATEGORY OF PERSONAL INFORMATION EXCEED STATUTORY REQUIREMENTS.....	15
1. Proposed Regulation: §999.305; 999.305(d)(2)(b).....	15
2. Problem with Proposed Regulation:	15
3. Recommended Change:	16
B. ISSUE: PROPOSED REGULATION’S REQUIREMENT FOR EXPLICIT CONSENT EXCEEDS STATUTORY REQUIREMENTS.....	16
1. Proposed Regulation: §999.305(a)(3).....	16
2. Problem with Proposed Regulation:	16
3. Recommended Change:	16

TABLE OF CONTENTS

(continued)

	Page
C. ISSUE: NOTICE AT COLLECTION IS IMPRACTICAL UNDER CERTAIN CIRCUMSTANCES AND EXCEEDS THE STATUTORY PURPOSE.....	16
1. Proposed Regulation: §999.305(a)(2); 999.305(c)	16
2. Problem with Proposed Regulation:	16
3. Recommended Change:	17
D. ISSUE: ACCESSIBILITY FOR CONSUMERS WITH DISABILITIES SHOULD BE CLARIFIED TO BE WHEN REQUIRED BY THE AMERICANS WITH DISABILITIES ACT OF 1990.....	17
1. Proposed Regulation: §999.305(a)(2)(d); <i>see also</i> §§999.306(a)(2)(d); 999.307(a)(2)(d); 999.308(a)(2)(d).....	17
2. Problem with Proposed Regulation:	17
3. Recommended Change:	17
E. ISSUE: REGULATION DOES NOT ACCOUNT FOR SCENARIO WHERE BUSINESS RECEIVES PERSONAL INFORMATION ABOUT A CONSUMER FROM ANOTHER BUSINESS AND THEN CREATES ITS OWN DIRECT RELATIONSHIP WITH THE CONSUMER.	17
1. Proposed Regulation: §999.305	17
2. Problem with Proposed Regulation:	17
3. Recommend Change:	17
VIII. SECTION 999.306 NOTICE OF RIGHT TO OPT-OUT OF SALE OF PERSONAL INFORMATION—CHAMBER PROPOSED CHANGES.....	18
A. ISSUE: PROPOSED REGULATION EXCEEDS STATUTORY LANGUAGE, LIMITING BUSINESS ABILITY TO OPERATE, AND CREATES UNTENABLE COMPLIANCE OBLIGATIONS.....	18
1. Proposed Regulation: §999.306; 999.306(a)(1).....	18
2. Problem with Proposed Regulation:	18
3. Recommended Change:	18
B. ISSUE: REGULATION IMPROPERLY FORCES BUSINESS TO MAKE FUTURE REPRESENTATIONS TO CUSTOMERS.....	18
1. Proposed Regulation: §§999.306(d)(1); 999.306(d)(2)	18
2. Problem with Proposed Regulation:	18
3. Recommended Change	18

TABLE OF CONTENTS

(continued)

	Page
C. ISSUE: REGULATION COMPLICATES OPT-OUT NOTICE AND CREATES UNNECESSARY BURDEN FOR BUSINESS	18
1. Proposed Regulation: §999.306(d)	18
2. Problem with Proposed Regulation:	18
3. Recommended Change:	19
IX. SECTION 999.312 METHODS FOR SUBMITTING REQUESTS TO KNOW AND REQUESTS TO DELETE–CHAMBER PROPOSED CHANGES	19
A. ISSUE: MANDATING A THIRD METHOD FOR SUBMITTING REQUESTS IS UNNECESSARY, POSES SECURITY RISKS, AND CREATES CONFUSION.	19
1. Proposed Regulation: §999.312	19
2. Problem with Proposed Regulation:	19
3. Recommended Change:	20
B. ISSUE: REGULATIONS REQUIRE SAME RESPONSE REQUIREMENTS REGARDLESS OF WHAT METHOD WAS USED TO SUBMIT THE REQUEST.	20
1. Proposed Regulation: §999.312(e); 999.313(f)	20
2. Problem with Proposed Regulation:	20
3. Recommended Change:	21
C. ISSUE: MANDATING A TWO-STEP PROCESS DISEMPOWERS THE CONSUMER.	21
1. Proposed Regulation: §999.312(d)	21
2. Problem with Proposed Regulation:	21
3. Recommended Change:	21
X. SECTION 999.317 TRAINING; RECORD-KEEPING–CHAMBER PROPOSED CHANGES	21
A. ISSUE: RECORD-KEEPING REQUIREMENT DOES NOT ALIGN WITH PURPOSES OF CCPA.	21
1. Proposed Regulation: §999.317(g)	21
2. Problem with Proposed Regulation:	21
3. Recommended Change:	21
XI. SECTION 999.316 REQUESTS TO OPT-IN AFTER OPTING OUT OF THE SALE OF PERSONAL INFORMATION–CHAMBER PROPOSED CHANGES	22

TABLE OF CONTENTS

(continued)

	Page
A. ISSUE: REGULATION’S TWO-STEP PROCESS CREATES UNNECESSARY FRICTION AND CONSUMER CONFUSION.	22
1. Proposed Regulation: §999.316(a).....	22
2. Problem with Proposed Regulation:	22
3. Recommended Change:	22
XII. SECTION 999.325 VERIFICATION FOR NON-ACCOUNTHOLDERS–CHAMBER PROPOSED CHANGES	22
A. ISSUE: SIGNED DECLARATION OF PERJURY REQUIREMENT IS UNNECESSARY.	22
1. Proposed Regulation: §999.325(c).....	22
2. Problem with Proposed Regulation:	22
3. Recommended Change:	23
B. ISSUE: REQUIREMENT THAT BUSINESSES PROVIDE TWO TIERS OF AUTHENTICATION FOR RIGHT TO KNOW REQUESTS IS OVERLY BURDENSOME AND NOT COMMON PRACTICE.	23
1. Proposed Regulation: §999.325	23
2. Problem with Proposed Regulation:	23
3. Recommended Change:	23
C. ISSUE: TYPES AND THRESHOLD OF PERSONAL INFORMATION FOR VERIFIABLE REQUEST MAY LEAVE CONSUMERS VULNERABLE TO FRAUDULENT REQUESTS.....	23
1. Proposed Regulation: §999.325(c); 999.325(e); <i>see also</i> 999.323	23
2. Problem with Proposed Regulation:	23
3. Recommended Change:	23
XIII. SECTION 999.308 PRIVACY POLICY–CHAMBER PROPOSED CHANGES	24
A. ISSUE: REQUIREMENT THAT BUSINESS PUBLICLY DESCRIBE VERIFICATION PROCESS SHOULD BE ELIMINATED OR SATISFIED BY GENERAL DESCRIPTIONS TO MITIGATE SECURITY RISKS.....	24
1. Proposed Regulation: §999.308(b)(1); <i>see also</i> 999.313(a)	24
2. Problem with Proposed Regulation:	24
3. Recommended Change:	24

TABLE OF CONTENTS

(continued)

	Page
B. ISSUE: REGULATIONS SHOULD PROVIDE CLARIFICATION REGARDING THE REQUISITE LEVEL OF DETAIL TO DESIGNATE AN AUTHORIZED AGENT TO MAKE CONSUMER REQUESTS.....	24
1. Proposed Regulation: §999.308(b)(5)(a);	24
2. Problem with Proposed Regulation:	24
3. Recommended Change:	24
XIV. SECTION 999.318 REQUESTS TO ACCESS OR DELETE HOUSEHOLD INFORMATION—CHAMBER PROPOSED CHANGES	25
A. ISSUE: PROPOSED REGULATION DOES NOT ADDRESS CONCERN THAT HOUSEHOLD INFORMATION COULD BE DISCLOSED INCORRECTLY	25
1. Proposed Regulation: §999.318(b)	25
2. Problem with Proposed Regulation:	25
3. Recommended Change:	25
XV. SECTION 999.323 GENERAL RULES REGARDING VERIFICATION—CHAMBER PROPOSED CHANGES	25
A. ISSUE: INCREASED COMPLEXITY FOR VERIFICATION OF CONSUMERS.	25
1. Proposed Regulation: §999.323; 999.323(d)	25
2. Problem with Proposed Regulation:	25
3. Recommended Change:	25
B. ISSUE: REQUIREMENT TO GENERALLY AVOID REQUESTING ADDITIONAL CONSUMER INFORMATION FOR VERIFICATION IS COUNTERINTUITIVE TO NEED TO ENSURE VERIFICATION AND PROTECT CONSUMER SECURITY.....	26
1. Proposed Regulation: §999.323(c).....	26
2. Problem with Proposed Regulation:	26
3. Recommended Change:	26
XVI. SECTION 999.326 AUTHORIZED AGENT—CHAMBER PROPOSED CHANGES.....	26
A. ISSUE: BUSINESSES NEED MORE GUIDANCE REGARDING VERIFICATION OF AUTHORIZED AGENTS.....	26
1. Proposed Regulation: §999.326	26
2. Problem with Proposed Regulation:	26

TABLE OF CONTENTS

(continued)

	Page
3. Recommended Change:	26
XVII. SECTION 999.336 DISCRIMINATORY PRACTICES–CHAMBER PROPOSED CHANGES	26
A. ISSUE: AMBIGUITY IN PROPOSED REGULATION RELATED TO “FINANCIAL INCENTIVE” CREATES CONFUSION CONCERNING HOW LOYALTY PROGRAMS WILL OPERATE UNDER THE CCPA.	26
1. Proposed Regulation: §999.336	26
2. Problem with Proposed Regulation:	26
3. Recommended Changes:	27
XVIII. SECTION 999.337 CALCULATING THE VALUE OF CONSUMER DATA– CHAMBER PROPOSED CHANGES	27
A. ISSUE: PROPOSED REGULATIONS ARE INCONSISTENT WITH STATUTORY LANGUAGE.....	27
1. Proposed Regulation: §999.337	27
2. Problem with Proposed Regulation:	27
3. Recommend Change:	27
XIX. SECTION 999.330 MINORS UNDER 13 YEARS OF AGE–CHAMBER PROPOSED CHANGES	27
A. ISSUE: REGULATIONS SHOULD ALLOW FOR ANY METHOD PERMITTED BY COPPA FOR DISCLOSURE.	27
1. Proposed Regulation: §999.330(a).....	27
2. Problem with Proposed Regulation:	27
3. Recommended Change:	27
XX. SECTION 999.331 MINORS 13 TO 16 YEARS OF AGE–CHAMBER PROPOSED CHANGES	28
A. ISSUE: BUSINESSES THAT DO NOT PLAN TO SELL PERSONAL INFORMATION OF 13 TO 16 YEARS OLD SHOULD NOT NEED TO HAVE AN OPT-IN MECHANISM.	28
1. Proposed Regulation: §999.331(a).....	28
2. Problem with Proposed Regulation:	28
3. Recommended Change:	28

I. SECTION 999.315 REQUESTS TO OPT-OUT-CHAMBER PROPOSED CHANGES

A. ISSUE: BUSINESSES NEED THE OPTION NOT TO TREAT BROWSER PLUG-INS OR SETTINGS AS OPT-OUT REQUESTS, AND INSTEAD HAVE THE CHOICE TO PROVIDE AN OPT-OUT BUTTON.

1. Proposed Regulation: 999.315(c); 999.315(g)
2. Problem with Proposed Regulation:
 - a. CalChamber proposes that the AG's Office defer the browser enabled signal issue until after the California Privacy Rights Act of 2020 (CPRA) is voted on in November 2020 if it qualifies. As the CPRA at section 1798.185 provides for rule making at subsection 20-21, it would represent cost savings to industry and regulators to undergo this process once rather than twice in two years.
 - b. Existing browser signals are not "opt-out of sale" signals. There is also no industry-accepted technical standard regarding opt-out via a browser mechanism. Further, there is no guarantee that a browser installed opt-out reflects actual consumer choice versus a technical default.
 - c. The proposed regulations do not provide sufficient clarity as to what criteria must be present with respect to mechanisms developed in the future that may be effectuating a consumer choice.
 - d. These types of technology were designed in other contexts and are not aligned with the CCPA's complex and extremely broad definitions of "sale" and "personal information." The CCPA emphasizes consumer choice. It specifically defines a mechanism, the "Do Not Sell" button, that businesses must make available to consumers on their Web sites to exercise their choices. It is not consistent with the statute to create this additional mechanism, nor is it clear that consumers, who use plug-ins, intend to opt-out of CCPA sales. Currently, browser-based opt-out technology is not sufficiently interoperable and developed to ensure that all parties that receive such a signal can operationalize it.
 - e. A business should not be required to treat these settings as an official CCPA opt-out request. A business should be able to accept the browser-enabled method or provide the 'Opt-Out Button' and related processes set forth herein as an alternative.
3. Recommended Change:
 - a. Revise Section 999.315(c): "If a business collects personal information from consumers online, the business ~~shall~~ may treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer, provided that the consumer undertakes an affirmative action to opt-out of the sale of their information. Default opt-outs shall not constitute an affirmative step to opt-out."

B. ISSUE: PROPOSED REGULATIONS GIVE BROWSERS SIGNIFICANT DISCRETION TO EXERCISE AGAINST BUSINESSES THAT BROWSERS MAY BE IN COMPETITION WITH AND WHOSE "SALES" THEY ARE BLOCKING.

1. Proposed Regulation: §999.315(a); 999.315(c)
2. Problem with Proposed Regulation:
 - a. Regulations describe permitting a browser plugin or privacy setting to communicate a consumer opt-out of the sale of their personal information. Codifying browser-based signals would give significant power to browsers, who could unilaterally turn on "Do Not Sell" or even do it selectively for certain companies. In the event a browser-based

program will be established, to avoid the potential for self-serving implementation by browsers/devices, the law should empower the AG/Agency (whichever is in charge) to establish a uniform mechanism that browsers/devices would be required to implement so there is a level playing field for businesses and clarity for consumers.

3. Recommended Change:

- a. Revise section 999.315(a): “A business shall provide two or more designated methods for submitting requests to opt-out, including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information,” or “Do Not Sell My Info,” on the business’s website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information. The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should: (i) ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business; (ii) ensure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer, and does not require that the consumer provide additional information beyond what is necessary; (iii) clearly represent a consumer’s intent and be free of defaults constraining or presupposing such intent; and (iv) ensure that the opt-out preference signal does not conflict with other commonly-used privacy settings or tools that consumers may employ.”

C. ISSUE: PROPOSED REGULATION’S REQUIREMENT TO SHARE OPT-OUT REQUESTS WITH THIRD PARTIES EXCEEDS STATUTORY REQUIREMENTS.

1. Proposed Regulation: §999.315(f)

2. Problem with Proposed Regulation:

- a. Under section 999.315(f), a business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business’s receipt of the request and notify the consumer when this has been completed. Under the CCPA, there is no requirement for the sharing of a consumer requests outside of a service provider relationship in the context of deletion. 1798.105(c). The provision would likely result in a burdensome obligation to monitor and track the performance of a third party’s compliance, with no additional benefit to the consumer. A requirement to share opt-out requests with third parties is outside the scope of the CCPA. Also, this would be impossible for a business to do if the browser controls opt-out from sale and the option remains part of the regulatory framework.
- b. The CCPA does not address how a business that collects data from another business can provide the required consumer disclosure at the point of collection. The draft regulations allow either (1) contacting the consumer directly or (2) contact the source of the personal information to confirm notice was provided and obtain a signed attestation with an example of the notice from the source. The draft regulations go beyond a signed attestation or contractual assurances to require a description and example of the notice at collection and require the business to provide a copy of the attestation to the consumer upon request. The obligation presumes that a data user has proximity to the original collector. The AG’s statement of reasons suggests that this additional information would provide additional consumer protections by providing internal checks. However, the requirement would result in a burdensome and expensive process and require an organization to manage the CCPA compliance obligations of first-party collection, despite these obligations already required by law.
- c. A consumer exercising its right to know will also receive a description of the categories of business in which its personal information is sold. This list should be a roadmap for the consumer to exercise its rights with each individual business. A consumer may not

want each business to be opted-out of the sale of its personal information and this provision would make it mandatory.

