Before the
California Department of Justice
Los Angeles, CA 90013

COMMENTS

of the

ASSOCIATION OF NATIONAL ADVERTISERS

on

The California Consumer Privacy Act

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
Tara Potashnik
Jared Bomberg
Venable LLP
600 Massachusetts Ave., NW
Washington, DC 20001
202.344.4613

March 8, 2019

California Consumer Privacy Act Comments

The Association of National Advertisers ("ANA") provides these comments in response to the California Attorney General's ("CA AG") request for public comment on the California Consumer Privacy Act ("CCPA").

ANA is the advertising industry's oldest trade association. ANA's membership includes nearly 2,000 companies and marketing solutions providers, 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 in print, online, or on TV is connected in some way to ANA members' activities. In California, advertising helps generate $767.7 billion (16.4% of the state's economic activity) and helps produce 2.7 million jobs (16.8% of all jobs in the state). ANA's members include a broad range of major national advertisers, leading marketing data science and technology suppliers, ad agencies, law firms, consultants, and vendors. We also count among our membership a large number of nonprofit organizations and charities that, while ostensibly exempted from the provisions of the CCPA, in fact, are significantly impacted by the CCPA, as they rely heavily on data and marketing to reach donors and carry out their missions. Many of ANA's members are headquartered in California or carry out significant business in the state.

ANA strongly supports the underlying goals of the CCPA. Privacy is an extraordinarily important value that deserves meaningful protections in the marketplace. As an industry, advertisers and marketers have taken a number of major steps to put these values into practice—investing multi-millions of dollars providing consumers greater control over data, transparency with respect to the collection, use and transfer of data, and implementing strong self-regulatory bodies and codes including the highly lauded Digital Advertising Alliance ("DAA") program to help ensure accountability in regard to privacy and fair practices in the marketplace.

As our members prepare to implement the CCPA, additional clarity regarding various provisions would help ensure compliance with the law and enhance consumer privacy. Such clarifications and interpretations fall specifically within the CA AG's regulatory authority provided under the law.[1] We urge the CA AG to issue regulations on the following matters:

Priority Issues for the California Attorney General to Address

1. Preserve Loyalty Discount Programs
2. Clarify the Rules for Consumer Requests by Authorized Representatives to Ensure that Consumers are Protected
3. Allow "Third Parties" to Rely on Written Attestations of "Explicit Notice"
4. Enable Granular Choices for Consumers Exercising CCPA Rights
5. Prevent the Need to Create an Ever-Expanding Multiplicity of Individualized Privacy Policies
6. Clarify "Household" in the Definition of "Personal Information"

[1] Cal. Civ. Code § 1798.185.

7. Clarify "Professional or Employment Related Information" in the Definition of "Personal Information"
8. Distinguish "Pseudonymized" Data from "Personal Information"
9. Clarify the "Cure" Requirement for Security Breaches

Key Additional Issues for the California Attorney General to Address

1. Clarify that Businesses Have Flexibility When Verifying Consumer Requests
2. Preserve Ad Measurement and Attribution Activities
3. Clarify the Scope of the "Publicly Available" Information Exclusion
4. Clarify the 12-Month Look-Back Provision
5. Limit the CCPA's Unintended Impact on Nonprofit Organizations, Including Charities
6. Preserve the Ability to Provide Expected Marketing Messages to Consumers
7. Ensure the Viability of the Fraud Exception
8. Clarify the Definition of "Business Purpose"
9. Clarify the Operative Ages in the Opt-In Requirement Related to Minors
10. Remove Backup Information from the Scope of a Deletion Request
11. Ensure that Businesses Do Not Have to Collect Extra Data to Comply with CCPA Requirements

I. Priority Issues for the California Attorney General to Address

This section identifies priority areas within the CCPA that would benefit from the CA AG's clarification, describes the real-world impacts of these issues, cites the CA AG's statutory authority for addressing such issues through regulation, and provides suggestions for the content of such rules.

1. Preserve Loyalty Discount Programs

The CCPA prohibits price and service "discrimination," among other practices, against consumers who have exercised their CCPA rights, but it creates these prohibitions with imprecise drafting that could be interpreted to prohibit traditional loyalty discount programs.[2] Loyalty discount programs could be considered a discriminatory practice under the CCPA because these programs create different price levels between consumers. Consumers who make deletion or opt-out requests of their data restrict the very data that allows them to participate in a loyalty program. As a result, those consumers who choose not to participate in a loyalty program will automatically be treated differently than other consumers in the program. This difference in treatment could run afoul of the ambiguous wording in the law, which states in one section that

[2] The CCPA states: "A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including… by:… [c]harging different prices or rates for goods or services, including through the use of discounts or other benefits imposing penalties…. Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data." Cal. Civ. Code §§ 1798.125(a)(1)-(2).

these programs must be "reasonably related" to the value provided to the consumer, while the law states in another section that these programs must be "directly related" to the value provided to the consumer.[3] Confusion exists as to which standard applies, and the law provides no additional guidance on how to measure whether a program is reasonably or directly related to the value provided to consumers.

