December 6, 2019

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

Dear Attorney General Becerra:

The retail industry is a driving force for California's economy. One in four jobs in California are in the retail industry. In California alone, over 3.2 million people are employed by retailers, eight times the number of employees in the entertainment industry.[1] The retail industry accounts for $330 billion in California's gross domestic product each year.[2]

California retailers have no higher priority than earning and maintaining the trust and confidence of their customers. Retailers embrace careful stewardship of customer data not only because maintaining customer trust is a core business imperative, but also because it is the right thing to do. That is why California retailers have worked closely with policymakers to help build a workable and transparent regulatory structure for consumer data that will meet the expectations of California consumers and align with the ability of retailers and other businesses to offer Californians the goods and services they desire – both on-line and at one of California's 400,000 retail establishments.

The California Retailers Association (the "Association") represents all segments of the retail industry, including general merchandise, department stores, mass merchandisers, online markets, restaurants, convenience stores, supermarkets and grocery stores, chain drugstores, and specialty retail such as auto, vision, jewelry, hardware and home stores. The Association respectfully submits the following comments to the Attorney General with the specific intent to improve the proposed Regulations so that consumers have more transparency and control over their personal information, while continuing to benefit from the retail experience they enjoy today.

---

[1] National Retail Foundation, *Retail's Impact in California*, available at https://ebef00ab1b55abc1234e-8b095d4996da583b75b9d81eb8199259.ssl.cf5.rackcdn.com/CALIFORNIA%20%7C%20National%20Retail%20Federation.pdf.

[2] *Id.*

I. The Regulations Should Not Be Effective Until at Least January 1, 2021.

The CCPA is the country's first comprehensive privacy and data security law. Many businesses, consumer groups, and individual consumers alike are working diligently to understand and comply with this new law.

The Regulations were published less than three months before the effective date of the CCPA and retailers need time to comply. The Regulations create several new obligations as discussed below and likely will not be finalized until at least six months after the effective date of the CCPA.

There are so many new obligations that require both internal and external resources not previously contemplated (e.g., designing and building the necessary infrastructure). And many retailers are engaged in a significant good-faith effort to comply with the CCPA. All stakeholders would benefit from additional time to understand and prepare for the application of the Regulations. For these reasons, the Association asks the Attorney General to set forth a compliance grace period for the Regulations, up to and including January 1, 2021.

II. The Regulations Should Not Treat Loyalty Programs, Which Provide Consumers With Long-Term Benefits Not Directly Tied to the Value of the Personal Information Collected, like Financial Incentives.

Loyalty, rewards, premium features, discounts, and club cards (hereinafter and collectively, "retailer loyalty programs") offer consumers the opportunity to provide personal information (*e.g.*, name, email address, postal address, phone number) so they can receive future offers of benefits from a retailer. Consumers have no obligation to accept these future offers and the consumer controls and measures receipt of her (potential or actual) benefit over time. Some examples include:

- Offering loyalty members exclusive sale days and sale prices throughout the year; and
- Providing loyalty members who spend a certain dollar amount on purchases in a calendar year additional benefits like free shipping, in-store tailoring, and points that can be redeemed on later purchases.

The incentive for a business to offer a consumer a benefit through a loyalty program is not a function of the value of that consumer's data to the business, but rather relates primarily to the value of retaining that consumer's business over an extended period of time.

On the other hand, financial incentive programs are economic exchanges where a business foregoes immediate revenue from the sale of a good or service in exchange for, among other things, the right to monetize the consumer's personal information currently or in the future. In contrast to a retailer loyalty program, where consumers choose to receive future offers for benefits, a financial incentive program generally contemplates a single consumer purchase of a good or service, perhaps at a discount, but without the potential for a future benefit. Some examples of financial incentive programs are:

- A mobile carrier that offers a discount on a smartphone in exchange for its collection of the consumer's current personal information through that smartphone, which may include the collection of the consumers' location, internet browsing history, and purchase history;
- Offering 0% APR financing on deals that expire in six months;
- Offering a free subscription service that automatically charges monthly fees once the free subscription period expires.