3. Recommended Change:
 - a. Strike section 999.315(f).
 - b. If this provision remains, there should be alternative options such as allowing the purchaser to deidentify or aggregate the data or continue selling the personal information for purposes exempt under CCPA.

D. ISSUE: VERIFICATION OR AUTHENTICATION OF CONSUMERS SUBMITTING OPT-OUT REQUESTS SHOULD NOT BE PREVENTED OR LIMITED.

1. Proposed Regulation: §999.315(h)
2. Problem with Proposed Regulation:
 - a. The restriction on verifying opt-out requests may be appropriate for advertising or marketing uses, but the CCPA opt-out rights extend to data sales that are actually fraud prevention or identity authentication services that are vital to protect consumers. It puts consumers at risk to limit the ability to “verify” or authenticate such requests because that will allow criminals to opt their planned victims out of data services designed to protect those consumers. For further discussion of this issue, see “GDPArrrr: Using Privacy Laws to Steal Identities,” a study done under the GDPR, warning of identity theft issues for unverified requests for data. <https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf>.
 - b. Not requiring verification means that the wrong consumer could be opted-out.
3. Recommended Change:
 - a. Revise section 999.315(h): “A request to opt-out need not be a verifiable consumer request. If a business, however, cannot verify the identity of a person making a request concerning personal information sold for purposes other than advertising or marketing, has a good faith, reasonable, and documented belief that a request to opt out is fraudulent, the business may deny the request. ~~The business and~~ shall inform the requestor that their identity cannot be verified. ~~requesting party it will not comply with the request and shall provide an explanation of why it believes the request is fraudulent.~~”

E. ISSUE: RESPONSE TO REQUEST TO OPT-OUT ONLY SHOULD APPLY TO BUSINESS THAT SELL PERSONAL INFORMATION AND MORE TIME TO RESPOND IS NECESSARY.

1. Proposed Regulation: §§999.315(d); 999.315(e)
2. Problem with Proposed Regulation:
 - a. Businesses need clarity that this section does not apply if the business does not sell information.
3. Recommended Change:
 - a. Revise section 999.315(d): “In responding to a request to opt-out, a business that sells personal information may present the consumer with the choice to opt-out of sales of certain categories of personal information as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices.”
 - b. Revise section 999.315(e) from 15 to 30 days to act upon a request.

II. SECTION 999.307 NOTICE OF FINANCIAL INCENTIVE—CHAMBER PROPOSED CHANGES

A. ISSUE: DATA DOES NOT HAVE INDEPENDENT VALUE.

1. Proposed Regulation: §999.307; 999.337
2. Problem with Proposed Regulation:
 - a. Data does not have independent, objective value: It is more accurate to think of data as a raw material like flour, where the thing that creates the value in a pastry is the expertise and work of the baker. The perceived value of data is subjective and always in flux.
 - b. Data enables ads-based services to provide the core of the service itself, which is personalized content. The reason certain businesses can offer their services for free isn't that they're being compensated with people's data. It is that they make money by selling ads: these businesses sell advertisers the opportunity to present their messages to people. And advertisers pay the businesses based on objective metrics such as the number of people who see their ads or the number of people who click on their ads.
 - c. However, the free, ad-supported model is also used by newspapers, blogs, professional associations, and services that people find really useful (like online surveys, EventBrite, trip planning apps).
3. Recommended Change:
 - a. Remove any requirements for providing an estimate of the value of consumer data in Section 999.307(b)(5): “[a]n explanation of why the financial incentive or price or service difference is permitted under the CCPA, ~~including: a good faith estimate of the value of the consumer’s data that forms the basis for offering the financial incentive or price or service difference, and a description of the method the business used to calculate the value of the consumer’s data.~~”
 - b. Also strike Section 999.337, which describes the methods in calculating the value of consumer data.

B. ISSUE: REGULATION CREATES ONEROUS DISCLOSURE REQUIREMENTS.

1. Proposed Regulation: §999.307(a); 999.307(a)(3); 999.307(b)(2); 999.307(b)(5)
2. Problem with Proposed Regulation:
 - a. Regulation’s disclosure requirements are onerous.
 - b. Requirement to disclose the value and the methodology goes beyond the statutory language of the CCPA.
3. Recommended Change:
 - a. Reduce the information required to be disclosed.
 - b. Is Section 999.307 intended to only apply (1) where consumers receive a financial incentive or price or service difference in connection with exercise of their rights of access, deletion and opt-out of sale under CCPA or (2) to any financial incentive or price or service difference offered by businesses in connection with simply the collection of personal information? If (1), recommend clarifying regulation Section 999.307 to make clearer that making a financial incentive or offering differing services or prices simply by collecting personal data is not within scope of requiring notice of financial incentive.

when “the archived or backup system is next accessed or used” considering multiple users and departments.

- d. If a consumer submits a CCPA request using the wrong method, a business must either treat it as being correctly submitted and respond or inform the consumer how they can properly submit request, thereby increasing mailing costs. The requirement to confirm receipt of request within 10 days also increases mailing costs.
 - e. Under Sections 999.313(d)(1) and 999.313(d)(6)(a), if a business cannot identify identity for purposes of deletion, how can it effectuate an opt-out? This may be feasible for online identifiers—where you can simply opt out on an identifier basis, rather than delete. But in the non-identifier context this would not be feasible. In addition, this entire requirement runs counter to the verification requirements in the regulations.
 - f. A request to know, under Section 999.301(n), includes any or all of a number of elements. However, in responding to a request to know under Section 999.313(c)(10) the regulations call for all four types of data categories to be displayed.
 - g. Section 999.313(d)(3) permits a business to delay deleting consumer data stored on a back-up or archived system, but only until the archived or backup system is “next accessed or used.” This is vague and ambiguous and ignores the reality of how businesses keep data. If a business accesses a backup system for security or integrity-verification purposes, for example, does that count as accessing consumer data that might be stored in another database on the backup system such that the consumer data then has to be retrieved and deleted even if no longer accessed or used?
 - h. Unless and until a company can extract personal information of restored data on a back-up drive on a per individual basis, the company should be allowed to develop systems and safeguards to ensure that any such personal information is not restored into active systems where it could be accessed or used in any manner.
 - i. Compliance in the context of these technical limitations would necessarily require the destruction of data critical to the fundamental purpose of the backup system, i.e. business continuity. This is especially concerning in a time of climatological change in California where increased threats of fire, cyclones, and earthquakes are already testing and compromising business operations and systems integrity. The need for increased vigilance and protection for backup systems, data, and controls should be recognized or at least, evaluated in this context.
 - j. Unverifiable requests pose additional security risks. For further discussion, see “GDPArrrr: Using Privacy Laws to Steal Identities,” a study done under the GDPR, warning of identity theft issues for unverified requests for data. <https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf>.
3. Recommended Change:
- a. Priority recommendation would be to strike this provision entirely noting there are separate requests for separate reasons.
 - b. An alternative recommendation would be instead to focus on a process for making an unverifiable request to delete become a verified request to delete.
 - c. Revise Section 999.313(d)(3): “If a business stores any personal information on archived or backup systems, it may delay compliance with the consumer’s request to delete, with respect to data stored on the archived or backup system, until the data on the archived or backup system is next accessed or used.”
 - d. Change “and” to “or, as requested by the consumer” in Section 999.313(c)(10).

B. ISSUE: ENSURE BUSINESSES HAVE ENOUGH TIME AND FLEXIBILITY TO RESPOND TO REQUESTS UNDER STATUTORY TIMEFRAME.

1. Proposed Regulation: §999.313(a); 999.313(b)
2. Problem with Proposed Regulation:
 - a. The 45-day period for responding to consumer requests should begin to run once the request has been verified (§ 999.313(b)). The proposed regulations recognize businesses' responsibility to verify requests properly, a task that may take days or weeks to complete and is reliant upon a consumer's collaboration in providing accurate information in a timely manner. After a request is verified, a company must then find the information that it holds on a consumer—information which may be kept in separate databases—and convert it into a form which can be delivered to the consumer. If receipt of the request initiates the 45-day period, businesses will be incentivized to rush through one of these processes, which does not serve the consumer.
 - b. The proposal specifically states that the 45-day time limit applies, “regardless of time required to verify the request.” This could lead to a situation where a business is out of compliance because a consumer has failed to respond to a verification request. It should be revised to delete the time a consumer takes to respond.
3. Recommended Change:
 - a. It is likely that in the months after the CCPA takes effect, businesses will receive a flood of consumer requests. The AG should incentivize businesses to handle these requests responsibly and efficiently.
 - b. Revise Section 999.313(a): “Upon receiving a request to know or a request to delete, a business shall confirm receipt of the request, through either mail, email, or another notification method, within 10 days and provide information about how the business will process the request. The information provided shall describe the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request.”
 - c. Revise Section 999.313(b): “Businesses shall respond to complete requests to know and requests to delete within 45 days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request unless the request is incomplete, or, unless the request is incomplete, or the consumer fails to provide information necessary to verify the request. If necessary, businesses may take up to an additional 45 days to respond to the consumer's request, for a maximum total of 90 days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.”
 - d. Businesses should have option for confirmation of request using the same method as the request was submitted, unless the consumer clearly indicates an alternative means of communication in the initial request.

C. ISSUE: PROPOSED REGULATION REQUIREMENTS HEIGHTEN BURDENS ON BUSINESS AND EXCEED STATUTORY LANGUAGE.

1. Proposed Regulation: §999.313
2. Problem with Proposed Regulation:
 - a. Section 999.313(a)-(c) creates substantial additional burdens on top of already-burdensome “right to know” requirements included in CCPA and GDPR, by requiring companies to produce a second set of responses in addition to the specific pieces of information retained about the customer—namely, customized metadata regarding the

information collected for each customer, categorized in a complicated manner outlined by the statute.

- b. Clarify that businesses do not need to provide categories of personal information if already providing specific information; remove requirements to provide information about each category of personal information; confirm that language used in statute is sufficiently meaningful for consumers; permit generic disclosures in the privacy notice in cases where response is accurate for most or substantially all consumers.
 - c. The draft regulations suggest that businesses must provide the categories of sources of information, uses of information, categories of third parties to which information is disclosed or sold, and the purposes of such disclosures or sales for each category of personal information that it collects. These requirements require disclosures beyond what the statute requires, as the statute does not require such disclosure for each category of information.
3. Recommended Change:
- a. Align language with statute.
 - b. A revision to Section 999.313(c)(9) expanding the circumstances in which a company could rely on a generic articulation of categories in the Privacy Notice, as opposed to a customer-specific feed. For example, the regulation could be broadened to clarify that we may refer to our privacy policy when our response would be the same for “substantially all” or “most” consumers.
 - c. A revision to Section 999.313(c)(10) that would not require the additional pieces of information listed there (categories of sources, business purpose, categories of parties to whom disclosed/sold and why) to be broken out for *each category of information collected*.
 - d. A revision to Section 999.313(c)(11) clarifying that use of the language specifically enumerated in either the statute or the regulation “provides consumers a meaningful understanding of the categories listed.”
 - e. A revision to Section 999.313(c) to add new Section 999.312(c)(12) that would clarify that a company need not *additionally* fulfill a request to provide *categories* of information collected if it is *also* providing specific pieces of information. (Perhaps this could be time-bound to make it more palatable?).
 - f. A revision to Section 999.313(c) to add new Section 999.312(c)(13) that would clarify a business shall identify the personal information responsive to a request to know by conducting a commercially reasonable search of its records.

D. ISSUE: REGULATION SHOULD CLARIFY THAT A BUSINESS’S OBLIGATION TO COMPLY WITH A CONSUMER REQUEST IS LIMITED TO ITS ABILITY TO IDENTIFY RESPONSIVE MATERIALS USING COMMERCIALY REASONABLE EFFORTS.

- 1. Proposed Regulation: §999.313(c); 999.313(d)
- 2. Problem with Proposed Regulation:
 - a. Regulation should address the level of diligence a business must use when complying with consumer requests to know or delete. The regulation does not address whether a business that engages in a good-faith, commercially reasonable and diligent search of its records, could be found non-compliant in the event it fails to identify a record containing personal information pertaining to a request. Without a specified standard, a business could spare no expense to comply, engaging an army of people to scour every record that the business holds manually for potential matches. Such a process would not be commercially reasonable or worthwhile to California consumers, as it would force

businesses to raise prices to cover the costs of searching. Analogous frameworks in which large volumes of information are requested from businesses with widespread records provide standards. For example, both the California and Federal Rules of Civil Procedure allow parties to consider the burden and expense associated with discovery requests.

3. Recommended Change:

- a. Add language, consistent with the statute (1798.145), to new subsections 999.313(c)(13) and 999.313(d)(8): “A business shall identify the personal information responsive to a request by conducting a commercially reasonable search of its records for documents that are responsive, considering the sensitivity of the personal information the business holds and the expense of compliance. A business does not violate the CCPA when, it conducts a commercially reasonable search of its records in good faith but fails to identify a responsive record.”

E. ISSUE: REGULATION SHOULD CONSIDER HOW RESPONDING TO REQUESTS COULD JEOPARDIZE OTHER CUSTOMERS’ SECURITY AS WELL.

1. Proposed Regulation: §999.313(c)(3); *see also* 999.313(d), 999.323

2. Problem with Proposed Regulation:

- a. Regulation should reference security risks to personal information of other consumers as well. Businesses are concerned that the CCPA’s requirement to provide certain specific pieces of personal information to consumers will create a risk of identity theft by malefactors. The prohibition on disclosing sensitive personal data elements to consumers represents good security practice. Additionally, the balancing tests laid out in the proposed regulations are helpful clarifications that businesses must weigh the benefit to the consumer of receiving specific pieces of personal information with the risk of facilitating improper disclosure of such information.
- b. We welcome the fact that de-identification of personal information serves as an acceptable method of deletion. This provisions similarly strikes the proper balance between consumers’ rights and the interests of businesses and the public in analyzing data that presents little risk to consumer privacy.

3. Recommended Change:

- a. Revise Section 999.313(c)(3) language to: “substantial, articulable, and unreasonable risk to the security of that personal information, the consumer’s or another consumer’s account with the business, or the security of the business’s systems or networks.”

F. ISSUE: REGULATION DOES NOT ADDRESS REQUESTS SEEKING PORTABILITY OF INFORMATION WHERE DISCLOSURE OF CONSUMER’S PERSONAL INFORMATION IS NECESSARY TO SUPPORT PORTABILITY.

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

2. Problem with Proposed Regulation:

- a. The language does not address requests seeking portability of information where such identifiers enumerated in Section 999.313(c)(4) are necessary to support portability.

3. Recommended Change:

- a. Revise Section 999.313(c)(4): “A business shall not at any time disclose a consumer’s Social Security number, driver’s license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers. This

subsection does not apply to requests seeking portability of information where such identifiers enumerated in Section 999.313(c)(4) are necessary to support portability.

G. ISSUE: NOTIFYING CONSUMER OF REASON FOR REQUEST DENIAL MAY INTERFERE WITH LAW ENFORCEMENT INVESTIGATION, HINDER BUSINESS OPERATIONS, AND IS CONTRARY TO THE PURPOSE OF AN EXEMPTION.