Without clarification, many loyalty programs could cease altogether when the CCPA becomes effective. Loyalty programs allow businesses to maintain and foster positive relationships with consumers. They provide consumers significant benefits in the form of lower prices and access to special offers. The vast number of consumers, including a broad range of California consumers, who have and are voluntarily participating in loyalty programs over many years demonstrates the popularity and value these programs provide. ANA therefore asks the CA AG to permit a business to offer loyalty-based discount programs that consumers value and expect without the program constituting discrimination under the CCPA. For instance, we ask that the CA AG interpret "reasonably related" and "directly related" to the value provided to consumers to include the collection, use, and sharing of any data that is needed to provide a loyalty discount program and other consumer benefits.[4] Consumers that provide such data to participate in a loyalty program would obtain value through the loyalty program that is reasonably and directly related to the value of the consumer's data because without the consumer's data, the loyalty program would not be possible. Such clarification would help ensure the continued use of loyalty programs under the CCPA.

2. Clarify the Rules for Consumer Requests by Authorized Representatives to Ensure that Consumers are Protected

The CCPA allows individuals and entities to make access, deletion, or opt-out requests on behalf of consumers, so long as such parties' actions constitute a "verifiable consumer request" under the law.[5] However, the CCPA is silent on whether these authorized representatives of consumers must inform consumers of the implications and outcomes of exercising their CCPA choices with respect to the personal information held by a particular business. As such, a third-party requestor could choose not to provide relevant information to a

[3] *Compare* Cal. Civ. Code § 1798.125(a)(2) ("reasonably related") *with* Cal. Civ. Code § 1798.125(b)(1) ("directly related").

[4] The CA AG has authority to issue regulations to "further the purposes of [the] title." Cal. Civ. Code §§ 1798.185(a), (b). The clarification we seek would further the purposes of the title because the current provision related to discrimination and the acceptable uses of customer incentives is: (a) vague and (b) may conflict with Section 1798.145 of the law, which states "[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." Cal. Civ. Code § 1798.145(j). Without the clarification we propose or a similar clarification, many loyalty programs would cease altogether, which would adversely affect the rights of other consumers who wish to participate in and receive the benefits of such programs.

[5] The CCPA states: "Verifiable consumer request" means a request that is made by a consumer… or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to regulations adopted by the CA AG pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information." Cal. Civ. Code § 1798.140(y).

consumer concerning the implications of exercising CCPA rights, which would impede the consumer's ability to make an informed choice because the consumer would not have necessary information. Furthermore, the CCPA is silent on whether authorized representatives must have any particular qualifications or make any representations about the use(s) they will make of the consumer data they receive. It is possible that an authorized representative with no relevant qualifications for handling consumer requests could make a request on behalf of a consumer without fully informing the consumer of the implications of making such a request. Such authorized representatives could also manipulate information presented to consumers to attempt to influence a consumer's decision on whether to make a request. This is not a theoretical concern—ANA members have had to combat unauthentic consumer requests by third parties allegedly acting on behalf of consumers under current privacy standards—but a present challenge that will increase significantly without guidance from the CA AG. Consumer choice works when the choice by consumers is informed. When businesses stand in between the consumer and the business that must carry out the request, the choice model is placed at risk because it is not clear what information will be presented to the consumer to trigger their choice and whether they effectively communicate those choices.

To serve as an authorized representative for a consumer request under the CCPA, we suggest that the CA AG issue a rule that the authorized representative must properly inform a consumer of their choices and the implications of exercising such choices (*e.g.*, no longer receiving new offers from the business).[6] This notification requirement is important because the business that ultimately must comply with the request may not be able to directly discuss potential impacts of the request with the consumer. For a business to obtain verifiable consumer consent, a consumer must be properly informed of choices. We also request that the CA AG issue a rule creating specific requirements for authorized representatives who gather and facilitate consumer CCPA requests and consider whether the business is serving the public interest or is manipulating consumers, or not effectuating their choices. For instance, the rule would require an authorized representative to obtain a consumer's written authorization detailing what requests will be made what the implications of those requests are, and how any data collected from the consumer will be used; the CA AG would conduct oversight over these entities.

3. Allow "Third Parties" to Rely on Written Attestations of "Explicit Notice"

The CCPA prevents a third party that has received consumer personal information from a business (and not consumers directly) from selling such personal information unless the consumer has received "explicit notice" and is provided an opportunity to exercise the right to opt out.[7] The CCPA does not define "explicit notice" or clarify how third-party companies that do not have a direct relationship with consumers must provide such notice. As a result, if the law

[6] The CA AG has authority to issue this clarification pursuant to Cal. Civ. Code § 1798.185(a)(7), which allows him to establish "rules and procedures… to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130…." By clarifying the meaning of a verifiable consumer request, the CA AG would facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to the regulatory authority listed in the law.

[7] Cal. Civ. Code § 1798.115(d).

is interpreted to require third parties to provide direct notice to consumers before selling covered information, third parties may not be able to do so and would be prevented from selling such data. This outcome could impact sales of data that have no privacy implications and that are necessary to deliver products and services that consumers value, or that would protect against fraud. In these circumstances, third parties ought to be able to rely on their data providers to ensure the CCPA-required "explicit notice" is given, as those data providers have a direct relationship with consumers or should have knowledge of whether legal obligations have been met. The law should recognize that written assurances from the provider of the data, along with explicit notice on a website by the receiver of the data, is a sufficient compliance approach under the circumstances.

