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

COMMENTS

of the

ASSOCIATION OF NATIONAL ADVERTISERS

on the

California Consumer Privacy Act Revised Proposed Regulations

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
2020 K Street, NW
Suite 660
Washington, DC 20006
202.296.1883

Counsel:
Stu Ingis
Mike Signorelli
Tara Potashnik
Allaire Monticollo
Venable LLP
600 Massachusetts Ave., NW
Washington, DC 20001
202.344.4613

February 25, 2020

On behalf of the Association of National Advertisers ("ANA"), we offer the following comments in response to the California Office of the Attorney General's ("CA AG") February 10, 2020 request for public comment on the revised proposed regulations implementing the California Consumer Privacy Act (the "CCPA").[1] We appreciate the opportunity to continue to engage with the CA AG on the important subject of consumer privacy and the content of the rules that will help implement the CCPA.

ANA is the advertising industry's oldest and largest trade association. ANA's membership includes nearly 2,000 companies, marketing solutions providers, charities and nonprofits, with 25,000 brands that engage almost 150,000 industry professionals and collectively spend or support more than $400 billion in marketing and advertising annually. Nearly every advertisement you'll see in print, online, or on TV is connected in some way to ANA members' activities. A significant portion of our membership is either headquartered or does substantial business in California.

ANA has closely followed the development of the CCPA through the legislative and regulatory process and has thoughtfully considered the impact the regulatory scheme will have on consumers and businesses. ANA participated in the CA AG's preliminary CCPA rulemaking forums in San Marcos on January 14, 2019 and Sacramento on February 2, 2019, and ANA submitted comments to the CA AG during the pre-rulemaking stage.[2] ANA also testified at a February 20, 2019 informational hearing on the CCPA held by the California State Assembly Committee on Privacy and Consumer Protection. In addition, ANA participated in the CA AG's December 4, 2019 San Francisco public hearing to offer input on the initial draft of proposed regulations implementing the CCPA, and ANA submitted written comments to the CA AG in response to the October 11, 2019 request for comment.[3]

We and our members strongly support the responsible use of data and the underlying goal of enhancing consumer privacy that is inherent in the CCPA and its implementing regulations. We are encouraged that the updated rules provide a degree of enhanced clarity surrounding some ambiguous provisions in the law. Nevertheless, the regulations remain significantly unclear in several areas of vital importance to both consumers and businesses.

The CCPA is a novel, operationally complex, and, in many ways, confusing law. The impending enforcement date of July 1, 2020 and the lack of final requirements for entities to implement make matters even more complicated and burdensome for businesses that are earnestly trying to develop processes to facilitate compliance with the CCPA. It is essential that the CA AG continue to work to provide more clarity to help ensure that consumers are given effective privacy protections and that businesses are equipped to structure systems and practices to offer those protections to consumers.

---

[1] California Department of Justice, *Updated Notice of Modifications to Text of Proposed Regulations and Addition of Documents and Information to Rulemaking File* (Feb. 10, 2020), located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-mod-020720.pdf?.

[2] *See* ANA, *California Consumer Privacy Act Regulation*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf at CCPA00000432 – 00000442.

[3] *See Comments of the Association of National Advertisers on the California Consumer Privacy Act Proposed Regulations*, located at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-comments-45day-pt2.pdf at CCPA_45DAY_00317 – 00342.

All of the topics we raise in the forthcoming comments represent issues that could have significant and detrimental impacts on consumers and businesses if they are not clarified by the CA AG. These issues, for example, could hinder consumers' ability to access programs, products, and services they enjoy and expect; thwart consumers' ability to make specific choices about entities' use of data in the marketplace; and impede the development of digestible and understandable privacy notices that appropriately inform consumers of business data practices. Moreover, the implementing regulations, as currently drafted, could impose significant costs on businesses and have a damaging impact on the California economy. We urge the CA AG to carefully consider the issues we address in these comments and to update the draft rules so they enhance consumer privacy and provide more clarity for businesses.

Our comments proceed by first addressing three issues of particular importance that we raised in prior submissions to the CA AG:

I. Provide Businesses a Reasonable Period of Time to Implement the New Regulations
II. Clarify Requirements Surrounding Loyalty Programs So Businesses May Continue to Offer Such Programs to Californians
III. Clarify that Businesses May Choose to Honor User-Enabled Global Privacy Controls *or* Provide Consumers Another, Equally Effective Method for Opting Out of Personal Information Sale

Next, we discuss other important issues that are created by certain provisions in the revised proposed regulations:

IV. Update the Household Definition to Better Reflect Appropriate Business Practices
V. Add a Provision Clarifying that Information Businesses Collect, Use, and Share for Fraud Prevention Purposes is Not Subject to Certain CCPA Rights
VI. Enable Flexibility for Providing the CCPA-Required Notice at Collection to Consumers Through the Telephone and in Person
VII. Remove New Duplicative and Unclear Transparency Requirements
VIII. Remove the Limitation on Service Providers' Internal Use of Personal Information