1. Proposed Regulation: §999.313(c)(5)
2. Problem with Proposed Regulation:
 - a. Section 999.313(c)(5) requires that if an access request is denied because of federal or state law, or because of an exception to the CCPA, the consumer must be notified of the reason why. Under certain circumstances, this could interfere with an active law enforcement investigation, or it could result in the disclosure of information that may interfere with a business's operations or the rights of others.
 - b. Under Section 999.313(c)(5), if a business denies a consumer's verified request to know specific pieces of personal information because of an exemption to the CCPA, the business must inform the requestor of the basis for the denial. This section would require a business to inform a consumer that it holds data subject to an exemption under the CCPA and undermines the purpose of an exemption from the obligations under the law. By providing data exemptions under the CCPA, the provision could require new tracking mechanisms to understand if an organization has exempted data about a consumer that could be included in disclosures.
3. Recommended Change:
 - a. Limit the disclosure regarding request denial.
 - b. Modify language so that if a company includes the CCPA exemptions in their privacy policy, they can just point consumers to those exemptions on their privacy policy and note that they are not responding because of an exemption listed in the privacy policy per the CCPA.
 - c. Revise Section 999.313(c)(5): "If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception pursuant to the CCPA, the business shall inform the requestor and explain the basis for its denial, provided however that a business shall be deemed to be in compliance with the requirement if bases for denial are set forth in its privacy policy and the business refers the consumer to its privacy policy. If the request is denied only in part, the business shall disclose the other information sought by the consumer."

H. ISSUE: INDIVIDUALIZED RESPONSES TO CATEGORIES OF SOURCES OR THIRD PARTIES IS TOO BURDENSOME FOR BUSINESSES.

1. Proposed Regulation: §999.313(c)(9)-(10)
2. Problem with Proposed Regulation:
 - a. Sections 999.313(c)(9)-(10) require a business to provide an "individualized response" as to categories of personal information, sources, and third parties to whom data is sold, rather than reporting the business's general business practices and categories. This will require businesses to provide for each category of information applicable to a consumer: (a) The categories of sources from which the personal information was collected; (b) The business or commercial purpose for which it collected the personal information; (c) The categories of third parties to whom the business sold or disclosed the category of personal information for a business purpose; and (d) The business or commercial purpose for which it sold or disclosed the category of personal information. Companies do not track

personal information elements in this manner and this requirement will burden companies significantly to comply with new requirements that at best will provide consumers with marginal incremental general information about their personal information and its use.

3. Recommended Change:
 - a. Remove language in Sections 999.313(c)(9)-(10) that require detailed disclosures for each category of personal information.
 - b. Remove the requirement that disclosures include reference to all elements of Section 999.313(c)(10), as the CCPA via sections 1798.100; 1798.110; and 1798.115, permit consumers to request to know about different types of practices in differing level of detail.

IV. SECTION 999.314 SERVICE PROVIDERS—CHAMBER PROPOSED CHANGES

A. ISSUE: PROPOSED REGULATIONS' LIMITATIONS ON SERVICE PROVIDERS' PERMISSIBLE USES OF DATA CONTRADICTS THE STATUTORY DEFINITION OF "BUSINESS PURPOSE" AND "SERVICE PROVIDER."

1. Proposed Regulation: §999.314(c)
2. Problems with Proposed Regulation:
 - a. Because the service provider's business purposes may include using personal information for the benefit of one business in a way that might also benefit other businesses, the CCPA statute is best interpreted to permit the service provider to use the personal information that it receives for business purposes that might provide a benefit to other of its business partners, as long as such use is permitted under the written agreement between the business and the service provider and otherwise consistent with the CCPA. In many circumstances, this information would be considered aggregate insights or information that is not personally identifiable, but here, as in other sections, the overly broad definition of personal information threatens an ordinary business practice that presents little risk to consumers.
 - b. Section 999.314(c) would severely limit the ability of service providers to improve and build services that can be used to process personal information. In many cases, service providers that process personal information may make improvements to their services in connection with the personal information in a way that does not identify, target, or otherwise impact any consumer or household—for example, an improvement in handling technical aspects of data. The language would restrict this kind of improvement as it could be interpreted to not allow improvements to be used for any other customer, thus limiting service innovation or improvement by service providers. Service providers that have permission from an entity to use provided information to improve their services should be able to do so as long as the improvement and use does not result in the disclosure of that information to a third party. The text of the statute explicitly permits disclosures to "service providers" for a broad list of enumerated "business purposes" defined under the statute. Importantly, the statute defines "business purpose" to include both a business's *or a service provider's* operational purposes or other notified purposes. The statutory text also permits a service provider to use the personal information it receives from one business for such business purposes of both that business and the service provider where the use is authorized as part of the contracted-for "services" provided to the business or as otherwise permitted by the Act.
 - c. The plain text of the section appears to prohibit service providers from using the personal information they receive from one entity to provide services to another person or entity, unless such services are necessary for detecting security incidents or preventing fraud or other illegal activity. The draft regulations improperly focus solely on the business purpose of the business and ignore the fact that the statutory definition of "business purpose" also includes the use of personal information for the "service provider's operational purposes or other notified purposes."

- d. The activities included in the list of business purposes (such as “performing services on behalf of the business or service provider, including providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider”) require the combination and use of personal information received from and for the benefit of multiple businesses.
 - e. As such, focusing solely on the business purposes of the business, as the proposed regulations do, would both render the bolded language surplusage, contrary to well-established canons of statutory interpretation, as well as potentially render impermissible a number of the activities explicitly included on the list of permissible business purposes.
 - f. Combining the data with other personal information to further the purposes of the services being provided should be permitted, especially when the services are to further deidentify or aggregate the personal information. Combining personal information from multiple businesses as a service provider for each business for purposes of aggregating the data should not be considered a “sale.”
 - g. The language in Section 999.314(c) is written very broadly and could be interpreted to not allow certain internal operations for the service provider that might require the combining of data, including improving the quality of the service providers services that it provides for businesses generally. To that end, the text should be modified as indicated.
3. Recommended Change:
- a. Modify language:
 - “(c) A service provider shall not use personal information received either from a person or entity it services or from a consumer’s direct interaction with the service provider, without the agreement of such person, entity, or consumer, for the purpose of providing services that result in the sale of a consumer’s personal information to a third party to another person or entity. A service provider may, however, combine personal information received from one or more entities to which it is a service provider, ~~on behalf of such businesses in order to provide the services specified in a contract with a business, or~~ to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.”
 - b. Revise use limitations to (1) permit service providers to use personal information for the benefit of all customers with the permission of the person, entity, or consumer from whom the service provider received the personal information; or (2) reduce the limitation to apply only to providing services that result in the disclosure of a consumer’s personal information to a third party.

B. ISSUE: PROPOSED REGULATION CREATES ADDITIONAL BURDENS FOR BUSINESS THAT EXCEED STATUTORY LANGUAGE.

- 1. Proposed Regulation: §999.314(d)
- 2. Problem with Proposed Regulation:
 - a. This is difficult to manage since many businesses act as a service provider, while also collecting additional personal information for their own business purposes (as is noted above in Section 999.314(c)). If a business receives a “request to know” from a consumer, the business should be able to focus only on the personal information collected by that business and not the personal information it is maintaining for a different business when acting as a service provider. In addition, many service provider relationships are confidential and proprietary to the business engaging the service provider. Disclosing the name of the business engaging the service provider could violate those restrictions while also sharing competitive information publicly.

- b. Section 999.314(d) requires that a service provider that receives but “does not comply” with a consumer’s request to know or delete must inform the consumer of the reason for the denial, explain that the consumer should submit the request directly to the business, and, when feasible, provide the contact information for the business. This requirement creates new obligations for service providers beyond the statutory text because service providers do not have an obligation to comply with such deletion requests.
3. Recommended Change:
- a. Revise Section 999.314(d): “If a service provider receives a request to know or a request to delete from a consumer regarding personal information that the service provider collects, maintains, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial. ~~If a service provider receives a request to know or a request to delete from a consumer regarding personal information that the service provider collects, maintains, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial.~~”

V. SECTION 999.301 DEFINITIONS—CHAMBER PROPOSED CHANGES

A. ISSUE: DEFINITION OF RIGHT TO KNOW CONFLICTS WITH REQUIREMENTS FOR HOW TO RESPOND TO RIGHT TO KNOW.

- 1. Proposed Regulation: §§999.301(n); 999.313(c)(10)
- 2. Problem with Proposed Regulation:
 - a. The definition of right to know under Section 999.301(n) says a consumer has a right to “any or all” of the following categories of personal information. However, Section 999.313(c)(10), instructing businesses how to respond to requests to know, uses the conjunctive “and”—not “and/or”—for the categories of information a business must disclose in response to a consumer request. Thus, under Section 999.313, a business is required to disclose all enumerated categories, even if consumer only makes a limited request.
- 3. Recommended Change:
 - a. Correct the wording in Section 999.313(c)(10) to say “and/or as requested by the consumer.”

B. ISSUE: DEFINITION OF RIGHT TO KNOW CREATES INFEASIBLE REQUIREMENTS FOR RESPONDING TO INDIVIDUAL CONSUMER REQUESTS.

- 1. Proposed Regulation: §999.301(n).
- 2. Problem with Proposed Regulation:
 - a. This definition is perceived as the most concerning. It lumps one request into different categories, sources, and a variety of different requests. It would be preferred if each subsection (1) through (6) were separately defined. Subsections (2) through (6) should be addressed through a notice so it is standardized across the board for all consumers. It is not feasible or scalable to provide the customized set of categories to each individual consumer.
- 3. Recommended Change:
 - a. The “Request to know” should be linked only to subsection (1).

- C. THE SCOPE OF THE DEFINITION OF “PRICE OR SERVICE DIFFERENCE” COULD PREVENT BUSINESS WITH SERVICE PROVIDERS.
1. Proposed Regulation: §999.301(l)
 2. Problem with Proposed Regulation:
 - a. Regarding the definition of “Price or service difference,” there is a concern that if a broker or provider (as a business partner) opts-out of the sale of personal information, this could unknowingly to the business partners) serve to prevent their continued business with a business.
 3. Recommended Change:
 - a. Revise Section 999.301(l) to include language that “If an individual working for a broker or provider as a business partner opts-out of the sale of personal information this will not prevent the continued relationship with a business.”
- D. ISSUE: DEFINITION OF “AFFIRMATIVE AUTHORIZATION” REQUIREMENT FOR TWO-STEP PROCESS TO OPT-IN IS OVERLY BURDENSOME FOR CONSUMERS AND BUSINESS.
1. Proposed Regulation: §999.301(a)
 2. Problem with Proposed Regulation:
 - a. For consumers 13 years and older, Section 999.301(a) mandates a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in. Mandating a two-step process can be cumbersome and disruptive for consumers and overly prescriptive for businesses. It can prevent businesses from developing innovative consent flows based on extensive UX/UI research.
 3. Recommended Change:
 - a. Strike the language in section 999.301(a) mandating a two-step process.
- E. ISSUE: PROPOSED REGULATIONS NEED TO PROVIDE CLARIFICATION REGARDING DEFINITION OF DIRECT NOTICE TO CONSUMERS.
1. Proposed Regulation: §999.301; *see also* §§999.305(a)(3), 999.305(d)(1), 999.306(d)(2)
 2. Problem with Proposed Regulation:
 - a. There is a lack of clarity as to direct notification under the regulations. Providing a definition of “directly notify” would provide certainty as well as coordination across all the rules that require some sort of direct notice to consumers.
 3. Recommended Change:
 - a. Add a new subsection 999.301(g): “Directly Notify” means contacting the consumer directly with the required information, provided, however, that a business will have been deemed to directly notify a consumer of changes to its policies and practices if the notification is published and made available on its website for a sufficient period of time or other standard method of providing privacy policies and notices to consumers.”

VI. SECTION 999.300 TITLE AND SCOPE—CHAMBER PROPOSED CHANGES

A. ISSUE: THE REGULATIONS SHOULD CLARIFY THE CCPA’S JURISDICTIONAL SCOPE AND EFFECTIVE DATE.

1. Proposed Regulation: §999.300
2. Problem with Proposed Regulation:
 - a. The CCPA’s broad definition of business suggests that a non-U.S. business that incidentally collects the personal information of a single California resident should comply with all of its requirements. This could sweep in a large number of entities over whom California would not normally have jurisdiction.
 - b. The effective date of enforcement should be delayed until January 1, 2021 to allow companies time to comply with the regulations.
 - c. The regulations should clarify and make specific the Health Insurance Portability and Accountability Act (HIPPA) and Confidentiality of Medical Information Act (CMIA) exemption language in Section 1798.145(c)(1)(B) of the CCPA.
3. Recommended Change:
 - a. The regulations should clarify that a business whose operations are outside of California and who only collect a *de minimus* amount of personal information from California residents—such as bbc.co.uk or lajornada.com.mx—are not required to comply with CCPA. Alternatively, the regulations might state that businesses that operate outside of California and do not target their services to California residents are not covered.
 - b. Revise section 999.300 to include the following: “The title shall not apply to a provider of health care governed by CMIA or HIPAA, to the extent the provider or covered entity collects personal information in connection with the provision or sale of health care-related products or services, and to the extent that the provider or covered entity maintains that personal information in a way that meets HIPAA Security Rule requirements.”

VII. SECTION 999.305 NOTICE AT COLLECTION OF PERSONAL INFORMATION—CHAMBER PROPOSED CHANGES

A. ISSUE: PROPOSED REGULATION REQUIREMENTS FOR EACH CATEGORY OF PERSONAL INFORMATION EXCEED STATUTORY REQUIREMENTS.

1. Proposed Regulation: §999.305; 999.305(d)(2)(b)
2. Problem with Proposed Regulation:
 - a. Section 999.305 mandates that the notice at collection includes requirements that go beyond the statute, which only requires that businesses describe the categories of personal information collected and the purpose for which such information is used for employee data.
 - b. The proposed regulations do not seem to distinguish between the notice to employees and the notice to customers. Each notice would address different types of data. Also, the proposed regulation’s notice requirement to include a link to the business’s privacy policy creates confusion whether a business needs two privacy policies, one for employee data and one for customer data.

3. Recommended Change:
 - a. We first recommend deletion of Section 999.305(d)(2)(b). In the alternative, the regulations should clarify that a business that receives personal information from an indirect source may comply with its CCPA obligations through contractual provisions that require other businesses to provide the requisite notice to consumers. The requirements to contact the source and obtain signed attestations are confusing and duplicative.
 - b. The AG should provide a different set of regulations to apply to the employee notice separate from the customer notice.