We urge the CA AG to clarify the "explicit notice" requirement for third parties to ensure that a third party can rely on written attestations of compliance when receiving data from other businesses.[8] Businesses that rely on written attestations of compliance also should be required to make the same disclosures to consumers in their online privacy policy representations. With this interpretation of the statute, consumers will have better access to the information contemplated in the explicit notice requirement because contractual representations and warranties mandated by this interpretation will help ensure that appropriate disclosures are provided to consumers. Also, requiring businesses that receive information down the chain to place consumer disclosures in their online privacy policies would advance the intent behind the "explicit notice" requirement. Without this interpretation, third parties will be forced to operate as first parties in the digital ecosystem, which may be impossible for many third parties that have no direct relationship with consumers and no clear way to create such a relationship. As a result, many third parties may no longer be able to operate, which could substantially unravel the seamless nature of the Internet that consumers rely upon. In particular, many products and services in the digital economy that consumers value, including anti-fraud products that rely on consumer data to identify fraudulent activity, could be jeopardized because the data transfers by third parties without a direct consumer relationship needed to create or deliver those products would be prohibited.

4. Enable Granular Choices for Consumers Exercising CCPA Rights

The CCPA allows consumers to access all of their personal information, entirely opt out of the sale of their data, or entirely delete their data from businesses' systems.[9] The law, however, does not explicitly state that a business may allow a consumer the choice to access, delete, or opt out from the sale of *some, but not all*, of their data. As a result, a consumer request may be interpreted to cover all of the consumer's data even though a consumer only wants part of their data deleted or restricted from further sharing. This issue is especially challenging when

[8] The CA AG has authority to interpret the "explicit notice" provision pursuant to Cal. Civ. Code § 1798.185(a)(7), which contemplates rules to "facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130." Third parties should be required to provide an online opt-out notice and be allowed to ensure through contractual commitments from data providers that proper CCPA disclosures were made to consumers. Such activities will help ensure that opt-out notices and instructions are provided to consumers by the entities that have a direct relationship with them. The CA AG also has authority to interpret this provision pursuant to his general authority to issue rules "as necessary to further the purposes of [the] title." Cal. Civ. Code §§ 1798.185(a), (b).

[9] Cal. Civ. Code §§ 1798.100, 105(c), 110, 115, 120(a).

a company has multiple products or services with consumer information or multiple subsidiaries that interact with the same consumer. Determining what data sets a consumer refers to in a consumer request can be complex, and this job is made harder by vague consumer requests and by third parties acting as authorized representatives who may not know exactly what the consumer wishes to be deleted or restricted from sharing.

We ask that the CA AG clarify that consumers may have the option to choose the types of sales they want to opt out of or the types of data they want deleted instead of mandating one all-or-nothing opt-out or deletion requirement.[10] Consumers may wish to make granular choices regarding the use and maintenance of their data, and a regulation clarifying that such granularity is permissible should be issued. Paradoxically, failure to take this step may undermine privacy protections because a consumer may decide not to restrict any use of his data by a company if the consumer is only concerned about specific limited uses of his information.

5. Prevent the Need to Create an Ever-Expanding Multiplicity of Individualized Privacy Policies

Imprecise drafting in the CCPA may require privacy policies to disclose the "specific pieces of personal information the business has collected about that consumer."[11] Because data differs from one consumer to another, to comply with this provision, a business would need to create personalized privacy policies for each consumer that visits their website. This process would be incredibly burdensome, costly and could raise the likelihood of inadvertent disclosures of specific consumer information to wrong recipients. This requirement also is found in the part of the law describing consumer access rights, which suggests that the provision could be meant to cover specific consumer access requests, not the content of required privacy policies.

We ask that the CA AG clarify that a business should not be required to create individualized privacy policies for each consumer to comply with the CCPA's privacy policy provisions and that specific pieces of information should only be provided in response to a

[10] The CA AG has authority to clarify this issue with respect to the opt-out right pursuant to Cal. Civ. Code § 1798.185(a)(4)(A), which directs him to establish rules "[t]o facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information." The CA AG also has authority to interpret CCPA's access and deletion rights pursuant to regulatory authority to "further the purposes of [the] title" in Cal. Civ. Code §§ 1798.185(a), (b). To create a consistent experience for consumers that reflects their expectations, the CA AG should clarify in rulemaking that consumers may have the same granular options with respect to access, deletion, and opt-out requests.

[11] Cal. Civ. Code § 1798.110(c) ("A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130: (5) The specific pieces of personal information the business has collected about that consumer."); Cal. Civ. Code § 1798.130(a)(5)(B) ("In order to comply with [Section]… 1798.110… a business shall, in a form that is reasonably accessible to consumers… [d]isclose… in its online privacy policy… [f]or purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.").

verifiable consumer access request.[12] By clarifying that individualized privacy policies are not required, the CA AG would prevent inadvertent disclosure of specific consumer personal information and facilitate the actual consumer's (or the consumer's authorized agent's) ability to obtain specific pieces of personal information through an access request separate from a general privacy policy disclosure, which could be viewed by multiple individuals and lead to unwanted privacy invasions.

