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

COMMENTS
of the
ASSOCIATION OF NATIONAL ADVERTISERS
on the
California Consumer Privacy Act Proposed Regulations

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

Counsel:
Stu Ingis
Mike Signorelli
Tara Potashnik
Allaire Monticollo
Venable LLP
600 Massachusetts Ave., NW
Washington, DC 20011
202.344.4613

December 6, 2019
On behalf of the Association of National Advertisers ("ANA"), we provide the following comments in response to California Office of the Attorney General’s ("CA AG") October 11, 2019 request for public comment on the proposed regulations implementing the California Consumer Privacy Act (the "CCPA"). We appreciate the opportunity to engage with the CA AG on the important subject of consumer privacy and the content of the rules that will help implement the CCPA.

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

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

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

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

---

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

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

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

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

---


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

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

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

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

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

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

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

---

6 Cal. Code Regs. tit. 11, §§ 999.336(b), 337(a) (proposed Oct. 11, 2019).
7 Id. at §§ 999.307(b)(5)(a), 337(a).
8 Id. at § 999.307(b)(5).
must justify the price or service difference offered to consumers on a product-by-product basis (e.g., discounts for coffee must be justified independently and separately from discounts for pastries), or if businesses may justify their price or service differences for CCPA purposes in a more holistic sense. The method by which a business values personal information associated with a consumer may vary based on the situation at hand, the discount being offered at a particular time or in a particular place, and a variety of other factors. Additionally, the actual value the business attributes to such data may, in many cases, be difficult to quantify.

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

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

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

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

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

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

---

\(^9\) Id. at § 999.315(c).

\(^10\) AB 370 (Cal. 2013).
Per the proposed rules, upon receipt of a consumer opt out request, a business must: (1) “notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business’s receipt of the consumer’s request that the consumer has exercised their right to opt-out,” and (2) “instruct [the third parties] not to further sell the information.” This provision places requirements on businesses to communicate opt-out requests to third parties and instruct those third parties not to further sell information, which are obligations that are not included in the CCPA. To avoid regulatory provisions that are not within the scope of the statutory text of the CCPA and could cause significant unintended consequences that could result from these entirely new business obligations, the CA AG should update the proposed regulations to align with the CCPA such that businesses are not required to pass opt-out requests along to third parties. At a minimum, the CA AG should clarify that businesses are not required to pass opt-out requests along to third parties if such third parties are contractually prohibited from selling personal information received from the business.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

III. Consumer Requests to Know and Delete

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

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

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

18 Id. at § 999.330(a)(2); 16 C.F.R. § 312.5(b).
20 Id. at § 999.301(n)(1) (emphasis added).
proposed regulations, the CA AG noted its intent in providing a definition of “request to know.”\textsuperscript{22} The CA AG did not indicate a desire to alter the requirements of the CCPA in this description of its intent. Instead, the CA AG said it provided a definition of request to know to “allow… the regulations to group together the requirements businesses must follow,” suggesting the intent was to improve convenience and readability rather than substantively change the requirements of the law. The CA AG also stated that it provided a definition of request to know to offer further clarity and to avoid unnecessary confusion. As a result, it does not appear that the CA AG intended to change the meaning of the CCPA or create ambiguity by issuing this provision of the proposed regulations. ANA asks the CA AG to the extent practical to harmonize the language of the proposed rules with the text of the CCPA. This would help reduce confusion for businesses implementing the CCPA’s requirements. Therefore, ANA urges the CA AG to update the proposed rules’ definition of “request to know” so that requests for personal information apply to “personal information that a business has collected about the consumer” and “specific pieces of personal information that a business has collected about a consumer.” ANA submits this suggested clarification to the CA AG to help ensure that the regulations align with the text of the CCPA.

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

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

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

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


\textsuperscript{23} Cal. Code Regs. tit. 11, § 999.312(c)(2) (proposed Oct. 11, 2019).
c. Ensure the Definition of “Request to Delete” Aligns with the Requirements Businesses Must Meet in Describing Such Requests

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

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

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

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

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

24 Id. at § 999.308(b)(2)(a) (emphasis added).
25 Id. at § 999.301(o) (emphasis added).
27 ISOR at 7.
29 Id. at § 999.313(d)(2).
does nothing to further the purposes of the law, imposes significant compliance challenges for businesses, and may conflict with other provisions of the proposed regulations.

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

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

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

IV. Service Providers

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

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

31 Cal. Code Regs. tit. 11, § 999.317(b) (proposed Oct. 11, 2019).
32 Id. at §§ 999.312(a), (b); 999.315(a).
33 Id. at § 999.314(d).
marketplace or abridge the confidentiality clauses the service provider agreed to in contracts with its business clients.

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

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

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

V. Consumer Verification

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

34 Id. at § 999.314(c).
The proposed regulations state that if a business maintains personal information in a manner that is not associated with an actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the non-name identifying information. In addition, the proposed rules state that “[i]f a business maintains consumer information that is de-identified,” it is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request. The proposed regulations do not clearly explain how businesses may reasonably engage in verification when they do not maintain personal information in a manner that is associated with a named actual person. ANA asks the CA AG to clarify that businesses that do not maintain data sufficient to verify a consumer’s identity are not required to collect additional data from the consumer to do so.