Finally, we reassert certain issues that we discussed in our initial comment submission to the CA AG on the content of the original proposed regulations. These issues remain unclear in the revised proposed rules and should be clarified by the CA AG issuing revisions to the proposed regulations:

IX. Clarify the Requirement to Obtain Parental Consent for Minors "in addition to" Verifiable Parental Consent Under the Children's Online Privacy Protection Act ("COPPA")
X. Remove the Requirement to "Permanently and Completely" Erase Personal Information
XI. Remove the Requirement to Provide a General Toll-Free Contact Number to Receive Consumer CCPA Requests

I. Provide Businesses a Reasonable Period of Time to Implement the New Regulations

Our members have taken significant steps to create policies, processes, and procedures to facilitate compliance with the CCPA. Although the law became effective on January 1, 2020, the lack of finalized regulations to implement the CCPA has left our members and thousands of other California businesses uncertain concerning their ultimate compliance obligations. Additionally, changes to the regulatory scheme so close to the law's enforcement date of July 1, 2020 could facilitate the creation of differing compliance processes and tools, which would confuse and frustrate consumers in their efforts to submit rights requests under the law. We therefore respectfully ask the CA AG to delay enforcement of the CCPA until January 2021 so entities that do business in California have enough time to implement the final rules' requirements to provide consumers with consistent and effective mechanisms for exercising their new rights under the law.

It is presently unclear when the draft rules will be finalized and whether they will be further amended. Just months before enforcement is scheduled to begin, companies that are subject to the CCPA are faced with the possibility that the draft rules could change from their present form for a second time and impose other entirely new requirements. If the rules are updated again, the ensuing public comment period of 15 or 45 days will further delay the finalization of the rules. Moreover, the rules will not be effective until they are submitted and reviewed by the California Office of Administrative Law, further reducing the time available to businesses to implement the final regulations. This timeline increases the likelihood that the draft rules will not be finalized before, or only a short period prior, to the law's July 1, 2020 enforcement date.

The CCPA is a novel and operationally complex legal regime that has already caused businesses across the country to incur significant costs to fulfill the consumer rights created by the law. Additionally, business attempts to comply with an incomplete legal regime risk causing significant consumer frustration and the implementation of inadequate or duplicative compliance tools. Furthermore, the most recent February 10, 2020 updates to the implementing regulations added additional content to the legal regime that businesses will need to consider and build into the processes they have already created for the CCPA.

While the statute itself instructs the CA AG to refrain from bringing an enforcement action before July 1, 2020, the office is not restricted from providing an additional reasonable period of time for California businesses to review and implement the final rules before enforcement begins. In order to avoid consumer frustration and business confusion with respect to the updated regulations, we request that you delay the enforcement of the law to begin in January 2021. This short forbearance will give businesses the time they need to comprehend and effectively implement the rules to help ensure consumers may appropriately benefit from the rights afforded under the CCPA.

II. Clarify Requirements Surrounding Loyalty Programs So Businesses May Continue to Offer Such Programs to Californians

The revised proposed regulations still contain significant and onerous requirements surrounding financial incentives that could threaten the viability of loyalty programs offered to California consumers. Specifically, the revised proposed regulations state that a business may offer a price or service difference to a consumer only if it is reasonably related to the value of the consumer's data.[4] According to the revised proposed rules, "[i]f a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference."[5] Additionally, businesses must disclose this good faith estimate of the value of the consumer's data and the method of computing such value in a notice of financial incentive.[6]

The draft rules do not provide any guidance regarding how a business may justify that a price or service difference offered through a loyalty program is reasonably related to the value of a consumer's data. The revised proposed regulations do not account for how businesses should quantify nontangible value in terms of fostering consumer loyalty and goodwill. In addition, the method by which a business values personal information associated with a consumer may vary situationally. For instance, it may depend on the discount being offered at a particular time or in a particular place. The actual value the business attributes to such data may, in many instances, be difficult or impossible to quantify.

From grocery rewards programs to beauty store points and drugstore cash back benefits to sandwich punch cards, consumers regularly and enthusiastically participate in vast and varied loyalty programs offered by brands and marketers. These programs enable consumers to receive more tailored offers and better prices for the goods and services they regularly receive. Businesses gain from the loyalty and brand trust they receive from consumers through their participation in these programs. Californians greatly benefit from loyalty and rewards programs and the price differences and discounts they receive for participating in those programs. Moreover, they expect to receive and participate in those programs alongside the rest of the American public. The revised regulations, as currently drafted, would significantly undermine loyalty programs in California and could very well force businesses to stop offering the programs in the state.