6. Clarify "Household" in the Definition of "Personal Information"

"Personal information" under the CCPA "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*."[13] The CCPA requires that a business provide "specific pieces of personal information it has collected about [a] consumer," in response to a consumer request.[14] Because the law creates an access right for personal information and the law's definition of personal information includes both consumer and household data, the CCPA could require that a business disclose information about a consumer within a household to another consumer in the same household through the course of a consumer access request.[15] This interpretation, however, would effectively read out the specific language in the consumer access right provision that a consumer is entitled to personal information "about that consumer," not about the consumer's household.[16] If the CCPA is interpreted to require that all household information associated with a consumer be provided in response to each consumer access request, this interpretation would result in major privacy and safety concerns as personal information may be provided to a household member such as an abusive spouse or a dishonest and self-serving roommate who should not have such information.

The CA AG should clarify that access requests are limited to the personal information known about the individual consumer making the request or about others in the household only if the individual making the request is an authorized representative of those other persons in the household.[17] Specifically, the rulemaking should recognize that the term "about that consumer" in Section 1798.110 refers to only the personal information known about the individual consumer making the access request or the personal information that can be provided to the consumer as an authorized representative of other consumers in the same household.

---

[12] The CA AG has authority to interpret this provision pursuant to Cal. Civ. Code § 1798.185(a)(7), which directs him to establish "rules and procedures… to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130…."

[13] Cal. Civ. Code § 1798.140(o)(1) (emphasis added).

[14] Cal. Civ. Code § 1798.110(a)(5).

[15] Cal. Civ. Code §§ 1798.110; 140(o)(1).

[16] Cal. Civ. Code § 1798.110(a)(5).

[17] The CA AG has authority to issue this clarification pursuant to Cal. Civ. Code § 1798.185(a)(7), which allows him to "[e]stablish rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's…ability to obtain information…." The CA AG can carry out this directive by establishing rules that clarify when household information should be provided to a consumer.

7. Clarify "Professional or Employment Related Information" in the Definition of "Personal Information"

"Personal information" under the CCPA "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 [including]… [p]rofessional or employment-related information."[18] As such, consumer access, deletion, and opt-out rights apply to the undefined concept of professional or employment-related information. Without further clarification, any employee of a business can potentially request that another business or the company by whom they are employed that has information on file or in a business-to-business context delete such data as well as any business information capable of being associated with the data.[19] These deletion rights could create supply chain concerns and competitive concerns since the removal of business data could make due diligence on potential business partners or oversight of business partners impossible to carry out. Although professional and employment-related data in the CCPA could be interpreted to include employment information posted on social media or data used for marketing to individuals in their personal capacity, this data should not cover information on persons acting as a representative of an employer or business.

The phrase "professional or employment-related information" should be clarified to make clear it does not include information on persons acting as a representative of their employer or business such as business representatives and sole proprietors.[20] When a person is acting in the marketplace on behalf of an employer or business, the data that is captured is business data, not consumer data. Without a rule recognizing this distinction, an overly broad reading of the definition of personal information could allow employees to improperly access business information (thereby, potentially compromising confidential business data) or inappropriately take advantage of deletion and opt-out rights afforded to consumers under the CCPA. The CCPA is directed to consumer protection and this provision, if not clarified, would expand the law's reach far beyond that scope.

8. Distinguish "Pseudonymized" Data from "Personal Information"

The CCPA's definition of "personal information," means any data that "is capable of being associated with… a particular consumer or household," and a "consumer" is defined to include unique identifiers.[21] Because pseudonymized data is associated with a unique identifier, and a "consumer" includes unique identifiers, pseudonymized data could be captured by the definition of personal information. However, the CCPA also creates a separate definition for "pseudonymize," which suggests that pseudonymized data may be a distinct category of data

[18] Cal. Civ. Code § 1798.140(o)(1)(I).

[19] "Personal information" under the law includes "[p]rofessional or employment-related information." *Id*.

[20] The CA AG has specific authority to adopt rules to "updat[e] as needed additional categories of personal information." Cal. Civ. Code § 1798.185(a)(1). The clarification we propose aligns with this authority because the byproduct of the clarification is an additional category of personal information covering professional and employment-related information about an individual in his or her personal capacity and not their business capacity.

[21] Cal. Civ. Code § 1798.140(o)(1); 140(g).

apart from personal information. According to the CCPA, pseudonymized data is rendered in a manner that does not directly identify a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that it is not attributed to an identified or identifiable consumer.[22] Also, the CCPA's only reference to pseudonymized data is in the definition of research, where the CCPA lists pseudonymized data in the same category as de-identified data – data excluded from the definition of the term "personal information."[23] As such, the CCPA does not explicitly resolve whether pseudonymized data is personal information or if pseudonymized data falls outside the definition of personal information.