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

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

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

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

35 Id. at § 999.325(e)(2).
36 Id. at § 999.323(e).
37 Id.
38 See id. at §§ 999.325(b), (c).
39 Id. at § 999.323(a).
businesses to respond to requests to know and requests to delete within 45 days.\textsuperscript{40} Consistent with the proposed regulations’ verification provisions, a business may require a consumer to submit information to verify his or her identity before responding to a request.\textsuperscript{41} The draft rules note that the 45-day time period to respond to requests to know and requests to delete “will begin on the day that the business receives the request, regardless of time required to verify the request.”\textsuperscript{42}

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

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

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

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

\textsuperscript{40} Id. at § 999.313(b).
\textsuperscript{41} Id. at §§ 999.323(b), (c).
\textsuperscript{42} Id.
\textsuperscript{43} Id. at § 999.312(d).
\textsuperscript{44} Id. at § 999.313(d)(1).
\textsuperscript{45} Id. at § 999.315(h).
entirely new obligation that is not required by the CCPA itself and is outside of the scope of the law. The CA AG’s proposed rule requiring businesses to pass along opt out requests to third parties to whom they have sold personal information in the prior 90 days would mean that a consumer’s unverified deletion request could have a ripple effect throughout the ecosystem by removing personal information associated with that consumer from the entire online environment. This result may not align with the consumer’s desires, particularly if the consumer thought he or she was submitting a deletion request to be effective solely on an individual business. Such an application may not reflect the consumer’s preferences and denies them the ability to allow some businesses to sell personal information while restricting others from doing so. The CA AG should therefore clarify that consumers must affirmatively request that a business opt the consumer out from personal information sale before the business may treat a deletion request as an opt out request.

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

VI. Privacy Policies

a. Clarify the Required Granularity of Privacy Policies

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

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

46 Id. at § 999.308(b)(1)(d)(2).
respect to personal information generally. This would detract from the purpose of a robust consumer privacy notice, as it would induce notice fatigue and could discourage consumers from taking the time to read and understand the full privacy notice and its contents. Additionally, requiring granular disclosures for each category of personal information collected could impede businesses from satisfying the requirement that a privacy policy must “be written in a manner that provides consumers [with] a meaningful understanding of the categories listed.”47 The CA AG should clarify that businesses may make required disclosures for personal information generally and do not need to make granular disclosures relevant to each category of personal information collected. Businesses should be able to provide consumers with privacy policies that logically disclose required information in a digestible and understandable format, as this approach would further the ultimate goal of robust consumer notice in a more effective way than requiring disclosures pertaining to each category of personal information collected.

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

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

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

47 Id.
48 Id. at § 999.308(a)(3).
50 Privacy on the Go at 10.
c. Clarify that Businesses Do Not Have to Make Statements About Minors In Privacy Policies Unless They Have Actual Knowledge They Collect Personal Information From Minors Under the Age of 16

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

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

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

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

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

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

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

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

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

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

56 Cal. Code Regs. tit. 11, § 999.317(g) (proposed Oct. 11, 2019).
share personal information of 4 million or more consumers. As a result, we ask the CA AG to clarify that sharing personal information about a consumer with a service provider does not count towards determining whether a business is subject to these additional reporting requirements.

VII. Other Required Notices

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

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

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

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

58 Id. at § 999.301(j).
59 Id. at § 999.306(b)
60 Id. at § 999.307(a)(3).
61 Id. at § 999.305(a)(2)(e).
The CA AG should clarify that the notice at collection, notice of right to opt-out, and notice of financial incentive may be provided to consumers in a privacy policy, and if such notices are provided in a privacy policy that is made available to consumers where required, they do not need to be provided through any other means. Such a rule would enable business compliance with the CCPA and offer consumers a centralized place through which they may receive required business disclosures. Providing such notices within the privacy policy is consistent with consumer expectations. Consumers have come to expect such disclosures and information to be accessible from a privacy policy. Consumers would benefit from receiving all the necessary information through a single notice, and businesses would benefit from being able to focus privacy-related information in one unified disclosure.

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

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

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

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

---

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

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

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

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

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

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

64 Id. at § 999.312(a).
65 Id. at § 999.305(b)(1).
66 Id. at § 999.308(b)(1)(d)(1).
Furthermore, this discrepancy between the need to provide information about future practices and information about past practices fails to adequately clarify what information must be provided in required notices. If a business may make all CCPA-required disclosures in one privacy policy, it is not clear whether it must provide a section for categories of personal information to be collected in the future and a section for categories of personal information it collected in the past 12 months. We request that the CA AG clarify this provision by regulation.

VIII. Provisions of the Proposed Regulations that ANA Supports

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

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

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

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

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

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

---

67 Id. at § 999.306(e)(1).
68 Id. at § 999.313(c)(4).
69 Cal. Civ. Code §§ 1798.82(g), (h).
effects, such as indirectly exposing private details about a consumer’s life. ANA supports the CA AG’s efforts to restrict certain data elements from disclosure all together, as this restriction is privacy protective for consumers and serves to help businesses comply with California law.

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

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

* * *

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

---

70 Cal. Code Regs. tit. 11, § 999.323(a) (proposed Oct. 11, 2019).
71 Id. at § 999.323(b)(3).