Making matters even more confusing is that businesses very regularly offer numerous price or service differences to consumers through loyalty and rewards programs at one time. For example, a coffee shop may offer participating loyalty program customers a punch card that gives the consumer a free coffee after the fifth punch on the card (representing a purchase of five coffees). The coffee shop may simultaneously offer 5% discounts on pastries purchased in the shop through the store's mobile application. If the "value of the consumer's data" does remain a constant number, it is unclear how the business may show that both incentives are reasonably related to the value of the consumer's data. The draft rules remain ambiguous on this point and

[4] Cal. Code Regs. tit. 11, § 999.336(b) (proposed Feb. 10, 2020).
[5] *Id*.
[6] *Id*. at § 999.307(d).

could therefore threaten to diminish loyalty programs in California due to business uncertainty in how to implement the proposed regulations' mandates.

The revised proposed rules still require businesses to disclose a good faith estimate of the value of the consumer's data and the method of calculating such value in a notice of financial incentive.[7] As ANA noted in its prior comment submission, requiring this information to be included in a consumer notice could reveal confidential information about a business that could jeopardize its competitive position in the market. Forcing businesses to reveal their proprietary, internal calculations and valuations in this fashion could have a negative impact on competition and pose significant risks to business proprietary information. Additionally, this valuation information and even the estimated value itself will be meaningless to consumers. A single business may offer several financial incentives to consumers through loyalty programs. Requiring businesses to make disclosures about their valuation methods and provide actual estimated values of consumer data for each financial incentive offered would overwhelm and inundate consumers with far too many notices without achieving the goal of providing meaningful information about business practices.

We respectfully ask the CA AG to clarify or remove the unreasonably onerous financial incentive requirements inherent in the revised rules, particularly the provisions requiring businesses to disclose a good faith estimate of the value of the consumer's data, disclose their methods of calculating such value, and ensure that financial incentives offered through loyalty programs are reasonably related to the value of the consumer's data. These provisions are exceedingly burdensome if not impossible to operationalize, and, if left unchanged, could have a chilling effect on the availability of loyalty programs offered in the state.

III. Clarify that Businesses May Choose to Honor User-Enabled Global Privacy Controls *or* Provide Consumers Another, Equally Effective Method for Opting Out of Personal Information Sale

The revised proposed regulations would require a business that collects personal information from consumers online to "treat user-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request…."[8] The requirement to honor browser signals and user-enabled privacy controls is not present in the text of the CCPA itself and exceeds the scope of the law. Consequently, businesses have had no ability to anticipate or prepare for this new obligation. In addition, because global privacy controls cast a single opt out signal to every business across the entire Internet ecosystem, the draft rules threaten to hinder consumers' ability to make specific, business-by-business choices about which entities can and cannot sell personal information. We ask the CA AG to clarify that businesses have the choice to honor user-enabled global privacy controls *or* provide consumers with another, equally effective method of opting out of personal information sale.

[7] *Id*. at § 999.307(b)(5).
[8] *Id*. at § 999.315(d).

In our prior comment submission, we explained that the unprecedented browser signal requirement certainly does not further the purposes of the law. In fact, the requirement to honor user-enabled privacy settings would thwart the informed and granular consumer choice that the CCPA endeavors to provide to California consumers. In the past, the California legislature considered global privacy controls and elected to refrain from enshrining them in law.[9] Requiring such settings to be honored now, therefore, would not be in line with legislative intent in passing the CCPA. Such a requirement would also be ripe for intermediary tampering with no way for businesses to authenticate whether a signal is a genuine consumer set preference. Intermediaries can inject signals into the marketplace and are able to change settings that may not accurately reflect a consumer's wishes. This capability has the potential to obstruct consumers' expressed choices. Furthermore, entities such as browsers and others can block the individualized signals set by consumers with various businesses. As noted in our prior submission, intermediaries are interfering with businesses using cookies, plugins, JavaScript and other technologies to maintain consumer preferences. Without preventing such interference, consumer preferences and choices cannot be respected.

Mandating that businesses honor user-enabled global privacy settings could have the unintended result of turning the CCPA's opt out regime into an opt in regime. After receiving a global privacy setting opt out signal, businesses would have no choice but to contact consumers on an individual by individual basis to see if they would like to opt in to sales of personal information to continue receiving the products and services they expect. In passing the CCPA, the California legislature set forth an opt out right to sales of personal information.[10] It was not the aim of the legislature to require consumers to opt in to every business's sale of personal information associated with them. As such, the user-enabled privacy control requirement would have the effect of thwarting legislative intent. Moreover, the draft rules do not clarify how businesses should operationalize consumers' subsequent requests to opt in to sales of personal information after a global privacy setting has been set. Browser-based global privacy settings would continue to broadcast opt out signals to businesses across the Internet in direct violation of the express opt in choice a consumer made with respect to a particular business. The regulations would limit a business's ability to seek "opt in" consent to once every twelve months. It is not clear how this restriction would affect the ability of companies to communicate with consumers in regard to these choices. The lack of clarity on this issue will likely hinder consumers' ability to make choices in the marketplace about data associated with them.