If pseudonymized data is considered personal information under the law, the CCPA has the potential to force businesses to collect substantially more data about consumers so that they can individually identify a specific person that makes a CCPA request. For example, to effectuate consumer rights such as the rights to access, delete, or opt out of the sale of personal information under the CCPA, a business that does not have identifying information such as a name or email address could be forced to associate this data from the requester with non-identifiable device data that the business holds. This approach would remove existing data privacy protections enjoyed by California residents pursuant to self-regulatory codes such as the Digital Advertising Alliance's ("DAA") Self-Regulatory Principles for Online Behavioral Advertising by forcing businesses to reidentify data in order to verify a consumer's request.[24]

To help ensure consumer privacy is appropriately protected by pseudonymized data, the CA AG should clarify that pseudonymized data is not covered within the definition of personal information when the data is governed by the pseudonymized data controls listed in the CCPA (*i.e.*, the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that it is not attributed to an identified or identifiable consumer).[25] If such a clarification is not made, we request that the CA AG issue a rule that states that a business need not link pseudonymized data to personally identifiable information (such as a name or email address) to effectuate a consumer request when the company does not maintain any personally identifiable information. To effectuate the request, a consumer should provide only the pseudonymized information that the business maintains through a recognized opt-out tool such as the opt-out provided by the Digital Advertising Alliance. Such a rule would ensure that

[22] Cal. Civ. Code § 1798.140(r).

[23] Cal. Civ. Code § 1798.140(s); 140(o).

[24] *See* 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.

[25] The CA AG has the authority to make this clarification based on CCPA's directive to the CA AG adopt rules to "further the purposes of this title." Cal. Civ. Code §§ 1798.185(a), (b). Such an interpretation would further the purposes of this title because when pseudonymized data is considered personal information, businesses may need to collect more information from consumers in order to effectuate CCPA requests. The collection of this identifiable information creates privacy concerns including increased risks to personal data and identity theft that did not previously exist.

companies that have made the choice not to link pseudonymized data to personally identifiable data are not forced to do so to comply with the CCPA.[26]

9. Clarify the "Cure" Requirement for Security Breaches

Under the CCPA, no action for statutory damages may be initiated against a business for an alleged data security failure if the business actually *cures* the noticed data security violation within 30 days.[27] The CCPA, however, does not define "cure," and as a result there is a risk that a strict interpretation of the term would mean that any data that was lost, corrupted, or subject to unauthorized access due to the breach must be retrieved or restored in order to constitute a "cure" of the violation. Such an overly restrictive interpretation of "cure" would be difficult, if not impossible, in many cases to attain and would essentially render moot the law's cure option.

The CA AG should clarify that the "cure" requirement refers to curing the security procedures and practices that may be found to be deficient under the statute, and the term "cure" does not require that a company retrieve or restore data that may have been lost, corrupted, or subject to unauthorized access where no consumer harm has occurred.[28] In cases where demonstrable harm has occurred, "curing" the breach would be to cure the security procedures and practices that may be deficient under the statute and providing a process to reasonably reimburse consumers for any actual loss that a consumer suffered as a direct result of the breach and providing such reimbursement within a reasonable period. Such an interpretation is consistent with the CA AG's authority to further the purposes of the CCPA, as it would incentivize companies to implement and maintain reasonable security procedures and practices.

II. Key Additional Issues for the California Attorney General to Address

This section identifies key additional issues within the CCPA that would benefit from the CA AG's clarification.

1. Clarify that Businesses Have Flexibility When Verifying Consumer Requests

Generally speaking, the CCPA affords consumers rights to access, delete, and opt out from the sale of personal information but, despite affording consumers these expansive rights, the CCPA provides little guidance on how businesses should comply with these rights. Specifically, no guidance exists on the steps a business must take when a consumer does not provide enough information to identify the data the business holds about him or her. Currently, the only validated method for confirming consumer identities is dependent on the consumer having an account with the entity to whom the request is directed.[29] Under this provision, a request submitted through a password-protected account maintained by the consumer is

[26] *Id.*

[27] Cal. Civ. Code § 1798.150(b).

[28] The CA AG may clarify this issue based on his authority to adopt rules to "further the purposes of [the] title." Cal. Civ. Code §§ 1798.185(a), (b).

[29] Cal. Civ. Code § 1798.185(a)(7).

considered a verifiable consumer request.[30] This method of verification, however, may have limited utility for businesses that do not offer consumers the ability to create consumer accounts in the normal course of business. Also, the CCPA does not address the format or level of detail businesses should provide in response to consumer access requests.

The CA AG should clarify how a business should comply with vague or incomplete requests. In particular, we request that the CA AG clarify that: (1) a business may use commercially reasonable methods to verify a consumer request before effectuating an access, opt-out, or deletion request under the law; (2) the process of verifying consumer requests may take many different forms; and (3) businesses may ask consumers for necessary information to ensure the request can be addressed.[31] Additionally, businesses should be permitted to respond to consumer access requests in any commercially reasonable way, provided the response is complete and given in a consumer-friendly and portable format. The CA AG can make this interpretation pursuant to its specific authority to adopt rules related to verifiable consumer requests as articulated in the CCPA's definition of a "verifiable consumer request."[32]

2. Preserve Ad Measurement and Attribution Activities

The CCPA does not create explicit exceptions for ad measurement and attribution activities, which involve the analysis of advertising practices to help refine advertising tactics, mediums, and content so it is more appropriate and enjoyable for consumers. As a result, a consumer potentially could delete data or restrict the sharing of data that would prevent the ability to carry out ad measurement and attribution. Without the ability to use information for these purposes, consumers would view less relevant ads as businesses would have a much more difficult time improving ad content and placement, gauging ad effectiveness, and understanding consumer preferences.