B. ISSUE: PROPOSED REGULATION’S REQUIREMENT FOR EXPLICIT CONSENT EXCEEDS STATUTORY REQUIREMENTS.

1. Proposed Regulation: §999.305(a)(3)
2. Problem with Proposed Regulation:
 - a. Section 999.305(a)(3) requires businesses to obtain explicit consent from consumers to use personal information for a purpose not disclosed at the time of collection. Explicit consent is such a high bar that is likely to make it either infeasible to use previously collected information for a purpose not previously disclosed or incentivize broad disclosures that may cut against data minimization principles.
 - b. This new purpose limitation requiring obtaining explicit consent from the consumer to use personal information for a new purpose also exceeds the scope of the CCPA’s statutory language, which only requires notice of new purposes. *See* 1798.100(b).
 - c. There should be a way of expanding usage and ability to sell personal information without having to directly notify consumers and obtain explicit consent (e.g. data uses within the same category of business or which align with the consumer’s expectations when the data was collected).
3. Recommended Change:
 - a. Revise Section 999.305(a)(3) to permit businesses to use personal information for a purpose not disclosed at the time of collection upon notice to the consumer. The change would be consistent with Section 178.100(b), which requires only notice consistent with the Section, not explicit consent as contemplated by the regulations.
 - b. Revise Section 999.305(a)(3): “A business shall not use a consumer’s personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer’s personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall notify the consumer of this new use ~~and obtain explicit consent from the consumer to use it for this new purpose.~~”

C. ISSUE: NOTICE AT COLLECTION IS IMPRACTICAL UNDER CERTAIN CIRCUMSTANCES AND EXCEEDS THE STATUTORY PURPOSE.

1. Proposed Regulation: §999.305(a)(2); 999.305(c)
2. Problem with Proposed Regulation:
 - a. Section 999.305(a)(2)(e) requires businesses to provide notice of collection of personal information before any information is collected. This approach is not practical for online environments, where information such as IP addresses is collected automatically.

- b. Also need clarity whether, under section 999.305(c), cookie data collection requires a pop-up for the Notice at Collection.
 - 3. Recommended Change:
 - a. Revise Section 999.305(a)(2) to require notice at or before the time of collection, rather than before collection. The change would be consistent with Section 1798.100(b), which requires notice at or before the point of collection.
- D. ISSUE: ACCESSIBILITY FOR CONSUMERS WITH DISABILITIES SHOULD BE CLARIFIED TO BE WHEN REQUIRED BY THE AMERICANS WITH DISABILITIES ACT OF 1990.
- 1. Proposed Regulation: §999.305(a)(2)(d); *see also* §§999.306(a)(2)(d); 999.307(a)(2)(d); 999.308(a)(2)(d)
 - 2. Problem with Proposed Regulation:
 - a. The ambiguity created by this proposal is that the Americans with Disabilities Act of 1990 (ADA) currently does not apply to marketing-only websites. Does this proposed regulation extend the breadth of the ADA to marketing-only websites that do not offer sales/service such that *all* websites operated by entities within the scope of the CCPA have to also be ADA compliant?
 - 3. Recommended Change:
 - a. Revise Sections 999.305(a)(2)(d); 999.306(a)(2)(d); 999.307(a)(2)(d); 999.308(a)(2)(d): “Be accessible to consumers with disabilities when required by the Americans with Disabilities Act of 1990, Pub. L. No. 101-336, 104 Stat. 328 (1990). At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.”
- E. ISSUE: REGULATION DOES NOT ACCOUNT FOR SCENARIO WHERE BUSINESS RECEIVES PERSONAL INFORMATION ABOUT A CONSUMER FROM ANOTHER BUSINESS AND THEN CREATES ITS OWN DIRECT RELATIONSHIP WITH THE CONSUMER.
- 1. Proposed Regulation: §999.305
 - 2. Problem with Proposed Regulation:
 - a. The regulations cover how a business that collects information *directly* from consumers provides notice and how a business that *does not collect information directly from consumers* is to comply with the notice requirement. The regulations do not provide clarity as to the middle ground between those two scenarios— i.e. a business that receives information about a consumer from another business and then creates its own direct relationship with the consumer. In that scenario, it is impossible to provide notice before the initial “collection” of information from the other business, but it is possible to provide notice before the business begins to collect information *directly* from the consumer as part of the consumer’s direct, intentional, interaction with the business.
 - b. We suggest that the regulations be revised to provide clarity that a business that receives consumer information from another business may comply with the notice requirement by providing a notice at or before additional information is collected *directly* from the consumer.
 - 3. Recommend Change:
 - a. If feasible, providing notice within a reasonable time frame upon receiving the information, and *no later than at the time of directly collecting additional information from the consumer.*

VIII. SECTION 999.306 NOTICE OF RIGHT TO OPT-OUT OF SALE OF PERSONAL INFORMATION—CHAMBER PROPOSED CHANGES

A. ISSUE: PROPOSED REGULATION EXCEEDS STATUTORY LANGUAGE, LIMITING BUSINESS ABILITY TO OPERATE, AND CREATES UNTENABLE COMPLIANCE OBLIGATIONS.

1. Proposed Regulation: §999.306; 999.306(a)(1)
2. Problem with Proposed Regulation:
 - a. The CCPA does not govern a business’s future potential to sell personal information, but instead governs the practices of businesses that sell personal information at the time of processing the personal information. The proposed regulation references not only businesses that actually sell personal information, but also businesses that may in the future, exceeding the current statutory language.
 - b. This requirement means that if a business did not sell personal information, and then did not have a “Do Not Sell” button, if it then chooses to sell and has a button, then personal information collected about consumers during the time the button was not shown will automatically be subject to the opt-out. Accordingly, businesses will then have the option to request that consumers authorize the sale pursuant to Section 1798.135. First, this is counter to the text of the CCPA, which allows for new uses of data pursuant to notice (whereas explicit consent is required under the draft regulations, and we have already pointed out that this is in contravention to the statute). In addition, there is lack of clarity as to when businesses will be able to seek authorization from these consumers who will have been “deemed” to have opted-out.
3. Recommended Change:
 - a. Remove “future sell” language from Section 999.306(a)(1).

B. ISSUE: REGULATION IMPROPERLY FORCES BUSINESS TO MAKE FUTURE REPRESENTATIONS TO CUSTOMERS.

1. Proposed Regulation: §§999.306(d)(1); 999.306(d)(2)
2. Problem with Proposed Regulation:
 - a. The proposed rules also state that businesses are exempt from providing a notice of right to opt-out if does not sell “and will not” sell personal information and if it states in its privacy policy that it does not and “will not” sell not personal information. Mandating that businesses make future representations like this unnecessarily restricts businesses from evolving their business models and roadmaps. And in the event that a business in good faith makes a representation that it will not sell information and at a later time decides to sell personal information with adequate notice to consumers, the business now risks that it has made an unfair and deceptive claim to consumers by previously representing that it will not sell personal information.
3. Recommended Change
 - a. Remove “will not” sell language from Sections 999.306(d)(1) and 999.306(d)(2).

C. ISSUE: REGULATION COMPLICATES OPT-OUT NOTICE AND CREATES UNNECESSARY BURDEN FOR BUSINESS

1. Proposed Regulation: §999.306(d)
2. Problem with Proposed Regulation:

- a. First, the proposed rule conflates general personal information collection (not selling) with the right to opt-out of the selling of personal information. A business that does not post an opt-out notice because it does not sell personal information shouldn't be deemed to have received an opt-out because there is nothing from which the consumer can opt-out (the business doesn't sell information).
 - b. Second, the CCPA explicitly references that a business shall be prohibited from selling a consumer's information after receiving "direction from a consumer not to sell the consumer's personal information" 1708.120(d). The draft regulation has replaced this "direction" requirement, which requires an explicit action through the opt-out button, with a "default" opt-out.
 - c. Third, pursuant to the draft regulations, businesses are required to keep a record of the opt-outs they receive. For businesses who don't sell personal information but to whom consumers can be deemed to have submitted the default opt-out mentioned above, this creates an unnecessary compliance burden.
 - d. Also, if a business receives "default" opt-outs at a time where it didn't sell information but decides to sell information within 12 months, the business will be preemptively prohibited from selling information for 12 months even though the business has not received explicit "direction from a consumer not to sell the consumer's personal information," as required by the CCPA.
 - e. Section 999.306(d)(2) may not be operable for businesses.
3. Recommended Change:
- a. Allow businesses to instead publish a change in policy for a sufficient period of time to give consumers the right to opt out.
 - b. Revise Section 999.306(d)(2): ~~"It states in its privacy policy that that it does not and will not sell personal information. A consumer whose personal information is collected while a notice of right to opt-out notice is not posted shall be deemed to have validly submitted a request to opt-out."~~

IX. SECTION 999.312 METHODS FOR SUBMITTING REQUESTS TO KNOW AND REQUESTS TO DELETE—CHAMBER PROPOSED CHANGES

A. ISSUE: MANDATING A THIRD METHOD FOR SUBMITTING REQUESTS IS UNNECESSARY, POSES SECURITY RISKS, AND CREATES CONFUSION.

- 1. Proposed Regulation: §999.312
- 2. Problem with Proposed Regulation:
 - a. The proposed regulations in Sections 999.312(a) and (b) require that businesses provide two or more designated methods for submitting requests to know and requests to delete. However, Section 999.312(c) increases the burden on certain businesses beyond the statutory requirements from a minimum of two to a minimum of three methods to submit a request.
 - b. The requirement in Section 999.312(c) that submissions be accepted at physical locations is not contemplated by statute, is not considered sound security practice, and imposes disproportionate obligations on brick and mortar stores. Using paper forms increases risks to security and privacy because they can be misplaced or mishandled even if a company has certain protocols in place, especially given the high turnover of employees in retail.
 - c. For companies with multiple physical locations, providing a toll-free number along with an online portal provide effective and consumer friendly methods for consumers to

submit requests. Mandating a *third* method for certain businesses with physical locations creates confusion and uncertainty depending on how the term “primarily interacts” is construed. We suggest that businesses who elect to provide *both* a toll-free number and online portal are providing consumers with ample opportunity to submit requests and therefore should not be required to provide another option that is unlikely to provide any additional consumer benefit.

- d. This section needs to be revised to allow for businesses that interact with consumers online only to not have the toll-free number requirement, but rather an email requirement per AB 1564.
3. Recommended Change:
- a. Modify the language in Section 999.312(c)(2) so that a business operating a website, but primarily interacting with customers in person, shall offer two—not three—methods: a toll-free telephone number, and an interactive webform, or a form that can be submitted in person.
 - b. Modify the language so that a business providing both a toll-free number and online portal for customers to submit requests would be sufficient.
 - Add new subsection 999.312(c)(3): “Example 3: If the business operates a website and interacts with customers in person at a retail location, but primarily collects data online (such as a travel company website), the business can offer two methods to submit requests to know—a toll-free telephone number and an interactive webform accessible through the business’s website. In this case, a form that can be submitted in person at the retail location is not necessary.”
 - c. Modify the language so that businesses that interact with consumers online only to not have the toll-free number requirement, but rather only an email requirement per AB 1564.
 - Delete existing subsection 999.312(f) and add new 312(f) to include: “A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.”

B. ISSUE: REGULATIONS REQUIRE SAME RESPONSE REQUIREMENTS REGARDLESS OF WHAT METHOD WAS USED TO SUBMIT THE REQUEST.

- 1. Proposed Regulation: §999.312(e); 999.313(f)
- 2. Problem with Proposed Regulation:
 - a. It is unclear how this section interacts with Section 999.313, which requires a business to confirm receipt of a request within 10 days of the date received and to respond within 45 days (regardless of how long verification takes).
 - b. Potentially broadens training requirements for personnel who handle consumer requests, since personnel may have to be trained to forward requests internally.
 - c. CCPA only requires that a business designate two or more methods for such requests to be submitted and this proposed language defeats the purpose of a business designating a method if consumers can still submit requests not using a designated method of submission (i.e. to be able to staff with trained personnel and meet statutory deadlines).
 - d. This timeline is challenging. Additional time akin to 45 days would be reasonable in light of the steps a business will need to take to coordinate. Especially where vendors are

involved in supporting the process, things like monthly data feeds could be affected. Also, the 15 versus 90 days as noted in Section 999.312(f) below are not congruent.

3. Recommended Change:
 - a. Strike existing section 999.312(f).

C. ISSUE: MANDATING A TWO-STEP PROCESS DISEMPOWERS THE CONSUMER.

1. Proposed Regulation: §999.312(d)
2. Problem with Proposed Regulation:
 - a. Mandating a two-step process actually disempowers the consumer as many companies may operate a “self-serve” type process where consumers can make their choices as to information to be deleted. Requiring this two-step process could frustrate consumers. Companies should have the flexibility on process flow; in some cases it may make sense to have a two-step process, in other cases it may not.
3. Recommended Change:
 - a. Modify section 999.312(d): “A business ~~shall~~ may use a two-step process for online requests to delete where the consumer must first, clearly submit the request to delete and then second, separately confirm that they want their personal information deleted.”

X. SECTION 999.317 TRAINING; RECORD-KEEPING—CHAMBER PROPOSED CHANGES

A. ISSUE: RECORD-KEEPING REQUIREMENT DOES NOT ALIGN WITH PURPOSES OF CCPA.

1. Proposed Regulation: §999.317(g)
2. Problem with Proposed Regulation:
 - a. The CCPA does not impose the record-keeping requirements mentioned in this section.
 - b. It imposes an additional burden on businesses, does not appear tied to consumer benefits or rights, and it requires the collection of more personal information, thereby contravening the spirit of the CCPA. Imposing additional record-keeping and disclosure requirements on businesses that handle the personal information of four million or more consumers appears arbitrary. The CCPA already requires that businesses provide multiple disclosures to consumers, and this information is unlikely to give them a more meaningful understanding of their privacy protections.
 - c. Also, it is very unclear what would constitute a request that is “complied with” or “denied.” If a consumer could not be verified, how would that be characterized? What if the request was subject to a statutory exception? The lack of specificity will make this extremely challenging.
 - d. The release of metrics in the business’s privacy policy does not benefit consumers nor do the regulations provide any guidance relating to the calculation of the four million or more consumers.
3. Recommended Change:
 - a. The record-keeping requirements in section 999.317(g) should be struck.
 - b. Alternatively, if the effective date of the regulation is after January 1, 2020, revise the regulation to require recordkeeping information only after the date the regulations become effective. This requirement does not appear to be reflected in the statute, and it’s

unreasonable to require companies to begin collecting this information on January 1, 2020 if the regulations have not been finalized.

- c. Also, as an alternative to including the information in the privacy policy, these metrics should instead be provided to the AG upon request.
- d. If section 999.317(g) is kept, revise “median” to “average” because median is a difficult number to calculate.

XI. SECTION 999.316 REQUESTS TO OPT-IN AFTER OPTING OUT OF THE SALE OF PERSONAL INFORMATION—CHAMBER PROPOSED CHANGES

A. ISSUE: REGULATION’S TWO-STEP PROCESS CREATES UNNECESSARY FRICTION AND CONSUMER CONFUSION.

- 1. Proposed Regulation: §999.316(a)
- 2. Problem with Proposed Regulation:
 - a. This requirement is not consistent with other laws or with consumer expectations. It would require businesses to build new systems and to make users jump through unnecessary hurdles in order to express a preference. It appears to nudge consumers toward a course of action, rather than empowering them to make their own decisions in a straightforward manner.

Relatedly, it is burdensome and confusing to require this two-step, opt-in consent in situations in which a business may use personal information for additional purposes that are related to those that were disclosed to the consumer (§999.305(a)(3)). The CCPA deliberately adopts an opt-out regime rather than one that is opt-in, making this proposal inconsistent with the law. Furthermore, data protection principles typically do not require additional consent for the use of data that is consistent with the context in which the consumer receives the service.

The GDPR’s Article 6(4) allows further processing of personal data for compatible purposes, provided the controller puts safeguards in place. The proposed regulations would go beyond this requirement.

- b. Requires a two-step process: consumer requests to opt-in and then confirms opt-in. Businesses should be given flexibility concerning how consumers should use an opt-in process.
- 3. Recommended Change:
 - a. Strike the reference to a “two-step” process in section 999.316(a).