The Association respectfully requests that the Regulations recognize the fundamental differences between retailer loyalty programs and financial incentive programs by defining retailer loyalty programs as follows:

> A loyalty, rewards, premium features, discounts or club program includes an offering to one or more consumers of lower prices or rates for goods or services or a higher level or quality of goods or services, including through the use of discounts or other benefits, or a program through which consumers earn points, rewards, credits, incentives, gift cards or certificates, coupons, or access to sales or other discounts on a priority or exclusive basis.

A. The Regulations Should State Explicitly that the Price and Service Differences Available to Consumers Who Choose to Participate in Retailer Loyalty Programs and the Value of the Personal Information Consumers Provide are Necessary and Therefore Reasonably Related.

The Regulations provide:

> A financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations.[3]
>
> Notwithstanding [the above], a business may offer a price or service difference if it is reasonably related to the value of the consumer's data as that term is defined in section 999.337.[4]
>
> *Example 2*: A retail store offers discounted prices to consumers who sign up to be on their mailing list. If the consumer on the mailing list can continue to receive discounted prices even after they have made a request to know, request to delete, and/or request to opt-out, the differing price level is not discriminatory.[5]

[3] 11 CCR §999.336(a). *See also*. CIV. CODE 1798.125.

[4] 11 CCR §999.336(b).

[5] 11 CCR §999.336(c)(2).

As described above, the Regulations exacerbate the confusion created in the CCPA by incorrectly treating retailer loyalty programs like financial incentive programs, when in fact they serve very different functions and provide different benefits to consumers. Unlike financial incentive programs, retailer loyalty programs are not directly tied to the exchange of personal information for a known and current financial benefit.

For example, the *Example 2* above in the Regulations should be considered a retailer loyalty program and not a financial incentive program. A consumer opting-in to a mailing list in exchange for future offers of benefits has chosen to participate in a retailer loyalty program. Likewise, a retailer that offers those same loyal consumers 10% coupons throughout the year does so to keep the consumer loyal. The amount of the coupon is not tied necessarily to the monetization of the personal information collected but rather to help establish and strengthen long-term relationships between consumers and retailers.

For this reason, we respectfully request that the Regulations make it clear that, where **a consumer voluntarily participates in a retailer loyalty program, any price or service differences offered to those consumers, and the value of the personal information tied to such loyalty programs, are necessarily reasonably related**. The Regulations should state as follows:

> A price, rate, level, or quality of goods or services offered to a consumer, including an offer of goods or services for no fee, is reasonably related to the value of the consumer's data so long as the offer is made in connection with a consumer's voluntary participation in a loyalty, rewards, premium features, discounts, or club card program where the business has clearly described the material terms of the program, the consumer gives the business prior opt-in consent, and the consumer may revoke consent at any time.

B. The Proposed Methods to Calculate the Value of Personal Information Cannot Reasonably be Applied to Retailer Loyalty Programs in a Way That Will be Transparent and Helpful to Consumers.

The Regulations provide:

> [A] business shall include the following in its notice of financial incentive…An explanation of why the financial incentive or price or service difference is permitted under the CCPA, including:
>
> a. A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and
> b. A description of the method the business used to calculate the value of the consumer's data.[6]

As they are currently drafted, because they treat retailer loyalty programs the same as financial incentive programs, the proposed Regulations would require retailers to estimate, under pain of

[6] 11 CCR §999.307(b)(5).

penalty, the "value of the consumer's data that forms the basis for offering the…price or service differences." As described above, retailer loyalty program offers of benefits are not calculated or provided based on the value of consumer data, but the Regulations nevertheless would require these businesses to fit their loyalty program into one of the prescribed valuation methods.[7] These valuation methods, if applied to retailer loyalty programs, would implicate serious trade secret considerations, trigger difficult reporting obligations under U.S. securities laws, and, most importantly, cause substantial uncertainty for consumers and businesses alike.