The CA AG should clarify that: (1) personal information strictly used for ad measurement and attribution activities constitute an internal use of personal information exempt from the deletion right under the law; and (2) ad measurement and attribution activities constitute "analytic services"[33] within business purposes exempt from the definition of "sale" under the

[30] *Id.*

[31] The CA AG has authority to issue this clarification with respect to the access and deletion provisions pursuant to Cal. Civ. Code § 1798.185(a)(7), which allows him to establish "rules and procedures… to facilitate a consumer's… ability to obtain information pursuant to Section 1798.130…." The CA AG can use Cal. Civ. Code § 1798.185(a)(4)(B) to interpret the opt-out right, as it allows him to issue regulations "[t]o govern business compliance with a consumer's opt out request." Alternatively, the CA AG can use his general authority to issue rules "as necessary to further the purposes of this title." Cal. Civ. Code §§ 1798.185(a), (b).

[32] Cal. Civ. Code § 1798.140(y) ("Verifiable consumer request" means a request that…the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information.")

[33] Cal. Civ. Code §§ 1798.140(d); 140(t).

law.[34] This interpretation would allow for internal, analytic uses of data that are contemplated by already existing exemptions to the deletion right and the "sale" definition.

3. Clarify the Scope of the "Publicly Available" Information Exclusion

Publicly available information is excluded from the CCPA's definition of personal information, but the law is unclear with respect to what constitutes publicly available information.[35] In particular, the law states that information is not publicly available unless it is used for the purpose for which it was made available in a government record, even though these records often do not fully identify the purposes for which the information was released.[36] Publicly available information is for public use. To say data is not publicly available unless it is used for the purpose for which it was made available in a government record is a departure from the general notion that publicly available information is for public use. It also defies the common sense understanding of the term "public" and is an unintended consequence of the way the publicly available information exemption is currently drafted. The law's terms should reflect the exclusion as it is typically featured in state and federal privacy statutes throughout the country.

The definition of "publicly available" information should be clarified so that information made available by government disclosures can be used unless the government specifically prohibits a certain use.[37]

4. Clarify the 12-Month Look-Back Provision

The CCPA imposes a 12-month look-back provision that requires businesses to "[d]isclose and deliver the required information to a consumer… [which] shall cover the 12-month period preceding the business's receipt of the verifiable consumer request…."[38] The law is unclear if this 12-month look-back provision: (1) imposes a 12-month data retention requirement on businesses, even though no specific retention requirement is created by the law; or (2) creates an affirmative requirement for businesses to retain data held as of January 1, 2019, even though the law becomes effective on January 1, 2020 and compliance mechanisms will not be built until the CA AG completes the rulemaking process.

---

[34] The CA AG can clarify that ad measurement and attribution activities are not subject to the opt-out to sale right pursuant to his authority to issue rules "[t]o facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information." Cal. Civ. Code § 1798.185(a)(4)(A). For the deletion right, the CA AG has authority to interpret this provision pursuant to his general regulatory authority to further the purposes of the CCPA, which already envisions the use of data for similar analytic purposes regardless of a consumer deletion request. Cal. Civ. Code §§ 1798.185(a), (b).

[35] Cal. Civ. Code § 1798.140(o)(2).

[36] *Id*.

[37] The CA AG can clarify this definition under the Attorney General's authority to adopt rules to update additional categories of personal information and the general authority to adopt rules to further the purposes of the CCPA. Cal. Civ. Code §§ 1798.185(a)(1), (b).

[38] Cal. Civ. Code § 1798.130(a)(2).

We request that the CA AG clarify that: (1) there is no data retention requirement; and (2) the 12-month look-back provision takes effect 12 months *after* the CA AG's rulemaking is complete.[39] Regarding the data retention request that would clarify that no data retention requirement exists, we ask the AG to clarify this point so that the law does not inadvertently create new rules that require the retention of data, creating new privacy concerns. Regarding the effective timeline for access requests, the CCPA already anticipates that some consumer access requests will not be fulfilled (where requests are "manifestly unfounded" or "excessive").[40] As such, it would not be inconsistent for the CA AG to take the position that providing access rights before the implementing regulations interpreting the CCPA are written would be manifestly unfounded, since there is no sufficient clarity on the scope of data involved. Moreover, providing access rights to data before the rules on the scope of data involved or how to verify a consumer request are promulgated creates risks of fraud and privacy violations. As a result, clarifying the 12-month look-back via regulation would further the purposes of the CCPA by minimizing such risks of fraud and privacy violations and increasing the ability of businesses to comply with the CCPA in privacy-conscious and privacy enhancing ways.