Although the CA AG's updates to the draft rules allow businesses to inform consumers if a global privacy control conflicts with a consumer's existing business-specific privacy setting and give the consumer the ability to indicate their intentions, this change does not fix the practical, consumer choice issues that are inherent in the requirement. This new term gives an advantage to certain businesses over others, particularly businesses that have a direct relationship with consumers through which they may confirm a consumer's choices. Certain entities who do not have a direct touchpoint with consumers will not have the ability to surface a notice to consumers asking if they intended to opt out of personal information sale. Additionally, as the revised proposed rules are presently drafted, businesses *must* treat user-enabled privacy controls as a valid request to opt out of personal information sale. Consequently, any subsequent

[9] *See* AB 370 (Cal. 2013).
[10] Cal. Civ. Code § 1798.120.

clarification the business receives from a consumer about their intentions to opt out would be too little too late; the business would have to honor the global privacy control, which would result in the consumer's loss of any number of products and services, as well as access to valuable content online. If the consumer did not intend to make such a selection, the business would not be able to reverse the effects of the opt out after complying with the mandated global privacy control.

A better approach to user-enabled privacy settings would be to adopt a rule allowing businesses that sell personal information to *either* (1) honor user-enabled privacy controls as valid requests to opt out, *or* (2) offer another effective mechanism for the consumer to submit a request to opt out, such as a "Do Not Sell My Info" link and an interactive form that enables the consumer to opt out of personal information sale. This approach would provide consumers with the ability to express individualized choices about particular entities' use of data. Updating the draft rules in this fashion would place the power and control back where it should be in the hands of consumers instead of concentrating it in the intermediary or browser that controls the global privacy control or setting. There is no privacy-enhancing reason to require businesses to respect user-enabled privacy controls over choice provided by a business.

IV. Update the Household Definition to Better Reflect Appropriate Business Practices

The revised proposed regulations set forth a new definition of the term household. Pursuant to the updated draft rules, a "household" is a person or group of people "who (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier."[11] While this definition represents an improvement from the definition that was in the original release of the draft rules, it still risks exposing consumer information to others. It also does not accurately reflect the way that businesses identify individuals who are part of the same household in the ordinary course of business. We therefore ask the CA AG to make slight alterations to the definition of household so it provides more protection for California consumers, better reflects the intent and purpose of the CCPA, and aligns with businesses' actual practices.

We suggest that the CA AG update the household definition to apply to a person or group of people who (1) reside at the same address, (2) share a common device, (3) share the same service provided by the business, and (4) are identified by the business as sharing the same group account or unique identifier. Without this change, consumers would be put at risk of having personal information associated with them exposed to other individuals in the household, including to individuals that do reside together who should not have access to such information. Providing data in response to a household request to know, for example, has risks of exposing data associated with a consumer to a person the consumer may not want to receive the information. Consumers should have the right to keep data associated with them private if they do not wish for that information to be shared with other individuals in their home. Updating the draft rules to better define "household" would consequently provide more privacy protection for consumers, thereby furthering the purposes of the CCPA. Moreover, this change to the definition of household would better reflect actual business practices in categorizing individuals as part of the same household. We therefore respectfully ask the CA AG to alter the definition of

[11] Cal. Code Regs. tit. 11, § 999.301(k) (proposed Feb. 10, 2020).

household so it better provides consumers living in the same household with the protections set forth in the CCPA and its implementing regulations.

V. Add a Provision Clarifying that Information Businesses Collect, Use, and Share for Fraud Prevention Purposes is Not Subject to Certain CCPA Rights

The revised proposed regulations do not address businesses' use of personal information for fraud prevention purposes, and the CCPA's exemptions do not provide a clear carve out for such activities to ensure that beneficial uses of data for fraud prevention can persist. The use of data for anti-fraud purposes provides consumers with considerable benefit by protecting them from harmful activities and making markets more efficient. We therefore request that the CA AG clarify that the fraud exemption to the deletion right applies to the collection, use, and sharing of personal information to create and distribute fraud prevention and detection tools. We also ask the CA AG to clarify that a similar exemption exists for the right to opt out of personal information sale so consumers may not prevent a business from sharing information necessary to detect fraudulent activity.

The fraud exemption to the CCPA's data deletion right applies to entities that "maintain the consumer's personal information in order to… protect against malicious, deceptive, fraudulent, or illegal activity."[12] As a result, the exemption covers the users of important fraud tools that are necessary for businesses to protect consumers from deceptive or illegal activity on their accounts, but it does not explicitly cover data suppliers that provide the information necessary to create vital fraud prevention services. This is because those data suppliers do not necessarily maintain the imperative information that makes fraud tools work in order to protect against fraudulent activity.