XII. SECTION 999.325 VERIFICATION FOR NON-ACCOUNTHOLDERS—CHAMBER PROPOSED CHANGES

A. ISSUE: SIGNED DECLARATION OF PERJURY REQUIREMENT IS UNNECESSARY.

- 1. Proposed Regulation: §999.325(c)
- 2. Problem with Proposed Regulation:
 - a. The language could be interpreted to require “a signed declaration under penalty of perjury” but there could be separate methods of verifying identity that are more reliable than a signed declaration in a business’s particular environment (e.g., blockchain or otherwise).

3. Recommended Change:
 - a. We recommend deleting Section 999.325(c).
 - b. In the event this request is not accepted, the language should be clarified to provide that a business may choose to execute or maintain “a signed declaration under penalty of perjury” or any other higher standard in order to verify requests.
 - c. In the alternative, revise Section 999.325(c): “A business’s compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury and/or any other information that the business determines in necessary to confirm that the requestor is the consumer whose personal information is the subject of the request. Businesses shall maintain all signed declarations as part of their record-keeping obligations.”

- B. ISSUE: REQUIREMENT THAT BUSINESSES PROVIDE TWO TIERS OF AUTHENTICATION FOR RIGHT TO KNOW REQUESTS IS OVERLY BURDENSOME AND NOT COMMON PRACTICE.
 1. Proposed Regulation: §999.325
 2. Problem with Proposed Regulation:
 - a. The requirement that businesses provide two tiers of authentication for right to know requests, depending on whether the request is for categories of specific pieces of personal information, would impose additional burdensome implementation requirements beyond the statute. This is not common practice for third party verification service providers.
 3. Recommended Change:
 - a. Strike section 999.325(c).

- C. ISSUE: TYPES AND THRESHOLD OF PERSONAL INFORMATION FOR VERIFIABLE REQUEST MAY LEAVE CONSUMERS VULNERABLE TO FRAUDULENT REQUESTS.
 1. Proposed Regulation: §999.325(c); 999.325(e); *see also* 999.323
 2. Problem with Proposed Regulation:
 - a. Concerns about feasibility and sufficiency. Name, SSN, DOB are commonly available. If those are provided to a business to request to know specific information (account numbers, for instance), and those data points match what the business has on a consumer, they could be providing the consumer’s account number to a fraudster who bought that identifying data on the web. A fraudster is not going to be deterred by a signed declaration under penalty of perjury.
 - b. Under Section 999.325(c), the requirement that businesses shall “generally avoid” requesting additional information from a consumer for the purposes of verification is at odds with the need to ensure verification.
 3. Recommended Change:
 - a. Strike section 999.325(c).

XIII. SECTION 999.308 PRIVACY POLICY—CHAMBER PROPOSED CHANGES

A. ISSUE: REQUIREMENT THAT BUSINESS PUBLICLY DESCRIBE VERIFICATION PROCESS SHOULD BE ELIMINATED OR SATISFIED BY GENERAL DESCRIPTIONS TO MITIGATE SECURITY RISKS.

1. Proposed Regulation: §999.308(b)(1); *see also* 999.313(a)
2. Problem with Proposed Regulation:
 - a. By requiring a business to publicly communicate how it will verify a consumer request, it could make it easier for an individual to impersonate another in an attempt to illegally collect consumer data. It would be best for each business to design a verification process that is communicated to an individual upon inquiry, and not posted for the public. This section is further made ambiguous by the proposed Section 999.313(a) which says that a business will confirm receipt of a request within 10 days and also provide information on the business's verification process. This latter situation seems the appropriate time/method to disclose such information—not the former and certainly not both on the website and within the private communication.
 - b. The requirement that a business describe the process used to verify consumer requests, including any information the consumer must provide, may be satisfied with a description at a high level of generality in order to mitigate security risks.
3. Recommended Change:
 - a. Strike section 999.308(b)(1)(c).
 - b. For consistency with Section 1798.130(a)(5)(C)(i) of the statute, revise regulation section 999.308(b)(1)(d)(2) to: "For each category of personal information collected, provide the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties ~~with to~~ whom the business ~~shares~~ sells personal information. The notice shall be written in a manner that provides consumers a meaningful understanding of the categories listed."

B. ISSUE: REGULATIONS SHOULD PROVIDE CLARIFICATION REGARDING THE REQUISITE LEVEL OF DETAIL TO DESIGNATE AN AUTHORIZED AGENT TO MAKE CONSUMER REQUESTS.

1. Proposed Regulation: §999.308(b)(5)(a);
2. Problem with Proposed Regulation:
 - a. The AG should clarify the level of detail required under Section 999.308(b)(5)(a) to explain how a consumer can designate an authorized agent for making requests.
3. Recommended Change:
 - a. Revise Section 999.308(b)(5)(a): "Explain generally how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf."

XIV. SECTION 999.318 REQUESTS TO ACCESS OR DELETE HOUSEHOLD INFORMATION—CHAMBER PROPOSED CHANGES

A. ISSUE: PROPOSED REGULATION DOES NOT ADDRESS CONCERN THAT HOUSEHOLD INFORMATION COULD BE DISCLOSED INCORRECTLY.

1. Proposed Regulation: §999.318(b)
2. Problem with Proposed Regulation:
 - a. Section 999.318(b) does not eliminate the risk that household information could be disclosed incorrectly because a business has no way of knowing whether the members of the household who have verified their identity are in fact all of the members of the household (i.e. if there's one member who's not there, a business might not know.)
 - b. The current definition of “household” in Section 999.318 is problematic and might cause businesses to provide data to members of households that might not have a right to see that data or delete that data. Businesses need further clarity regarding the security issue of providing data to household members that may not have a right to see or delete the data of other household members.
3. Recommended Change:
 - a. Revise Section 999.318(b): “If all consumers of the household jointly request access to specific pieces of information for the household or the deletion of household personal information, and the business can individually verify all the members of the household subject to verification requirements set forth in Article 4, then the business shall comply with the request. This obligation exists for businesses only if (i) all users have verified their identity, and (ii) they can verify that these are all of the members of the household.”

XV. SECTION 999.323 GENERAL RULES REGARDING VERIFICATION—CHAMBER PROPOSED CHANGES

A. ISSUE: INCREASED COMPLEXITY FOR VERIFICATION OF CONSUMERS.

1. Proposed Regulation: §999.323; 999.323(d)
2. Problem with Proposed Regulation:
 - a. Proposed regulations create a complicated process for verifying consumers: two data point match for categories, but three data point match and a signed declaration under penalty of perjury are required for specific pieces. If there is not enough information to verify for one purpose, a company must proactively determine whether there is enough to verify for another type of request, even if the consumer did not request it.
 - b. On the one hand, the amended statute says that businesses should use a verification process that makes sense given the sensitivity, etc. of the data at issue. On the other hand, the proposed regulations set forth a formulaic statement for verification (two data points versus three data points). Those two provisions need to be reconciled.
 - c. Section 999.323(d) is vague. What are “reasonable security measures to detect fraudulent identity-verification activity?”—this entire process will involve matching what consumers are willing to provide with incomplete data kept in business databases? How are businesses to determine reasonable security measures without more guidance from the AG?
3. Recommended Change:
 - a. Strike Section 999.323(d).

- a. The illustrative examples in Section 999.336(c) are ambiguous. This ambiguity and the confusing term “financial incentive” all point to the serious concerns about how loyalty programs will operate under the CCPA and whether loyalty programs should even be considered “financial incentive” in the first place, especially if a consumer will be inherently treated differently if their data is deleted from a loyalty program (won’t receive the same personalized discounts, points/reward removed, etc.)
- 3. Recommended Changes:
 - a. Remove 999.336(c)(2) illustrative Example 2.

XVIII. SECTION 999.337 CALCULATING THE VALUE OF CONSUMER DATA—CHAMBER PROPOSED CHANGES

A. ISSUE: PROPOSED REGULATIONS ARE INCONSISTENT WITH STATUTORY LANGUAGE.

- 1. Proposed Regulation: §999.337
- 2. Problem with Proposed Regulation:
 - a. Section 999.337 permits a business to offer a price or service difference if “reasonably related to the value of the consumer’s data.” The amended statute, as defined in CCPA Section 1798.125, allows financial incentives if “reasonably related to the value provided to the business by the consumer’s data.” These are inconsistent guidelines.
- 3. Recommend Change:
 - a. Strike Section 999.337.
 - b. In the alternative, align language with CCPA Section 1798.125 such that this regulation section reads “reasonably related to the value provided to the business by the consumer’s data.”

XIX. SECTION 999.330 MINORS UNDER 13 YEARS OF AGE—CHAMBER PROPOSED CHANGES

A. ISSUE: REGULATIONS SHOULD ALLOW FOR ANY METHOD PERMITTED BY COPPA FOR DISCLOSURE.

- 1. Proposed Regulation: §999.330(a)
- 2. Problem with Proposed Regulation:
 - a. The regulations should allow for any method permitted by COPPA for disclosure. This will allow for any new methods approved by the FTC to be also permitted under CCPA.
- 3. Recommended Change:
 - a. Revise Section 999.330(a) to simply be a reference to the methods approved by the FTC for disclosure.
 - b. Revise Section 999.330(a) to add Section 999.330(a)(2)(g): “Any other method of disclosure permitted by the Children’s Online Privacy Protection Act.”

XX. SECTION 999.331 MINORS 13 TO 16 YEARS OF AGE—CHAMBER PROPOSED CHANGES

- A. ISSUE: BUSINESSES THAT DO NOT PLAN TO SELL PERSONAL INFORMATION OF 13 TO 16 YEARS OLD SHOULD NOT NEED TO HAVE AN OPT-IN MECHANISM.
1. Proposed Regulation: §999.331(a)
 2. Problem with Proposed Regulation:
 - a. If a company does not plan to sell this personal information, they need not have an opt-in mechanism.
 3. Recommended Change:
 - a. Revise Section 999.331(a): “A business that has actual knowledge that it collects or maintains the personal information of minors at least 13 and less than 16 years of age, and wishes to sell such personal information, shall establish, document, and comply with a reasonable process for allowing such minors to opt-in to the sale of their personal information, pursuant to section 999.316.

EXHIBIT A

**TITLE 11. LAW
DIVISION 1. ATTORNEY GENERAL**

**CHAPTER 20. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS
PROPOSED TEXT OF REGULATIONS**

Article 1. General Provisions

§ 999.300. Title and Scope

- (a) This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as “these regulations.” These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have.
- (b) A violation of these regulations shall constitute a violation of the CCPA, and be subject to the remedies provided for therein.
- (c) A business whose operations are outside of California and that only collects a de minimus amount of personal information from California residents – such as a business with a domain .co.uk or .com.mx – are not required to comply with CCPA.
- (d) Businesses that operate outside of California and do not target their services to California residents are not covered.
- (e) The title shall not apply to a provider of health care governed by CMIA or HIPAA, to the extent the provider or covered entity collects personal information in connection with the provision or sale of health care-related products or services, and to the extent that the provider or covered entity maintains that personal information in a way that meets HIPAA Security Rule requirements.
- (b)(f) These regulations shall be operative on the effective date of January 1, 2021.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100-1798.199, Civil Code.

§ 999.301. Definitions

In addition to the definitions set forth in Civil Code section 1798.140, for purposes of these regulations:

- (a) “Affirmative authorization” means an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a child under 13, it means that the parent or guardian has provided consent to the sale of the child’s personal information in accordance with the methods set forth in section 999.330. For consumers 13 years and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

- (b) "Attorney General" means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General.
- (c) "Authorized agent" means a natural person or a business entity registered with the Secretary of State that a consumer has authorized to act on their behalf subject to the requirements set forth in section 999.326.
- (d) "Categories of sources" means types of entities from which a business collects personal information about consumers, including but not limited to the consumer directly, government entities from which public records are obtained, and consumer data resellers.
- (e) "Categories of third parties" means types of entities that do not collect personal information directly from consumers, including but not limited to advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers.
- ~~(f)~~ "CCPA" means the California Consumer Privacy Act of 2018, Civil Code sections 1798.100 *et seq.*
- ~~(g)~~ "Directly notify" means contacting the consumer directly with the required information, provided, however, that a business will have been deemed to directly notify a consumer of changes to its policies and practices if the notification is published and made available on its website for a sufficient period of time or other standard method of providing privacy policies and notices to consumers.
- ~~(h)~~ "Financial incentive" means a program, benefit, or other offering, including payments to consumers as compensation, for the disclosure, deletion, or sale of personal information.
- ~~(i)~~ "Household" means a person or group of people occupying a single dwelling.
- ~~(j)~~ "Notice at collection" means the notice given by a business to a consumer at or before the time a business collects personal information from the consumer as required by Civil Code section 1798.100(b) and specified in these regulations.
- ~~(k)~~ "Notice of right to opt-out" means the notice given by a business informing consumers of their right to opt-out of the sale of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations.
- ~~(l)~~ "Notice of financial incentive" means the notice given by a business explaining each financial incentive or price or service difference subject to Civil Code section 1798.125(b) as required by that section and specified in these regulations.
- ~~(m)~~ "Price or service difference" means (1) any difference in the price or rate charged for any goods or services to any consumer, including through the use of discounts, financial payments, or other benefits or penalties; or (2) any difference in the level or quality of any goods or services offered to any consumer, including denial of goods or services to the consumer. If an individual working for a broker or provider as a business partner opts out.

of the sale of personal information this will not prevent the continued relationship with a business.

~~(n)~~ “Privacy policy” means the policy referred to in Civil Code section 1798.130(a)(5), and means the statement that a business shall make available to consumers describing the business’s practices, both online and offline, regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their own personal information.

~~(o)~~ “Request to know” means a consumer request that a business disclose personal information that it has about the consumer pursuant to Civil Code sections 1798.100, 1798.110, or 1798.115. It includes a request for any or all of the following:

- (1) Specific pieces of personal information that a business has about the consumer;
- (2) Categories of personal information it has collected about the consumer;
- (3) Categories of sources from which the personal information is collected;
- (4) Categories of personal information that the business sold or disclosed for a business purpose about the consumer;
- (5) Categories of third parties to whom the personal information was sold or disclosed for a business purpose; and
- (6) The business or commercial purpose for collecting or selling personal information.

~~(p)~~ “Request to delete” means a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105.

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

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

~~(s)~~ “Third-party identity verification service” means a security process offered by an independent third party who verifies the identity of the consumer making a request to the business. Third-party verification services are subject to the requirements set forth in Article 4 regarding requests to know and requests to delete.

~~(t)~~ “Typical consumer” means a natural person residing in the United States.

~~(u)~~ “URL” stands for Uniform Resource Locator and refers to the web address of a

specific website.

(+)(v) “Verify” means to determine that the consumer making a request to know or request to delete is the consumer about whom the business has collected information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100-1798.199, Civil Code.