1. Trade Secrets

Several of the methods listed in Section 999.337 are problematic if interpreted to require that businesses publicly disclose information that qualifies as a trade secret or proprietary information. The Regulations assume that common industries will value consumer data using similar if not identical methods. In the retailer loyalty program context, where the value of the benefit is based on the consumer's choices and not on the personal information provided, any valuation determination would require consideration of many factors including the current number of loyalty program members, the expected increase or decrease in the number of members, the amount the average member spends in the loyalty program, and many other factors. Businesses should not be forced to disclose publicly this information where competitors can see and use such information to their own advantage.

2. U.S. Securities Exchange Commission Prohibited Disclosures

Some of the novel methods of valuation proposed by the Regulations also implicate the reporting requirements that publicly-traded retailers have under U.S. securities laws. Specifically, the Regulations would require that businesses implement methods of calculation that are untested and unverified. Applying this valuation method to a business' intangible assets may not be compliant with Generally Accepted Accounting Practices ("GAAP").

3. Substantial Uncertainty for Consumers and Businesses as Applied to Retailer Loyalty Programs

The Reasons to the Regulations acknowledge that there is no generally accepted method available to the regulated community to calculate the value of a consumer's data to a business, or to a consumer.[8] Despite this, the Regulations propose a menu of unproven methods businesses would be required to choose to calculate the value of the benefit they are offering. We respectfully submit that the methods generally do not align with current accounting and financial systems retailers and other businesses use in their current operations.

[7] 11 CCR §999.337(b).

[8] Initial Statement of Reasons (ISOR), *V. 11 CCR §999.337. Calculating the Value of Consumer Data*.

C. If Price and Service Differences for Retailer Loyalty Program Participants are not Deemed to be Reasonably Related to the Value of Consumer Personal Information in the Program, the Regulations Should Authorize Retailers to Rely on the Loyalty Program Benefit Reports They Already Provide to Their Customers.

In the event that the Attorney General is not willing to find that the price and service differences in loyalty programs are reasonably related to the value of the personal information, the Association recommends that the Regulations provide for valuation methods that make sense for consumers already implemented by retailers. Specifically, the Association recommends that the Regulations support valuation based on information retailers already disclose to consumers who participate in their loyalty programs (e.g., regular receipts or statements that identify the value in savings, discounts, or other benefits received or still available). This valuation should be deemed reasonably related to the value of the consumer's data. For example, a consumer who joins a grocery store loyalty program receives points on purchases that can be used at the gas pump. When a consumer gets a receipt from the grocery store, or at the pump, the number of points gained and used are printed on the receipt. The Attorney General could easily conclude that this method, that consumers and retailers have been relying on for years, will satisfy the obligation that the benefit received by the consumers be reasonably related to the value of the consumer's data. Consumers see the value every time they receive a benefit.

III. The Regulations Must Address Unique Brick-and-Mortar Challenges With Respect to the Notice at Collection Requirements.

Although the attention of the CCPA's drafters and legislators was skewed toward new technology,[9] the breadth of the law sweeps up many businesses that remain unquestionably low-tech. Retailers within scope of the CCPA include cash-only restaurants that need consumer addresses for delivery purposes, boutiques that record credit card information by hand, and hair salons that collect phone numbers in order to remind clients of the next appointment. The variations among retail businesses are vast, but a common thread is an element of human interaction. In fact, e-commerce makes up only about 10% of total retail sales.[10]

Counterintuitively, the Regulations focus on the digital world while imposing the same—or even more onerous—obligations on businesses operating substantially offline. This is despite the fact that these offline interactions with consumers are often more transparent in the collection and use of consumer information, and more directly benefit the consumer taking part in the interaction. Collection of information often takes place closer in time to the benefit provided to the consumer in offline interactions, making the use and purpose obvious. For example, a sales associate

[9] *See* Legislative Findings: "As the role of technology and data in the every daily lives of consumers increases, there is an increase in the amount of personal information shared by consumers with businesses. . . . In March 2018, it came to light that tens of millions of people had their personal data misused by a data mining firm called Cambridge Analytica. A series of congressional hearings highlighted that our personal information may be vulnerable to misuse when shared on the Internet. As a result, our desire for privacy controls and transparency in data practices is heightened."