5. Limit the CCPA's Unintended Impact on Nonprofit Organizations, Including Charities

The CCPA is unclear if businesses subject to the CCPA must delete or refrain from selling consumers' personal data when such data will be provided to nonprofit organizations, including charities. The CCPA was not intended to impact charities and nonprofits, as the law applies to "for profit" businesses and does not explicitly create rules for nonprofits.[41] Nonprofit activities and charitable giving are reliant on smart, informed data sources. Using data from businesses for charitable purposes is foundational to the operations of legitimate nonprofit organizations. Charities use such data to communicate with donors, potential supporters, and new contacts about vitally important missions that help Californians. Requiring compliance with CCPA rules for businesses that provide data to charities and nonprofits would cripple such entities' ability to access information in order to further their nonprofit missions. The CCPA creates a risk that nonprofits will be able to access few legitimate data resources, which could jeopardize the future growth of charities, their missions, and charitable giving in California.

The CA AG should clarify that consumer personal information maintained by a business strictly to provide such data to nonprofits, including charities, is exempt from the CCPA's deletion and opt-out rules.[42] This interpretation would further the purposes of the CCPA, which is designed to cover businesses, not nonprofit organizations and charities.

---

[39] As further described in this section, the CA AG may clarify this issue based on his authority to adopt rules to "further the purposes of [the] title." Cal. Civ. Code §§ 1798.185(a), (b).

[40] Cal. Civ. Code § 1798.145(g)(3).

[41] Cal. Civ. Code § 1798.140(c).

[42] As further described in this section, the CA AG may clarify this issue based on his authority to adopt rules to "further the purposes of [the] title." Cal. Civ. Code §§ 1798.185(a), (b).

6. Preserve the Ability to Provide Expected Marketing Messages to Consumers

The CCPA states that a business or a service provider shall not be required to comply with a consumer's deletion request if: (1) it is necessary for the business or service provider to maintain the consumer's personal information in order to provide a good or service requested by the consumer; or (2) if maintaining such information would be reasonably anticipated within the context of a business's ongoing business relationship with the consumer.[43] However, the CCPA is unclear with respect to whether expected marketing messages, such as subscription renewal reminders, are reasonably anticipated and can be provided within the context of a business's ongoing business relationship with the consumer.

We ask the CA AG to clarify that the deletion exception for providing a service requested by the consumer or reasonably anticipated by the consumer can include expected marketing messages (*i.e.* subscription renewal reminders).[44] Because consumers expect and value these messages from their ongoing commercial activities, including them in the scope of the aforementioned deletion exception would further the purposes of the title by preserving consumer expectations in a specific area that consumers value.

7. Ensure the Viability of the Fraud Exception

The CCPA creates a deletion right and an exception to this right for business activities related to combatting fraud, such as: detecting security incidents; protecting against malicious, deceptive, fraudulent, or illegal activity; and prosecuting those responsible for such activity.[45] However, the CCPA is unclear as to whether the fraud exception to a consumer's deletion right covers businesses that collect and use data to create anti-fraud products and services. If the exception does not cover these activities, the CCPA could jeopardize the availability of the anti-fraud tools the law already recognizes should be protected. Also, under the CCPA, a consumer may authorize a third party to delete information on the consumer's behalf, which could allow a cottage industry to develop for offering deletion services for anti-fraud databases and other identity verification and fraud detection networks. Some of the areas that could be impacted by an incomplete fraud exception include: anti-terrorism efforts (ensuring people on terrorist watch lists do not have access to financing), anti-money laundering efforts, locating persons of interest in criminal investigations, verification of identities, and officer safety measures, such as the identification of the occupants of an address.

The deletion exception for fraud should be clarified to include the collection and use of personal information to create and sell anti-fraud tools. Such an interpretation by the CA AG would further the purposes of the CCPA by helping businesses access robust tools, products, and

[43] Cal. Civ. Code § 1798.105(d)(1).

[44] As further described in this section, the CA AG may clarify this issue based on his authority to adopt rules to "further the purposes of [the] title." Cal. Civ. Code §§ 1798.185(a), (b).

[45] Cal. Civ. Code § 1798.105(d)(2).

services for fighting fraud.[46] These tools, products, and services enhance consumer privacy by allowing businesses to employ reliable efforts to combat fraudulent practices in order to protect consumer identities and personal information.

8. Clarify the Definition of "Business Purpose"

The CCPA definition of "sale" excludes the sharing of personal information with a service provider if such sharing "is necessary to perform a business purpose."[47] As a result, a business that shares a consumer's personal information with a service provider for a business purpose will not constitute a sale of information from which a consumer can opt out. According to the CCPA, a "business purpose" means the use of personal information for the business or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed, or for another operational purpose that is compatible with the context in which the personal information was collected.[48] The CCPA also lists seven permissible "business purposes."[49] Specifically, the CCPA states, "Business purposes are:" and then lists the seven permissible purposes.[50] Because the CCPA stated that business purposes "are" instead of business purposes "include," the CCPA could be read to limit the general definition of "business purpose" to those seven examples, which is too narrow for consumers and businesses alike. For instance, undertaking research for retail store site selection or product placement is a business purpose that should be included in the definition but is not specifically mentioned in the CCPA's seven enumerated examples of business purposes.