Article 2. Notices to Consumers

§ 999.305. Notice at Collection of Personal Information

(a) Purpose and General Principles

- (1) The purpose of the notice at collection is to inform consumers at or before the time of collection of a consumer’s personal information of the categories of personal information to be collected from them and the purposes for which the categories of personal information will be used.
- (2) The notice at collection shall be designed and presented to the consumer in a way that is easy to read and understandable to an average consumer. The notice shall:
 - a. Use plain, straightforward language and avoid technical or legal jargon.
 - b. Use a format that draws the consumer’s attention to the notice and makes the notice readable, including on smaller screens, if applicable.
 - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.
 - d. Be accessible to consumers with disabilities when required by the Americans with Disabilities Act of 1990, Pub. L. No. 101-336, 104 Stat. 328 (1990). At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.
 - e. Be visible or accessible where consumers will see it before any personal information is collected. For example, when a business collects consumers’ personal information online, it may conspicuously post a link to the notice on the business’s website homepage or the mobile application’s download page, or on all webpages where personal information is collected. When a business collects consumers’ personal information offline, it may, for example, include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to the web address where the notice can be found.
- (3) A business shall not use a consumer’s personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer’s personal information for a purpose that was not previously disclosed to

the consumer in the notice at collection, the business shall directly notify the consumer of this new use ~~and obtain explicit consent from the consumer to use it for this new purpose.~~

- (4) A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection.
 - (5) If a business does not give the notice at collection to the consumer at or before the collection of their personal information, the business shall not collect personal information from the consumer.
- (b) A business shall include the following in its notice at collection:
- (1) A list of the categories of personal information about consumers to be collected. Each category of personal information shall be written in a manner that provides consumers a meaningful understanding of the information being collected.
 - (2) For each category of personal information, the business or commercial purpose(s) for which it will be used.
 - (3) If the business sells personal information, the link titled “Do Not Sell My Personal Information” or “Do Not Sell My Info” required by section 999.315(a), or in the case of offline notices, the web address for the webpage to which it links.
 - (4) A link to the business’s privacy policy, or in the case of offline notices, the web address of the business’s privacy policy.
- (c) If a business collects personal information from a consumer online, the notice at collection may be given to the consumer by providing a link to the section of the business’s privacy policy that contains the information required in subsection (b).
- (d) A business that does not collect information directly from consumers does not need to provide a notice at collection to the consumer, but before it can sell a consumer’s personal information, it shall do either of the following:
- (1) ~~Contact~~ Directly notify the consumer ~~directly~~ to provide notice that the business sells personal information about the consumer and provide the consumer with a notice of right to opt-out in accordance with section 999.306; or
 - (2) Contact the source of the personal information to:
 - a. Confirm that the source provided a notice at collection to the consumer in accordance with subsections (a) and (b), ~~and~~
 - b. ~~Obtain signed attestations from the source describing how the source gave the notice at collection and including an example of the notice. Attestations shall be retained by the business for at least two years and made available to the consumer~~

Commented [SLD(1): We suggest deletion. In the alternative, the regulations should clarify that a business that receives personal information from an indirect source may comply with its CCPA obligations through contractual provisions that require other businesses to provide the requisite notice to consumers. The requirements to contact the source and obtain signed attestations are confusing and duplicative.

~~upon request.~~

Note: Authority: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.115, and 1798.185, Civil Code.

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

(a) Purpose and General Principles

- (1) The purpose of the notice of right to opt-out of sale of personal information is to inform consumers of their right to direct a business that sells ~~(or may in the future sell)~~ their personal information to stop selling their personal information, and to refrain from doing so in the future.
- (2) The notice of right to opt-out shall be designed and presented to the consumer in a way that is easy to read and understandable to an average consumer. The notice shall:
 - a. Use plain, straightforward language and avoid technical or legal jargon.
 - b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.
 - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.
 - d. Be accessible to consumers with disabilities. ~~when required by the Americans with Disabilities Act of 1990, Pub. L. No. 101-336, 104 Stat. 328 (1990). At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.~~

(b) A business that sells the personal information of a consumer shall provide a notice of right to opt-out to the consumer as follows:

- (1) A business shall post the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link on the website homepage or the download or landing page of a mobile application. The notice shall include the information specified in subsection (c) or link to the section of the business's privacy policy that contains the same information.
- (2) A business that substantially interacts with consumers offline shall also provide notice to the consumer by an offline method that facilitates consumer awareness of their right to opt-out. Such methods include, but are not limited to, printing the notice on paper forms that collect personal information, providing the consumer with a paper version of the notice, and posting signage directing consumers to a website where the notice can be found.
- (3) A business that does not operate a website shall establish, document, and comply with

another method by which it informs consumers of their right to direct a business that sells their personal information to stop selling their personal information. That method shall comply with the requirements set forth in subsection (a)(2).

- (c) A business shall include the following in its notice of right to opt-out:
- (1) A description of the consumer's right to opt-out of the sale of their personal information by the business;
 - (2) The webform by which the consumer can submit their request to opt-out online, as required by Section 999.315(a), or if the business does not operate a website, the offline method by which the consumer can submit their request to opt-out;
 - (3) Instructions for any other method by which the consumer may submit their request to opt-out;
 - (4) Any proof required when a consumer uses an authorized agent to exercise their right to opt-out, or in the case of a printed form containing the notice, a webpage, online location, or URL, where consumers can find information about authorized agents; and
 - (5) A link or the URL to the business's privacy policy, or in the case of a printed form containing the notice, the URL of the webpage where consumers can access the privacy policy.

- (d) A business is exempt from providing a notice of right to opt-out if:
- (1) It does not, ~~and will not~~, sell personal information collected during the time period during which the notice of right to opt-out is not posted; and
 - (2) It states in its privacy policy that that it does not ~~and will not~~ sell personal information. ~~A consumer whose personal information is collected while a notice of right to opt-out notice is not posted shall be deemed to have validly submitted a request to opt-out.~~

(e) Opt-Out Button or Logo

- (1) The following opt-out button or logo may be used in addition to posting the notice of right to opt-out, but not in lieu of any posting of the notice. [BUTTON OR LOGO TO BE ADDED IN A MODIFIED VERSION OF THE REGULATIONS AND MADE AVAILABLE FOR PUBLIC COMMENT.]
- (2) This opt-out button or logo shall link to a webpage or online location containing the information specified in section 999.306(c), or to the section of the business's privacy policy that contains the same information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

§ 999.307. Notice of Financial Incentive

(a) Purpose and General Principles

- (1) The purpose of the notice of financial incentive is to explain to the consumer each financial incentive or price or service difference a business may offer in exchange for the retention or sale of a consumer's personal information so that the consumer may make an informed decision on whether to participate. A financial incentive or price or service difference offered in connection with only collecting personal data but unrelated to a consumer's exercise of rights under CCPA does not require a notice of financial incentive.
- (2) The notice of financial incentive shall be designed and presented to the consumer in a way that is easy to read and understandable to an average consumer. The notice shall:
 - a. Use plain, straightforward language and avoid technical or legal jargon.
 - b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.
 - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.
 - d. Be accessible to consumers with disabilities when required by the Americans with Disabilities Act of 1990, Pub. L. No. 101-336, 104 Stat. 328 (1990). ~~At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.~~
 - e. Be available online or other physical location where consumers will see it before opting into the financial incentive or price or service difference.
- (3) If the business offers the financial incentive or price of service difference online, the notice may be given by providing a link to the section of a business's privacy policy that contains the information required in subsection (b).

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

- (1) A succinct summary of the financial incentive or price or service difference offered;
- (2) A description of the material terms of the financial incentive or price of service difference, ~~including the categories of personal information that are implicated by the financial incentive or price or service difference;~~
- (3) How the consumer can opt-in to the financial incentive or price or service difference;
- (4) Notification of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and
- ~~(5) An explanation of why the financial incentive or price or service difference is permitted under the CCPA.~~

~~a. A good faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and~~

~~b. A description of the method the business used to calculate the value of the consumer's data.~~

Formatted: Indent: Hanging: 0.31", Right: 0.71", Tab stops: 0.77", Left + Not at 1.08"

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.130, Civil Code.

§ 999.308. Privacy Policy

(a) Purpose and General Principles

- (1) The purpose of the privacy policy is to provide the consumer with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information. The privacy policy shall not contain specific pieces of personal information about individual consumers and need not be personalized for each consumer.
- (2) The privacy policy shall be designed and presented in a way that is easy to read and understandable to an ~~average typical~~ consumer. The notice shall:
 - a. Use plain, straightforward language and avoid technical or legal jargon.
 - b. Use a format that makes the policy readable, including on smaller screens, if applicable.
 - c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.
 - d. Be accessible to consumers with disabilities ~~when required by the Americans with Disabilities Act of 1990, Pub. L. No. 101-336, 104 Stat. 328 (1990). At a minimum, provide information on how a consumer with a disability may access the policy in an alternative format.~~
 - e. Be available in an additional format that allows a consumer to print it out as a separate document.
- (3) The privacy policy shall be posted online through a conspicuous link using the word "privacy," on the business's website homepage or on the download or landing page of a mobile application. If the business has a California-specific description of consumers' privacy rights on its website, then the privacy policy shall be included in that description. A business that does not operate a website shall make the privacy policy conspicuously available to consumers.

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

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

- a. Explain that a consumer has the right to request that the business disclose what personal information it collects, uses, discloses, and sells.
- b. Provide instructions for submitting a verifiable consumer request to know and provide links to an online request form or portal for making the request, if offered by the business.
- c. ~~Describe the process the business will use to verify the consumer request, including any information the consumer must provide.~~
- d. Collection of Personal Information
 1. List the categories of consumers' personal information the business has collected about consumers in the preceding 12 months. The notice shall be written in a manner that provides consumers a meaningful understanding of the information being collected.
 2. For each category of personal information collected, provide the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties ~~with to~~ whom the business ~~sells shares~~ personal information. The notice shall be written in a manner that provides consumers a meaningful understanding of the categories listed.
- e. Disclosure or Sale of Personal Information
 1. State whether or not the business has disclosed or sold any personal information to third parties for a business or commercial purpose in the preceding 12 months.
 2. List the categories of personal information, if any, that it disclosed or sold to third parties for a business or commercial purpose in the preceding 12 months.
 3. ~~State whether or not the business sells the personal information of minors under 16 years of age without affirmative authorization.~~

(2) Right to Request Deletion of Personal Information

- a. Explain that the consumer has a right to request the deletion of their personal information collected ~~or maintained~~ by the business.
- b. Provide instructions for submitting a verifiable consumer request to delete and provide links to an online request form or portal for making the request, if offered by the business.

- c. Describe the process the business will use to verify the consumer request, including any information the consumer must provide.
- (3) Right to Opt-Out of the Sale of Personal Information
- a. Explain generally that the consumer has a right to opt-out of the sale of their personal information by a business.
 - b. Include the contents of the notice of right to opt-out or a link to it in accordance with section 999.306.
- (4) Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights
- a. Explain that the consumer has a right not to receive discriminatory treatment by the business for the exercise of the privacy rights conferred by the CCPA.
- (5) Authorized Agent
- a. Explain generally how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf.
- (6) Contact for More Information: Provide consumers with a contact for questions or concerns about the business's privacy policies and practices using a method reflecting the manner in which the business primarily interacts with the consumer.
- (6)
- (7) Date the privacy policy was last updated.
- (8) If subject to the requirements set forth section 999.317(g), the information compiled in section 999.317(g)(1) or a link to it.

Formatted: Indent: Left: 0.77", No bullets or numbering

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.115, 1798.120, 1798.125 and 1798.130, Civil Code.

Article 3. Business Practices for Handling Consumer Requests

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

- (a) A business shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number, and if the business operates a website, an interactive webform accessible through the business's website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.
- (b) Subject to 999.312(a) above which shall be sufficient to comply with this section under all circumstances. A business shall provide two or more designated methods for submitting requests to delete. Acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a link or form available online through a business's

website, a designated email address, a form submitted in person, and a form submitted through the mail.

- (c) A business shall consider the methods by which it interacts with consumers when determining which methods to provide for submitting requests to know and requests to delete. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer, even if it requires a business to offer three methods for submitting requests to know. Illustrative examples follow:

- (1) *Example 1:* If the business is an online retailer, at least one method by which the consumer may submit requests should be through the business's retail website.

- (2) *Example 2:* If the business operates a website but primarily interacts with customers in person at a retail location, the business shall offer ~~three-two~~ methods to submit requests to know—a toll-free telephone number, and an interactive webform accessible through the business's website, ~~and-or~~ a form that can be submitted in person at the retail location.

- ~~(2)(3)~~ *Example 3:* If the business operates a website and interacts with customers in person at a retail location, but primarily collects data online (such as a travel company website), the business can offer two methods to submit requests to know—a toll-free telephone number and an interactive webform accessible through the business's website. In this case, a form that can be submitted in person at the retail location is not necessary.

Formatted: Widow/Orphan control, Tab stops: Not at 0.77"

Formatted: Font: 11 pt, Underline

- (d) A business ~~shall may~~ use a two-step process for online requests to delete where the consumer must first, clearly submit the request to delete and then second, separately confirm that they want their personal information deleted.

- (e) If a business does not interact directly with consumers in its ordinary course of business, at least one method by which a consumer may submit requests to know or requests to delete shall be online, such as through the business's website or a link posted on the business's website.

- (e)(f) A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

- ~~(f)~~ ~~If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either:~~

- ~~(1) Treat the request as if it had been submitted in accordance with the business's designated manner, or~~

- ~~(2) Provide the consumer with specific directions on how to submit the request or remedy any deficiencies with the request, if applicable.~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140, and 1798.185, Civil Code.

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

- (a) Upon receiving a request to know or a request to delete, a business shall confirm receipt of the request through either mail, email, or another notification method, within 10 days and provide information about how the business will process the request. The information provided shall describe the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request.
- (b) Businesses shall respond to complete requests to know and requests to delete within 45 days. The 45- day period will begin on the day that the business receives the request, unless the request is incomplete, or the consumer fails to provide information necessary to verify the request, regardless of time required to verify the request. If necessary, businesses may take up to an additional 45 days to respond to the consumer's request, for a maximum total of 90 days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.
- (c) Responding to Requests to Know
 - (1) For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the consumer that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (c)(2).
 - (2) For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall provide or direct the consumer to its general business practices regarding the collection, maintenance, and sale of personal information set forth in its privacy policy.
 - (3) A business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's or another consumer's account with the business, or the security of the business's systems or networks.
 - (4) A business shall not at any time disclose a consumer's Social Security number, driver's license number or other government-issued identification number, financial

account number, any health insurance or medical identification number, an account password, or security questions and answers. This subsection does not apply to requests seeking portability of information where such identifiers enumerated in section 999.313(c)(4) are necessary to support portability.

- (5) If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception pursuant to the CCPA, the business shall inform the requestor and explain the basis for its denial. provided however that a business shall be deemed to be in compliance with the requirement if bases for denial are set forth in its privacy policy and the business refers the consumer to its privacy policy. If the request is denied only in part, the business shall disclose the other information sought by the consumer.
- (6) A business shall use reasonable security measures when transmitting personal information to the consumer.
- (7) If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 4.
- (8) Unless otherwise specified, the 12-month period covered by a consumer's verifiable request to know referenced in Civil Code section 1798.130(a)(2) shall run from the date the business receives the request, regardless of the time required to verify the request.
- (9) In responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response to the consumer as required by the CCPA. It shall not refer the consumer to the businesses' general practices outlined in its privacy policy unless its response would be the same for substantially all or most consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories.
- (10) In responding to a verified request to know categories of personal information, the business shall provide for each identified category of personal information it has collected about the consumer:
 - a. The categories of sources from which the personal information was collected;
 - b. The business or commercial purpose for which it collected the personal information;
 - c. The categories of third parties to whom the business sold or disclosed the category of personal information for a business purpose; and or, as requested by the consumer.

d. The business or commercial purpose for which it sold or disclosed the category of personal information.

~~(11)~~ A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner, such as described in this section, that provides consumers a meaningful understanding of the categories listed.

~~(12)~~ A business need not additionally fulfill a consumer's request to provide categories of information collected if it is also providing specific pieces of information.

~~(13)~~ A business shall identify the personal information responsive to a request to know by conducting a commercially reasonable search of its records for documents that are responsive, considering the sensitivity of the personal information the business holds and the expense of compliance. A business does not violate the CCPA when it conducts a commercially reasonable search of its records in good faith but fails to identify a responsive record.

(d) Responding to Requests to Delete

(1) For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete.