Additionally, there is no exemption to the opt out right for data that is used to prevent fraud, which could cause vital information that industry members use to detect fraud to be removed from the marketplace. Many businesses regularly use and share personal information for legitimate fraud prevention purposes, and this sharing of information benefits consumers by providing enhanced protection for the purchases, interactions, and services they undertake on a daily basis. Businesses' ability to connect, associate, and share personal information with partners for fraud prevention is imperative for helping to prevent and monitor fraudulent activity on consumers' accounts.

To clarify that the CCPA should not restrict the ability to gather information needed to create, provide, enhance, or deliver anti-fraud tools and services, we urge the CA AG to provide additional detail on the scope of the fraud exemption to the deletion right. We also ask the CA AG to clarify that such an exemption exists for the opt-out right in the CCPA. In particular, the CA AG should issue a rule clarifying that the CCPA fraud exemption to the consumer deletion right covers the collection, use, and sharing of personal information to create and distribute fraud prevention and detection tools. We also ask the CA AG to clarify that an analogous exemption exists for the opt out right so consumers may not opt out of a business's sharing of personal information for fraud prevention purposes.

[12] Cal. Civ. Code § 1798.105(d)(2).

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

The revised proposed regulations state that when a business collects personal information over the telephone or in person from consumers, the business may provide the CCPA-required notice at collection orally.[13] We respectfully ask the CA AG to clarify that businesses may satisfy the CCPA's notice at collection requirement by directing consumers to a physical or online location where they may find and read the applicable privacy notice.

Providing oral CCPA disclosures to consumers on the phone and in person would cause substantial friction in consumers' ability to seamlessly interact and transact with businesses. Furthermore, oral CCPA notices would significantly hinder consumers' ability to efficiently access products and services. For example, if a consumer transacts with a business and provides personal information to that business through the telephone, and if the business representative reads the consumer the business's CCPA-required notice at collection, the consumer will be forced to stay on the phone with a business for a much longer period of time than the consumer would have been required to prior to the effective date of the CCPA solely for the purpose of satisfying the business's legal obligations. This outcome will result in consumer frustration and will likely not serve the purpose of appropriately notifying consumers of the business's data practices.

We ask the CA AG to affirm that a business may direct a consumer to a privacy notice posted online or elsewhere in order to satisfy the notice at collection requirement when personal information is collected by a business on the phone or in person. Such an express clarification in the regulations will reduce the potential for significant inconvenience to consumers and will decrease the likelihood that consumers will be forced to listen to a privacy notice orally. This outcome would better serve the CCPA's ultimate goal of providing consumers with clear and understandable notice of the business's data collection and use practices.

VII. Remove New Duplicative and Unclear Transparency Requirements

The updates to the proposed regulations require a business that collects personal information from consumers' mobile devices to provide just-in-time notice of any data collection "that the consumer would not reasonably expect."[14] We ask the CA AG to remove this requirement, as it provides an indefinite standard that forces businesses to attempt to guess what a consumer would reasonably expect and as a result does not provide clear privacy protections for Californians. This rule is also unnecessary because the CCPA and the draft regulations already contain consumer notice requirements mandating that businesses provide specific disclosures about their data practices.

Requiring businesses that collect information from mobile devices to provide just-in-time notice of any data collection the consumer would not "reasonably" expect is a legal requirement that gives no clear instructions to businesses. Tying the requirement to a reasonable person standard will not provide strong, clear, or definite protections for consumers and will leave

[13] Cal. Code Regs. tit. 11, § 999.305(a)(3)(d) (proposed Feb. 10, 2020).
[14] *Id*. at § 999.305(a)(4).

entities guessing at a reasonable consumer's expectations. Businesses would have no way to clearly understand when such a notice would be required. It would be difficult if not impossible for businesses to understand what rises to the level of a data collection activity that is not reasonably expected by consumers. The CA AG should remove this directive to minimize the number of vague requirements included in the CCPA's implementing regulations. More clarity and less ambiguity will better ensure that Californians receive the privacy protections that are intended by the law.

Additionally, the law already requires businesses to notify consumers of the categories of personal information to be collected and the purposes for which such categories of personal information will be used in a notice at collection.[15] This mandate appears in both the proposed regulations and the CCPA itself. It is therefore duplicative for the CA AG to require businesses to notify consumers of data collection they would not reasonably expect, as the CCPA and the draft rules plainly state that a business must provide information about their data collection practices at or before the time period when data collection occurs. As a result, we suggest the CA AG remove the requirement from the proposed rules to provide just-in-time notice for mobile application data collection practices that a consumer "would not reasonably expect."