We believe that the CA AG can reasonably conclude that the purposes identified in Section §1798.140(d)(1)-(7) are not exhaustive, and should clarify that the general definition of "business purpose" is still operative and the seven categories are examples rather than the full extent of the definition.[51] Although the purposes are introduced using the term "are" (which may suggest an exhaustive list), the overarching definition of a "business purpose" is functional. Ensuring that the seven categories are examples rather than the full extent of the definition would further the purposes of the title by maintaining the existing narrow, yet flexible, definition of "business purpose" without limiting the definition to the seven examples that are not fully reflective of the definition.

---

[46] As further described in this section, the CA AG may clarify this issue based on his authority to adopt rules to "further the purposes of [the] title." Cal. Civ. Code §§ 1798.185(a), (b).

[47] Cal. Civ. Code § 1798.140(t)(2)(C).

[48] Cal. Civ. Code § 1798.140(d).

[49] Cal. Civ. Code §§ 1798.140(d)(1)-(7).

[50] *Id.*

[51] The CA AG may clarify this issue based on his authority to adopt rules to "further the purposes of [the] title." Cal. Civ. Code §§ 1798.185(a), (b). Clarifying the scope of the fraud exception would ensure that data is maintained to combat fraud and any resulting unwanted privacy intrusions.

9. Clarify the Operative Ages in the Opt-In Requirement Related to Minors

As written, the CCPA requires businesses to refrain from selling the personal information of consumers they know to be "less than 16 years of age" without opt-in consent.[52] The effect of this rule is that businesses must receive opt-in consent to sell the personal information of children aged 15 or younger. However, the law also allows minors aged 16 (not *less* than 16) to consent on their own behalf even though age 16 is beyond the age where opt-in consent is required."[53] As such, the inconsistencies in descriptions of ages create confusion around the ages when opt-in consent is required.

The CA AG should clarify that the rule requiring opt-in consent to sell personal information of children relates to children aged 15 or younger.[54] This would help educate consumers on their rights and promote compliance with the CCPA by setting forth a definitive rule regarding the age at which opt-in consent is necessary.

10. Remove Backup Information from the Scope of a Deletion Request

The CCPA 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; however, the law is silent on whether those data requests cover data held in backup storage when the data is not used for other purposes.[55] Data held in backup storage is kept for a finite period of time and typically only to restore systems in the event of a data failure. As a result, the CA AG should issue a rule exempting data held on backup tapes from the scope of the deletion right under the CCPA.

In particular, we request that the CA AG interpret Section 1798.145(g)(3) of the CCPA (providing exceptions to consumer requests that are excessive or manifestly unfounded) to include requests related to data in backup storage.[56] If consumers' deletion requests could reach the data held on backup systems, businesses' ability to rebound from data failures and technological problems would be severely limited. Removing backup storage data from the scope of the deletion right would further the purposes of the CCPA by continuing to enable businesses to mitigate data loss issues without having to contact the consumer for assistance in restoring necessary information.

---

[52] Cal. Civ. Code § 1798.120(c).

[53] *Id.*

[54] As further described in this section, the CA AG may clarify this issue based on his authority to adopt rules to "further the purposes of [the] title." Cal. Civ. Code §§ 1798.185(a), (b).

[55] Cal. Civ. Code § 1798.105(a).

[56] As further described in this section, the CA AG may clarify this issue based on his authority to adopt rules to "further the purposes of [the] title." Cal. Civ. Code §§ 1798.185(a), (b).

11. Ensure that Businesses Do Not Have to Collect Extra Data to Comply with CCPA Requirements

The CCPA does not explain how a business should comply with a vague consumer request or a request that does not provide sufficient information to locate personal information maintained by the business about the consumer. Accordingly, an overbroad interpretation of the CCPA would mandate that a business collect additional information about a consumer sufficient to locate records maintained by the business. However, the law also states that businesses do not need to "reidentify or otherwise link information that is not maintained in a manner that would be considered personal information."[57] As such, there is ambiguity as to whether additional consumer information must be sought by a business to effectuate a consumer request.

The CA AG should clarify that businesses are not required (but may attempt) to collect additional information about a consumer to comply with a vague consumer request or a request that does not provide sufficient information to locate the personal information maintained by the business about the consumer.[58] This interpretation would further the purposes of the CCPA by refraining from mandating the transfer of additional information by consumers to businesses while simultaneously allowing the business to access the information it needs to comply with a consumer request.

* * *

The ANA appreciates this opportunity to comment on the California Consumer Privacy Act and looks forward to continuing to work with the CA AG on these issues.

Please contact Dan Jaffe, Group Executive Vice President, at djaffe@ana.net or (202) 296-1883 with any questions regarding these comments.

[57] Cal. Civ. Code § 1798.145(i).

[58] As further described in this section, the CA AG may clarify this issue based on his authority to adopt rules to "further the purposes of [the] title." Cal. Civ. Code §§ 1798.185(a), (b).