The business shall inform the requestor that their identity cannot be verified ~~and shall instead treat the request as a request to opt out of sale.~~

(2) A business shall comply with a consumer's request to delete their personal information by:

- a. Permanently and completely erasing the personal information on its existing systems with the exception of archived or back-up systems;
- b. De-identifying the personal information; or
- c. Aggregating the personal information.

(3) If a business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the data on the archived or backup system is next accessed or used.

(4) In its response to a consumer's request to delete, the business shall specify the manner in which it has deleted the personal information.

(5) In responding to a request to delete, a business shall disclose that it will maintain a record of the request pursuant to Civil Code section 1798.105(d).

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

Commented [VBM(2): Priority recommendation would be to strike this provision entirely noting there are separate requests for separate reasons. In the alternative, recommendation would be to focus on a process for making an unverifiable request to delete become a verified request to delete

- a. Inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including any statutory and regulatory exception therefor, provided however, that a business shall be deemed to be in compliance with this requirement if the bases for denial are set forth in its privacy policy and the business refers the consumer to its privacy policy;
- b. Delete the consumer's personal information that is not subject to the exception; and
- c. Not use the consumer's personal information retained for any other purpose than provided for by that exception or any other exception pursuant to the CCPA.

(7) In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information only if a global option to delete all personal information is also offered, and more prominently presented than the other choices. The business shall still use a two-step confirmation process where the consumer confirms their selection as required by section 999.312(d).

(7)(8) A business shall identify the personal information responsive to a request to delete by conducting a commercially reasonable search of its records for documents that are responsive, considering the sensitivity of the personal information the business holds and the expense of compliance. A business does not violate the CCPA when, it conducts a commercially reasonable search of its records in good faith but fails to identify a responsive record.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

§ 999.314. Service Providers

- (a) To the extent that a person or entity provides services to a person or organization that is not a business, no obligations under CCPA shall apply to such person or entity and would otherwise meet the requirements of a "service provider" under Civil Code section 1798.140(v), that person or entity shall be deemed a service provider for purposes of the CCPA and these regulations.
- (b) To the extent that a business directs a person or entity to collect personal information directly from a consumer on the business's behalf, and would otherwise meet all other requirements of a "service provider" under Civil Code section 1798.140(v), that person or entity shall be deemed a service provider for purposes of the CCPA and these regulations.
- (c) A service provider shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider, without the agreement of such person, entity, or consumer, for the purpose of providing services that result in the sale of a consumer's personal information to another person or entity to a third party. A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, in order to provide the services specified in a contract with the business, or

to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.

- (d) If a service provider receives a request to know or a request to delete from a consumer regarding personal information that the service provider collects, maintains, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial. ~~The service provider shall also inform the consumer that it should submit the request directly to the business on whose behalf the service provider processes the information and, when feasible, provide the consumer with contact information for that business.~~
- (e) A service provider that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140, and 1798.185, Civil Code.

§ 999.315. Requests to Opt-Out

- (a) A business shall provide two or more designated methods for submitting requests to opt-out, including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information,” or “Do Not Sell My Info,” on the business’s website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information. The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should: (i) ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business; (ii) ensure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer, and does not require that the consumer provide additional information beyond what is necessary; (iii) clearly represent a consumer’s intent and be free of defaults constraining or presupposing such intent; and (iv) ensure that the opt-out preference signal does not conflict with other commonly-used privacy settings or tools that consumers may employ.
- (b) A business shall consider the methods by which it interacts with consumers when determining which methods consumers may use to submit requests to opt-out, the manner in which the business sells personal information to third parties, available technology, and ease of use by the average-typical consumer. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer.
- (c) If a business collects personal information from consumers online, the business ~~shall~~ may treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120

for that browser or device, or, if known, for the consumer, provided that the consumer undertakes an affirmative action to opt out of the sale of their information. Default opt-outs shall not constitute an affirmative step to opt out.

- (d) In responding to a request to opt-out, a business that sells personal information may present the consumer with the choice to opt-out of sales of certain categories of personal information as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices.
- (e) Upon receiving a request to opt-out, a business shall act upon the request as soon as feasibly possible, but no later than 15-30 days from the date the business receives the request.
- (f) ~~A business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the consumer's request that the consumer has exercised their right to opt out and instruct them not to further sell the information. The business shall notify the consumer when this has been completed.~~
- (g) A consumer may use an authorized agent to submit a request to opt-out on the consumer's behalf if the consumer provides the authorized agent written permission to do so. A business may deny a request from an authorized agent that does not submit proof that they have been authorized by the consumer to act on the consumer's behalf. User-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall may be considered a request directly from the consumer, not through an authorized agent if they represent the consumer's affirmative choice.
- (h) A request to opt-out need not be a verifiable consumer request. If a business, however, cannot verify the identity of a person making a request concerning personal information sold for purposes other than advertising or marketing, the business has a good faith, reasonable, and documented belief that a request to opt out is fraudulent, the business may deny the request. The business and shall inform the requestor that their identity cannot be verified. ing party that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent.

Note: Authority cited: Sections 1798.135 and 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140, and 1798.185, Civil Code.

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

- ~~(a) Requests to opt in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt in and then second, separately confirm their choice to opt in.~~
- (b)(a) A business may inform a consumer who has opted-out when a transaction requires the sale of their personal information as a condition of completing the transaction, along with instructions on how the consumer can opt-in.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, and 1798.185, Civil Code.

§ 999.317. Training; Record-Keeping

- (a) All individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA shall be informed of all the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.
- (b) A business shall maintain records of consumer requests made pursuant to the CCPA and how the business responded to said requests for at least 24 months.
- (c) The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.
- (d) A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.
- (e) Information maintained for record-keeping purposes shall not be used for any other purpose.
- (f) Aside from this record-keeping purpose, a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.

~~(g) A business that alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers, shall:~~

- ~~(1) Compile the following metrics for the previous calendar year:
 - a. The number of requests to know that the business received, complied with in whole or in part, and denied;
 - b. The number of requests to delete that the business received, complied with in whole or in part, and denied;
 - c. The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and
 - d. The median number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.~~
- ~~(2) Disclose the information compiled in subsection (g)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy.~~
- ~~(3) Establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests or the business's compliance with the~~

Commented [VBM(3): Alternatively, add to 317(g), "except as otherwise exempted under the CCPA" and amend 313(g)(1)(d) from "median" to "average" number of days.

~~CCPA are informed of all the requirements in these regulations and the CCPA.~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.135, and 1798.185, Civil Code.

§ 999.318. Requests to Access or Delete Household Information

- (a) Where a consumer does not have a password-protected account with a business, a business may respond to a request to know or request to delete as it pertains to household personal information by providing aggregate household information, subject to verification requirements set forth in Article 4.
- (b) If all consumers of the household jointly request access to specific pieces of information for the household or the deletion of household personal information, and the business can individually verify all the members of the household subject to verification requirements set forth in Article 4, then the business shall comply with the request. This obligation exists for businesses only if (i) all users have verified their identity, and (ii) they can verify that these are all of the members of the household.
~~(b)~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.140, and 1798.185, Civil Code.

Article 4. Verification of Requests

§ 999.323. General Rules Regarding Verification

- (a) A business shall establish, document, and comply with a reasonable method for verifying that the person making a request to know or a request to delete is the consumer about whom the business has collected information.
- (b) In determining the method by which the business will verify the consumer's identity, the business shall:
 - (1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section.
 - (2) Avoid collecting the types of personal information identified in Civil Code section 1798.81.5(d), unless necessary for the purpose of verifying the consumer.
 - (3) Consider the following factors:
 - a. The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive or valuable personal information shall warrant a more stringent verification process. The types of personal information identified in Civil Code section 1798.81.5(d) shall be considered presumptively sensitive;

Formatted: Indent: Left: 0.38", No bullets or numbering

- b. The risk of harm to the consumer posed by any unauthorized access or deletion. A greater risk of harm to the consumer by unauthorized access or deletion shall warrant a more stringent verification process;
 - c. The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be;
 - d. Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated;
 - e. The manner in which the business interacts with the consumer; and
 - f. Available technology for verification.
- (c) ~~A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however,~~ the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, and for security or fraud-prevention purposes. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 999.317.
- ~~(d) A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information.~~
- ~~(e)(d)~~ If a business maintains consumer information that is de-identified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request

Commented [VBM(4): Primary recommendation is to strike Section 999.323(d). In the alternative, recommendation is to revise the language as follows:

"A business shall implement reasonable security measures, as defined in guidance documents provided by the Attorney General, to detect fraudulent identity- verification activity and prevent the unauthorized access to or deletion of a consumer's personal information."

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140, and 1798.185, Civil Code.

§ 999.324. Verification for Password-Protected Accounts

- (a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 999.323. The business shall also require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data.
- (b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to know or request to delete until further verification procedures determine that the consumer request is authentic

and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 999.325 to further verify the identity of the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

§ 999.325. Verification for Non-Accountholders

- (a) If a consumer does not have or cannot access a password-protected account with the business, the business shall comply with subsections (b) through (g) of this section, in addition to section 999.323.
- (b) A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business, and/or any other information which the business has determined to be reliable for the purpose of verifying the consumer.
- (c) ~~A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer, together with a signed declaration under penalty of perjury and/or any other information that the business determines in necessary to confirm that the requestor is the consumer whose personal information is the subject of the request. Businesses shall maintain all signed declarations as part of their record-keeping obligations.~~
- (d) A business's compliance with a request to delete may require that the business verify the identity of the consumer to a reasonable degree or a reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion. For example, the deletion of family photographs and documents may require a reasonably high degree of certainty, while the deletion of browsing history may require a reasonable degree of certainty. A business shall act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with the regulations set forth in Article 4.
- (e) Illustrative scenarios follow:
 - (1) If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if the business maintains the consumer's name and credit card number, the business may require the consumer to provide the credit card's security code and identifying a recent purchase made with the credit card to verify their

Commented [SLD(5)]:

(1) The Chamber recommends deleting 999.325(c). In the event this request is not accepted, the language should be clarified to provide that a business may choose to execute or maintain "a signed declaration under penalty of perjury" or any other higher standard in order to verify requests.

OR, in the alternative

(2) A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury and/or any other information that the business determines in necessary to confirm that the requestor is the consumer whose personal information is the subject of the request. Businesses shall maintain all signed declarations as part of their record-keeping obligations.

identity to reasonable degree of certainty.

- (2) If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the non-name identifying information. This may require the business to conduct a fact-based verification process that considers the factors set forth in section 999.323(b)(3).
- (f) If there is no reasonable method by which a business can verify the identity of the consumer to the degree of certainty required by this section, the business shall state so in response to any request and, if this is the case for all consumers whose personal information the business holds, in the business's privacy policy. The business shall also explain why it has no reasonable method by which it can verify the identity of the requestor. The business shall evaluate on a yearly basis whether such a method can be established and shall document its evaluation.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

§ 999.326. Authorized Agent

- (a) When a consumer uses an authorized agent to submit a request to know or a request to delete, the business may require that the consumer:
 - (1) Provide the authorized agent written permission to do so; and
 - (2) Verify their own identity directly with the business.
- (b) This section permits businesses to require (1) instruction directly from the consumer regarding agent authorization, (2) the agent to make requests only after accessing the consumer's account, and (3) return personal information only through the consumer's account (rather than to the agent directly).
- ~~(b)~~
- (c) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4000 to 4465.
- (d) A business may deny a request from an agent that does not submit proof that they have been authorized by the consumer to act on their behalf.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

Article 5. Special Rules Regarding Minors

§ 999.330. Minors Under 13 Years of Age

- (a) Process for Opting-In to Sale of Personal Information

Commented [SLD(6)]: In the alternative, the AG's office should provide more detailed guidance on the minimum level of proof a business should obtain regarding agent authorization and an express safe harbor for businesses that meet that level of proof. The concern here is that the current regulations provide inadequate guidance for businesses to follow and thereby could subject consumers' privacy to risks.

- (1) A business that has actual knowledge that it collects or maintains the personal information of children under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. This affirmative authorization is in addition to any verifiable parental consent required under the Children’s Online Privacy Protection Act, 15 U.S.C. sections 6501, *et seq.*
- (2) Methods that are reasonably calculated to ensure that the person providing consent is the child’s parent or guardian include:
 - a. Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;
 - b. Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;
 - c. Having a parent or guardian call a toll-free telephone number staffed by trained personnel;
 - d. Having a parent or guardian connect to trained personnel via video-conference;
 - e. Having a parent or guardian communicate in person with trained personnel; ~~and~~
f. Verifying a parent or guardian’s identity by checking a form of government-issued identification against databases of such information, where the parent or guardian’s identification is deleted by the business from its records promptly after such verification is complete and;
f.g. Any other method permitted by the Children’s Online Privacy Protection Act (COPPA).

- (b) When a business receives an affirmative authorization pursuant to subsection (a) of this section, the business shall inform the parent or guardian of the right to opt-out at a later date and of the process for doing so on behalf of their child pursuant to section 999.315.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, and 1798.185(a)(6), Civil Code.

§ 999.331. Minors 13 to 16 Years of Age

- (a) A business that has actual knowledge that it collects or maintains the personal information of minors at least 13 and less than 16 years of age, and wishes to sell such personal information, shall establish, document, and comply with a reasonable process for allowing such minors to opt-in to the sale of their personal information, pursuant to section 999.316.
- (b) When a business receives a request to opt-in to the sale of personal information from a minor at least 13 and less than 16 years of age, the business shall inform the minor of the right to opt-out at a later date and of the process for doing so pursuant to section 999.315.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, and 1798.185, Civil Code.

§ 999.332. Notices to Minors Under 16 Years of Age

- (a) A business subject to section 999.330 and 999.331 shall include a description of the processes set forth in those sections in its privacy policy.
- (b) A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell the personal information of such minors without their affirmative authorization, or the affirmative authorization of their parent or guardian for minors under 13 years of age, is not required to provide the notice of right to opt-out.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, and 1798.185, Civil Code.

Article 6. Non-Discrimination

§ 999.336. Discriminatory Practices

- (a) A financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations.

(b) Notwithstanding subsection (a) of this section, a business may offer a price or service difference if it is reasonably related to the value provided to the business by the consumer's data of the consumer's data as that term is defined in section 999.337.

~~(c)~~ A business may require (1) instruction directly from the consumer regarding agent authorization; (2) the agent to make requests only after accessing the consumer's account; and (3) return personal information only through the consumer's account (rather than to the agent directly).

~~(d)~~ Illustrative examples follow:

(1) *Example 1:* A music streaming business offers a free service and a premium service that costs \$5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale of their personal information, then the practice is discriminatory, unless the \$5 per month payment is reasonably related to the value of the consumer's data to the business.

~~(2) *Example 2:* A retail store offers discounted prices to consumers who sign up to be on their mailing list. If the consumer on the mailing list can continue to receive discounted prices even after they have made a request to know, request to delete, and/or request to opt out, the differing price level is not discriminatory.~~

~~(e)~~ A business's denial of a consumer's request to know, request to delete, or request to opt-out for reasons permitted by the CCPA or these regulations shall not be considered

discriminatory.

~~(e)(f)~~ A business shall notify consumers of any financial incentive or price or service difference subject to Civil Code section 1798.125 that it offers in accordance with section 999.307.

~~(f)(g)~~ A business's charging of a reasonable fee pursuant to Civil Code section 1798.145(g)(3) shall not be considered a financial incentive subject to these regulations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130, and 1798.185, Civil Code.

§ 999.337. Calculating the Value of Consumer Data

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

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130, and 1798.185, Civil Code.