VIII. Remove the Limitation on Service Providers' Internal Use of Personal Information

The revised proposed regulations state that a service provider may not retain, use, or disclose personal information obtained in the course of providing services to a business unless a certain expressly listed exception in the draft rules applies.[16] One of the explicit exceptions listed in the draft rules is that a service provider may retain, use, or disclose personal information obtained in the course of providing services for internal use by the service provider to build or improve the quality of its services, "provided that the use does not include building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source…."[17] We respectfully ask the CA AG to remove this limitation on service providers' ability to internally use data to improve services, as building consumer profiles and engaging in data hygiene activities enable service providers to improve their offerings in ways that provide considerable value to consumers.

Service providers internally use the personal information they receive for a variety of beneficial purposes, including improving the ability of their services to detect fraudulent activity on a consumer's account. If service providers cannot internally use data to build or modify profiles to improve their services' ability to detect anomalies in consumers' purchases or account activities, consumers will no longer receive robust protection from fraud in the marketplace and may be hindered in their ability to receive alerts or information about potentially harmful or illegal activities that could impact them.

In addition, consumers benefit from the data hygiene activities service providers undertake to improve their services, as these activities help ensure that the offerings service

[15] Cal. Civ. Code § 1798.100(b); Cal. Code Regs. tit. 11, § 999.305(a)(1) (proposed Feb. 10, 2020).
[16] Cal. Code Regs. tit. 11, § 999.314(c) (proposed Feb. 10, 2020).
[17] *Id*. at § 999.314(c)(3).

providers bring to the market are working on the most accurate and up-to-date information. Data hygiene activities like change of address information ensure consumers receive information they want and avoid receiving messages they do not want. Moreover, data hygiene activities do not give marketers leads or identify customers for a brand; they simply enable entities to maintain accurate records, thereby bolstering data integrity. Data hygiene makes markets more efficient, and it ensures consumers do not receive inaccurate information or too much information. Removing service providers' ability to internally use personal information to better their products through cleaning data acquired from another source could cause data integrity issues and would severely limit the value and accuracy of the services that consumers receive and expect.

The CCPA itself already requires service providers to maintain contracts with businesses that limit their ability to use personal information for purposes outside of the services specified in the contract.[18] This statutory requirement provides consumers with considerable protection that personal information will not be used externally in a manner that is outside of the scope of the services requested. Service providers should be empowered to use personal information internally to improve their products and services without unreasonable limitations. We therefore urge the CA AG to remove the language in the draft rules stating that service providers cannot retain, use, or disclose personal information internally to build or modify household or consumer profiles or clean or augment data acquired from another source.

IX. Clarify the Requirement to Obtain Parental Consent for Minors "in addition to" Verifiable Parental Consent Under COPPA

The revised proposed regulations require a business that has actual knowledge it collects or maintains the personal information of children under thirteen to establish, document, and comply with a reasonable method for determining that a person affirmatively authorizing the sale of personal information about the child is the parent or guardian of the child.[19] The CA AG did not alter the requirement to obtain such affirmative authorization "in addition to" any verifiable parental consent required under COPPA in the most recent update to the draft rules.[20] We therefore renew our request for the CA AG to clarify that a business may satisfy this additional consent requirement by sending a single consent communication to a parent or guardian with separate consent requests or check boxes for CCPA and COPPA.

Although the CCPA notes that affirmative authorization to sell a child's information must be in addition to any verifiable parental consent obtained to comply with COPPA, the law provides no guidance on how a business may satisfy this additional consent requirement. It is unclear if this provision will be interpreted by the CA AG to require separate consent communications or if a business may use a single communication with multiple consents in order to satisfy the requirements of both laws. The lack of guidance also creates ambiguities when it comes to interpreting parents' choices, as it is unclear what should happen if a consumer consents to personal information sale under the CCPA but rejects personal information collection, use and/or disclosure under COPPA. The draft rules also do not address or seem to

[18] Cal. Civ. Code § 1798.140(v).
[19] Cal. Code Regs. tit. 11, § 999.330(a) (proposed Feb. 10, 2020).
[20] *Id*.

contemplate the fact that COPPA could potentially preempt the CCPA requirement to obtain affirmative authorization to sell personal information.

We urge the CA AG to clarify how the additional consent requirement should function in practice. Specifically, ANA asks the CA AG to confirm by rule that a business may provide a parent or guardian with a single consent communication that is acceptable under both the CCPA and COPPA. Such a clarification would help to consolidate the number of consent requests a parent or guardian may receive and field and would provide enhanced clarity regarding what is required from businesses under the CCPA.