Article 7. Severability

Commented [SLD(7): In the alternative, align language with CCPA 1798.125 such that this section reads "reasonably related to the value provided to the business by the consumer's data."

Formatted: Indent: Left: 0.77", No bullets or numbering

§ 999.341.

- (a) If any article, section, subsection, sentence, clause or phrase of these regulations contained in this Chapter is for any reason held to be unconstitutional, contrary to statute, exceeding the authority of the Attorney General, or otherwise inoperative, such decision shall not affect the validity of the remaining portion of these regulations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.145, 1798.185, and 1798.196, Civil Code.

Message

From: Kevin Gould [REDACTED]
Sent: 12/6/2019 9:37:05 PM
To: Privacy Regulations [PrivacyRegulations@doj.ca.gov]
Subject: California Consumer Privacy Act of 2018 -- Proposed Rulemaking Comment Letter
Attachments: California Consumer Privacy Act of 2018 Proposed Rulemaking Comment Letter.pdf

Thank you for the opportunity to provide written comments during the proposed rulemaking pertaining to the California Consumer Privacy Act of 2018. Please find attached a comment letter prepared by the American Bankers Association, the California Bankers Association, the California Mortgage Bankers Association, and the Mortgage Bankers Association. Please let us know if you have any questions. Thank you.



Kevin Gould
SVP, Director of Government Relations
California Bankers Association
1303 J Street, Suite 600 | Sacramento, CA 95814
[REDACTED]
Connect: [Website](#) | [Twitter](#) | [LinkedIn](#)



December 6, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

RE: California Consumer Privacy Act of 2018 – Proposed Rulemaking Comment Letter

Dear Attorney General Xavier Becerra:

The American Bankers Association (ABA), the California Bankers Association (CBA), the California Mortgage Bankers Association (California MBA), and the Mortgage Bankers Association (MBA) appreciate the opportunity to submit written comments in response to the proposed rulemaking undertaken by the California Department of Justice pertaining to the California Consumer Privacy Act of 2018 (CCPA).

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

CBA is a division of the Western Bankers Association, one of the largest banking trade associations and regional educational organizations in the United States. CBA advocates on legislative, regulatory and legal matters on behalf of banks doing business in the state of California.

California MBA is a California corporation operating as a non-profit association that serves members of the real estate finance industry doing business in California. California MBA's membership consists of approximately three hundred companies representing a full spectrum of residential and commercial lenders, servicers, brokers, and a broad range of industry service providers.

The Mortgage Bankers Association is the national association representing the real estate finance industry, an industry that employs more than 280,000 people in virtually every community in the country. Headquartered in Washington, DC, the association works to ensure the continued strength of the nation's residential and commercial real estate markets; to expand homeownership; and to extend access to affordable housing to all Americans. MBA promotes fair and ethical lending practices and fosters professional excellence among real estate finance employees through a wide range of educational programs and a variety of publications. Its membership of over 2,200 companies includes all elements of real estate finance: mortgage companies, mortgage brokers, commercial banks, thrifts, REITs, Wall Street conduits, life insurance companies, and others in the mortgage lending field.

As your office prepares to issue final regulations in accordance with the CCPA, we respectfully urge that you consider the following requests to clarify aspects of the proposed regulations and the CCPA. These requests should not be considered an effort to undermine the CCPA but rather they are intended to assist in clarifying aspects of the law as a means to enhance compliance for financial institutions.

ARTICLE 2: NOTICES TO CONSUMERS. (SECTIONS 999.305-999.308).

➤ **Notice at Collection of Personal Information. (Section 999.305).**

Section 999.305(a)(3) of the draft regulations requires explicit consent to use a consumer's personal information for a purpose that was not specifically included in the required notice provided to the consumer at the time of collection. Pursuant to Civil Code Section 1798.100(b) of the CCPA, the only requirement in these scenarios is to deliver another notice that is compliant with the same notice to provide a consumer when information is first collected. As such, there is no additional statutory requirement that the business obtain the explicit consent from the consumer, as now required in the proposed rule.

Accordingly, we believe that this provision impermissibly amends the statute in place of implementing the intent of the Legislature. Moreover, this requirement creates a conflict between the statute and the regulations. A financial institution that provides notice consistent with the requirements of the law may nonetheless be charged with violating the statute because the regulations provide that a "violation of these regulations shall constitute a violation of the CCPA, and be subject to the remedies provided for therein." Given that this concept of obtaining explicit consent for the use of a consumer's personal information for a new purpose goes beyond the text of the CCPA, we request that it be removed.

➤ **Notice of Right to Opt-Out of Sale of Personal Information. (Section 999.306).**

Section 999.306(d)(2) requires businesses to treat as an opt-out any collection of personal information where a "Do Not Sell My Personal Information" button is not present. Under Civil Code Section 1798.100, a business must notify consumers of the purposes for which their

and the personal information that the business disclosed for a business purpose. Further, as it relates to personal information that is sold, Civil Code Section 1798.115(a)(2) states specifically, that the business must disclose “the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.” This different treatment is a logical consequence of the fact that the statute gives consumers the right to opt-out of sale. A consumer exercising that right has an interest in knowing which information is sold to which third party. Because there is no right to opt-out of the collection or sharing of personal information for a business purpose, a lower level of granularity will provide a less complex and more meaningful disclosure to the consumer.

ARTICLE 3: BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS. (SECTIONS 999.312-999.318).

➤ **Responding to Requests to Know and Requests to Delete. (Sections 999.313).**

Section 999.313(c)(5) requires that a business must specifically disclose the basis for denying a request to know or a request to delete if the denial was based on a conflict with federal or state laws or an exception to the CCPA. This is understandable. However, Section 999.313(d)(6)(c), applicable to a denial of a request to delete, provides that the business is not permitted to use the consumer’s personal information for any other purpose than provided for by that exception. This restriction improperly prevents a business from using the consumer’s personal information for other lawful purposes including fighting fraud or even completing a consumer’s transaction if that reason was not included in the denial letter. Accordingly, we request that these provisions be removed from the regulation.

Section 999.313(d)(1) requires that where a business cannot verify the identity of a requester seeking deletion, the business shall instead treat the request as a request to opt-out of the business selling the consumer’s personal information. This form of automatic opt-out is inconsistent with the CCPA and could have the unintended consequence of opting out consumers who do not wish to opt-out of sales. Further, if the request is not from the named consumer, such a requirement could lead to businesses opting out the wrong consumer infringing on the rights of consumers who have not chosen to opt-out from a sale.

The CCPA goes into great length to explain and reiterate that the consumer’s right to opt-out requires an affirmative act by the consumer. Examples of the law’s intent may be found in Civil Code Sections 1798.120 and 1798.135. If a requestor’s identity cannot be verified, all that should be required is notifying the requestor, stating that more information is needed for verification. Since this provision in the proposed regulation is inconsistent with the corresponding provision in the CCPA and since consumers are adequately protected by existing law, we request that this provision be removed from the regulations.

Section 999.313(d)(2) provides three methods of complying with a consumer's request to delete their personal information: permanently and completely erasing, de-identifying, and aggregating. In complying with Section 999.313(d)(4), a business apparently must specify the manner in which it has deleted personal information by identifying one of these three methods. This requirement is burdensome, confusing, and irrelevant to consumers and we request that it be removed.

➤ **Requests to Opt-Out. (Section 999.315).**

Section 999.315(e) requires that a business must act on a consumer's request to opt-out of the sale of their personal information in no more than 15 days. This period of time is significantly less than the time period provided to a business responding to a request to know or delete (45 days). Where a consumer makes an opt-out request, particularly a consumer who has authorized another person to opt-out of sale on their behalf, this proposed 15-day deadline fails to provide sufficient time to confirm that the individual making the request has the proper authorization. We request that this provision be removed or the time extended to 45 days.

Section 999.315(f) requires a business to (i) notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the opt-out request, (ii) instruct them not to further sell the information, and (iii) notify the consumer when this has been completed. This requirement is inconsistent with the corresponding provisions in CCPA, wherein a business is only required to cease selling the information it has collected from the consumer. There is no corresponding provision in the CCPA that the business takes further action and notify all third parties in this regard. Since this provision in the regulation is inconsistent with the corresponding provision in CCPA and given that consumers are adequately protected by existing law, we request that this section be removed from the regulations.

Proposed regulations have introduced a new method for a consumer to opt-out that is not included in the CCPA. The concept of "user-enabled privacy controls" in Section 999.315(g) is entirely new. In this regard, the regulations recognize the use of "user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information..." This new requirement is inconsistent with the CCPA.

Existing law has established robust provisions on how a business must message the consumer's right to opt-out and provides acceptable methods to evidence the consumer's intent to opt-out. Moreover, there has been no opportunity to assess the meaningfulness of this concept or the value that this may offer to consumers. In addition, businesses may not be able to comply with this new requirement if there is no technological capability to track or respond to such browser plugins or similar mechanisms.

Since this provision in the regulation is inconsistent with the corresponding provision in CCPA and given that consumers are adequately protected by existing law, we request that this provision be removed from the regulations. In the alternative, we request that the effective date of this provision be delayed, thereby allowing businesses the opportunity to investigate the current technological status of the functionality of user-enabled controls, and an opportunity to make adjustments to ensure they can comply with the provision.

➤ **Training: Record-Keeping. (Section 999.317).**

Section 999.317(g) of the proposed regulations expand record-keeping obligations for businesses that buy, receive, sell or share the personal information of four million or more consumers. For companies who meet this threshold, the regulation requires releasing consumer request metrics in the business's privacy policy or posted on their website. This mandate is not derived from the existing law and does not benefit consumers. Nor do the regulations provide any guidance relating to the calculation of the four million consumers.

We urge that this provision be removed from the regulations or alternatively that these metrics not be released publicly in privacy policies, but instead be provided to your office upon request. Should this provision remain, the regulations should clarify that businesses are required to calculate the 4 million threshold and compile metrics based on consumers who have the right to make requests under the CCPA. Including consumers who are not eligible to make requests, as a result of existing CCPA exemptions, skews the results in a manner that would make the results meaningless.

➤ **Requests to Access or Delete Household Information. (Section 999.318).**

While the draft regulations in Section 999.318 attempt to offer guidance with respect to requests to know or delete personal information for "households," we remain concerned with these requirements.

While we support the clarification that a business may comply with an individual request for household personal information by providing only aggregate personal information, if the requestor does not have a password protected account, the proposed regulations still expose individuals to the release or deletion of their personal information without their knowledge and consent. Aggregation is helpful but is not sufficient to protect people if the household consists of only two or three people.

Moreover, the proposed regulations do not address how the business should respond if the requestor has a password protected account. The implication is that if the requestor has a password protected account, the business must provide the household personal information to the requestor, or delete household personal information. Likewise, we believe it is virtually impossible for a financial institution to determine whether all members of a household jointly request access or deletion, without a level of investigation into a particular household that

would be extraordinarily burdensome—if not impossible. Our members are concerned about the transient nature of households – spouses may separate, or adult children may return or leave the household – and there is no practical method for a financial institution to determine the makeup of the household when a request is received.

For these reasons, we urge the deletion of “household” from the definition of “personal information.” We believe the unauthorized disclosure or deletion of personal information by one household member is an unintended consequence of the CCPA.

If the final rule does not delete “household” from the definition of personal information or otherwise exempt businesses from disclosing personal information or deleting personal information for a household, we respectfully request that the final rule create a safe harbor from liability if the business follows the procedures in the final regulation regarding verification of requests for access to or deletion of household personal information.

We would further request additional clarity as to the aggregate data that must be provided to the requesting household. It seems that the household information to be disclosed pursuant to this provision is that which applies to, and subject to inspection by, the household as a whole. It is not intended to include specific categories or pieces of information pertaining to a specific individual consumer residing in that household.

ARTICLE 4: VERIFICATION OF REQUESTS. (SECTIONS 999.323-999.326).

- **Provide additional clarity around what is necessary, and what will be deemed in compliance, when authenticating a verifiable consumer request and include a safe harbor. (Sections 999.323-999.325).**

As part of routine transactions with consumers, financial institutions collect personal information in order to facilitate customer requests. Furnishing personal information to consumers purporting to exercise their rights under the CCPA, in response to a verifiable consumer request, may result in unintended risk and harm to the consumer, including misuse of personal information to perpetrate fraud and identity theft.

A business receiving a consumer’s request will need sufficient data from the consumer as a safeguard to ensure the information provided in return is associated with the requesting individual. Regulations established by the Attorney General should provide flexibility for a business to decline a consumer’s request where the data presented by the consumer is insufficient to authenticate a request. Further, in circumstances where limited information is provided by the consumer, a business endeavoring to authenticate a request should have flexibility, but not be required, to furnish non-sensitive personal information (excluding personal information that if disclosed would otherwise result in a data breach) to the consumer as a means to satisfy its compliance and to protect the consumer against fraud and identity theft.

- **Affirm that the CCPA does not apply to a covered entity's intellectual property and that a business is not required to reveal data infringing on the rights of others.**

In subdivision (a)(3) of Section 1798.185, the CCPA grants the Attorney General 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."

In this regard, we urge rulemaking that establishes an exception from the Act for intellectual property or for data that, if disclosed, would have an adverse effect on the rights or freedoms of others. The CCPA should not apply to information that is the protected intellectual property of a business, including information subject to copyright, patent, service mark and/or trade secret protections. A business should not be required to disclose 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, or any information derived from such process or analysis.

In considering this request, your office may wish to consider the approach taken in the European General Data Protection Regulation (GDPR) which places reasonable limitations on the consumer privacy right it grants. Both the intellectual property exclusion and the avoidance of infringement on the rights of others are embedded in the GDPR. We believe that there should be similar recognition in the CCPA of circumstances where a business' attempt to comply with a consumer's request would place it in the position of violating the rights of others or placing it in jeopardy with its competitors.

Given the authority granted to your office pursuant to subdivision (a)(3) of Section 1798.185, we request that the final regulations affirm that intellectual property should not be disclosed in response to a verifiable consumer request.

- **Grant an 18-month delayed effective date with respect to the regulations.**

We urge your office to specify a later effective date for the regulations, such as 18 months after the final regulations are issued. When the CCPA was enacted, businesses were granted 18 months from the legislation's passage to its effective date. This period of time was granted recognizing the complexity of the CCPA, the potential for additional statutory revisions given the speed for which the CCPA was advanced through the Legislature, and was an acknowledgment of the time necessary for businesses to develop compliance protocols to implement the statutory provisions.

Financial institutions have been actively engaged in due diligence and establishing policies and procedures for compliance with the CCPA. The regulations will require financial institutions to re-evaluate their policies and procedures and adapt where necessary. In order to revise any

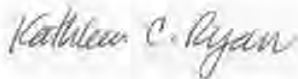
policies and procedures, financial institutions will require additional time to establish and test compliance procedures.

The authority for such as action may be found in Government Code section 11343.4(b)(2). That section provides that the agency issuing regulations can specify an effective date. In furtherance of this request, Section 11343.4(b)(1)'s limitations on an agency's ability to specify an effective date does not apply and that limitation only applies when the statute specifies an effective date.

Since the CCPA does not specify an effective date for the regulations and simply specifies that regulations should be adopted by July 1, 2020, with no reference to an effective date, we request an effective date for the regulations of no earlier than January 1, 2022.

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

Sincerely,



Kathleen C. Ryan
Vice President and Senior Counsel
American Bankers Association



Kevin Gould
SVP/Director of Government Relations
California Bankers Association



Susan Milazzo
Chief Executive Officer
California Mortgage Bankers Association



Pete Mills
Senior Vice President, Residential Policy &
Member Engagement
Mortgage Bankers Association