X. Remove the Requirement to "Permanently and Completely" Erase Personal Information

The draft rules implementing the CCPA still state that a business may comply with a consumer's request to delete personal information by "permanently and completely erasing" the personal information on its existing systems.[21] While the draft rules also offer businesses the option of deidentifying or aggregating the data to satisfy a consumer's request to delete,[22] the "permanently and completely" erasing language could create compliance challenges for businesses that do not aggregate or deidentify data and may use certain database architectures that do not allow for permanent and complete deletion of information.

For certain businesses, it is a technical impossibility to "permanently and completely" delete all records. Certain records may remain in cold storage for extended periods of time, and it may not be possible for some businesses to remove certain "ghost" copies or files of such information. Moreover, a business taking steps to effectuate "permanent and complete" deletion could also conflict with the proposed regulations' existing requirements for businesses to maintain records of consumer requests.[23] We therefore request that the CA AG replace this provision with an option to refrain from using, processing, sharing, or disclosing personal information that a consumer requested to delete in the event that "permanent and complete" deletion is not possible. Such a change would still provide consumers with the same level of protection because it would ensure they have control over data and are able to limit its use and disclosure. This change would also help ensure businesses can comply with deletion requests in a way that their database systems allow and avoid technical violations of the law in responding to consumer requests to delete.

XI. Remove the Requirement to Provide a General Toll-Free Contact Number to Receive Consumer CCPA Requests

The CA AG did not address the toll-free number method of submitting CCPA requests in the revisions to the draft regulations. The proposed rules require certain businesses to provide a toll-free number as a method for receiving requests to know and state that a business may provide one for receiving requests to delete and opt out of personal information sale.[24] We ask

[21] *Id*. at § 999.313(d)(2)(a).
[22] *Id*. at §§ 999.313(d)(2)(b), (d)(2)(c).
[23] *Id*. at §§ 999.313(d)(5), 317(g).
[24] *Id*. at §§ 999.312(a), (b); 999.315(a).

the CA AG to remove the requirement to provide a toll-free number for receiving requests to know. Businesses incur extra costs to offer such numbers to the public. While larger companies may be able to absorb such costs, smaller and start-up businesses may have difficulty complying with the requirement to offer a toll-free number. The CCPA recognizes that certain businesses may need to operationalize the law in different ways due to their size or other practices. We ask the CA AG to extend that understanding to this requirement and clarify that businesses *may* offer a toll-free number as a method of submitting a request to know, but they are not required to offer a toll-free number. Such a clarification would help provide flexibility for the methods businesses may provide to consumers to submit requests to know.

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

The draft regulations still state that if "a business maintains personal information in a manner that is not associated with a named actual person, the business may engage in verification by requiring the consumer to demonstrate that they are the sole consumer associated with the non-name identifying information."[25] ANA asks the CA AG to clarify that businesses that do not already maintain information sufficient to verify a consumer's identity are not required to collect additional data from a consumer in an attempt to do so.

The CA AG's updates to the draft rules added an example stating that a business that collects personal information about a consumer through a mobile application but does not require the consumer to create an account may ask the consumer to provide additional information or respond to a notification sent to their device in order to verify the consumer's identity.[26] This example does not address situations when businesses do not maintain personal information that is associated with a named actual person. It also does not address how a business that does not have a direct relationship with a consumer could ask the consumer to verify their identity. For example, a consumer's provision of his or her name to a business in response to a business's request for additional information to verify the consumer's identity will not enable the business to verify the consumer if the business only holds information in a manner that is not associated with a named actual person. The draft rules are therefore unclear with respect to how a consumer's provision of any additional information could verify the consumer if the business only holds unique online identifiers or other information that a consumer would not reasonably know or be able to submit in order to verify their identity.

Moreover, because the non-name identifying information businesses may hold, such as unique online identifiers, could be associated with or encompass the information of multiple consumers, it may be impossible for a user to demonstrate that he or she is the sole consumer associated with non-name identifying information. For this same reason, requiring a consumer to respond to a notification sent to a device would similarly be an insufficient method of verifying identity. Because unique online identifiers may cover entire households, libraries, universities, and shared devices, they may be linked to personal information from many individuals. Additionally, any number of individuals may be able to access a given mobile

[25] *Id*. at § 999.325(e)(2).
[26] *Id*.

application and respond to the notification presented through it. As a result, the methods listed in the draft rules for businesses that do not maintain information associated with a named actual person to verify consumers are insufficient and do not provide any clarity regarding how businesses should field or respond to consumer CCPA requests.

For these reasons, ANA asks the CA AG to clarify that businesses that do not already maintain data sufficient to verify a consumer's identity are not required to collect additional data in an attempt to engage in verification. Without such a clarification, the draft rules may be perceived to impose an obligation on them to collect identifying information about consumers when they would not have chosen to do so in their normal course of business. This result is not privacy protective for consumers, as it facilitates the provision of additional consumer information to a business when the business does not want to receive such information and when receiving such information may do little to actually enable the business to verify the consumer's identity.

XIII. Clarify and Alter the Disclosures Required of Businesses that Buy, Receive, Sell, or Share Personal Information of 10 Million or More Consumers

The draft regulations require "[a] business that alone or in combination annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers" to disclose certain information in a privacy policy about their responses to CCPA requests.[27] ANA requests that the CA AG remove the phrase "for commercial purposes" from this provision. ANA also asks the CA AG to consider removing the privacy policy disclosure obligations from this provision and replacing them with a requirement to report such information to the CA AG upon request.

ANA asks the CA AG to remove the phrase "for commercial purposes" from this provision because it could be interpreted to include sharing personal information about a consumer with service providers. Such an interpretation could drastically increase the number of businesses that would be subject to this additional reporting requirement and is likely not in line with the CA AG's intent. Sharing information with service providers should not be within the scope of the calculation for determining whether a business is subject to the extra reporting requirements listed in Section 999.317(g) of the proposed rules. The CA AG should remove the phrase "for commercial purposes" from the text of that section to help clarify that sharing information with service providers should not count towards the 10 million consumer threshold listed in the provision.

Additionally, ANA asks the CA AG to reconsider the mandatory privacy policy disclosures associated with this requirement. Businesses subject to this additional reporting requirement must disclose in a privacy policy annual numbers of CCPA requests received, complied with in whole or in part, and denied, as well as information about the timeline within which the business typically responds to such requests. Obligating businesses to make such information public in a privacy policy will not provide consumers with information that will help them better understand the business's data practices. Also, the public nature of this information could have anticompetitive effects, as it would be visible to competitors and could potentially

[27] *Id*. at § 999.317(g).

reveal confidential or proprietary insights about the business. ANA therefore asks the CA AG to consider replacing the privacy policy aspects of this requirement with an obligation to maintain the same records and report them to the CA AG upon request. Making such an update to the draft rules would serve the purpose of protecting consumers by holding businesses accountable for meeting CCPA requests but would relieve the potential anticompetitive effects of requiring such disclosures in a privacy policy.

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

The proposed rules require a business to provide a privacy policy, a notice at collection, a notice of the right to opt out of the sale of personal information (if the business engages in sales), and a notice of financial incentive (if the business offers financial incentives or price or service differences to consumers).[28] The CA AG should clarify that a business may satisfy these consumer disclosure requirements by providing all of the necessary notices in a privacy policy accessible to consumers where required. Such a clarification would helpfully enable all privacy-related disclosures to be provided to consumers in one place, so consumers do not need to access many different pages or obtain various forms in order to receive important information about businesses' data practices. Giving consumers a centralized disclosure through which they may receive required privacy-related information will better enable consumers to review the information and refer back to it at a later date if they desire to do so. Specifically, we ask the CA AG to add a term to Section 999.304 stating that all of the required notices listed in that section may be provided in a privacy policy so long as they meet all of the content and other requirements set forth in Sections 999.305 through 999.308 of the proposed rules.

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

According to the draft rules, a business that operates a website must provide an interactive form accessible via an online link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info" to enable consumers to opt out.[29] However, information provided to businesses through such a webform may not actually enable the business to effectuate the consumer's opt out request. The CA AG should clarify that online businesses that do not maintain information in a manner that can identify a named actual person do not need to provide an interactive form for consumers to submit opt out requests and may instead use another effective method to allow consumers to submit a request to opt out, such as through other standard channels used for customer service.

While an interactive form may work efficiently for businesses that maintain personally identifiable information such as a consumer's name, email address, or postal address, an interactive form may not adequately enable a business that does not maintain personally identifiable information to facilitate an opt out. For example, businesses that hold unique online identifiers and do not associate personally identifiable information with such identifiers may not be able to process a consumer's opt out request if it is submitted through an interactive form. Additionally, consumers may not have access to these identifiers, so they may not be able to

[28] *Id*. at §§ 999.304 – 308.
[29] *Id*. at § 999.306(c)(2), 315(a).

submit any information that the business can use to verify the consumer's identity by matching the information the consumer provides to the information maintained in the business's systems.

The proposed regulations recognize that methods for submitting consumer rights requests may need to be different depending on the way the business interacts with a consumer. The rules should similarly address the differences that may be necessary for businesses that collect personally identifiable information and businesses that do not collect information that is associated with a named actual person. We therefore respectfully ask the CA AG to clarify that online businesses that do not maintain personally identifiable information or information in a manner that can identify a named actual person do not need to provide an interactive form for consumers to submit requests to opt out of personal information sale and may use another method, such as other common channels used for customer service, to enable a consumer to submit a request to opt out.

* * *

Thank you for the opportunity to provide input on the revised proposed regulations implementing the CCPA. We look forward to continuing to work with the OAG on these important matters. Please do not hesitate to contact us with any questions you may have regarding these comments.