[10] *See* https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

asking for identification so a consumer can return an item without a receipt is understood to be collecting that information for the protection of the consumer as well as the business: to confirm the consumer's identity and credit the correct account. This transaction occurs many times every day in more than 400,000 retail stores across the state. By applying the same requirements designed to provide more information on the opaque data transfers that occur online, the Regulations burden both the business and consumer by creating unnecessary disclosure obligations. Moreover, the Regulations failed to take into account the amount of time and effort it takes to design, manufacture, and install signage in 400,000 stores across the state of California. The result is a disproportionate impact on retailers, without providing the protections against third party data use that the law was intended to provide. The Association offers the following recommendations to help align the Regulations with the thousands of offline transactions California retailers have with their customers every day.

A. The Regulations Should Provide Guidance on When and Where Offline Consumers Should Expect to See the "Notice at Collection" and What the Offline "Notice at Collection" Must Contain.

The Regulations provide:

> The notice [at collection] shall…Be visible or accessible where consumers will see it before any personal information is collected…When a business collects consumers' personal information offline, it may, for example…post prominent signage directing consumers to the web address where the notice can be found.[11]

The Regulations should specify that businesses may provide the Notice at Collection at the point of sale, before a transaction is completed, so consumers and businesses will understand what is required. This will promote uniformity and make it easier for consumers to seek and compare notices at the various retail stores they visit. The Attorney General should also confirm that signage directing consumers to a web address will be considered fully compliant with Notice at Collection for offline transactions so long as the addressed website contains the required disclosures. Finally, the Attorney General should specify text for the signage that will be deemed to comply. The Association recommends the following language:

> California Consumer Privacy Act Notice
> [INSERT BUSINESS NAME] collects personal information as defined in California Law. Please visit [INSERT WEB ADDRESS] to view our privacy policy and learn more about your California consumer privacy rights.

Should the Attorney General choose not to provide specific guidance on the text of the notice, the Association recommends that the Attorney General implement a safe harbor or right to cure for businesses that demonstrate a good-faith attempt to provide adequate notice at collection.

[11] 11 CCR §999.305(a)(2)(e). *Reference: CIV. CODE 1798.100, 1798.115 and 1798.185.*

B. The Regulations Should Permit Consumers Full Choice with Their Personal Information and Provide Limited Flexibility Regarding the Disclosures Required in the "Notice at Collection."

The Regulations provide:

> A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.[12]

> A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection. [13]

Given the extensive requirements of the Notice, most retailers will post signs directing their customers to an online version of the Notice, as permitted in §999.305(a)(2)(e) quoted above at the beginning of Section I.A. The Association is concerned that prohibiting any further collection beyond what is in the written Notice could impede the organic nature of in-store customer interactions. The Regulation as written could be construed to prohibit any spontaneous collection of personal information even if the customer requests or directs it (*e.g.*, as a result of a customer concern or to accommodate a special request).

We recommend the Attorney General revise §999.305(a)(3) and (4) to allow businesses to receive personal information without providing a new written Notice where the collection is at the direction of the consumer, necessary to advance a consumer interaction or request at the point of collection, or in other circumstances where providing a new written Notice would substantially impede, delay, or disrupt everyday business transactions.

C. The Attorney General Should Provide Consumers with a Uniform System to Exercise their Opt-Out Right.

The Regulations provide:

> A business that substantially interacts with consumers offline shall also provide notice to the consumer by an offline method that facilitates consumer awareness of their right to opt-out. Such methods include, but are not limited to, printing the notice on paper forms that collect personal information, providing the consumer with a paper version of the notice, and

[12] 11 CCR §999.305(a)(3).

[13] 11 CCR §999.305(a)(4).

> posting signage directing consumers to a website where the notice can be found.[14]
>
> A business shall consider the methods by which it interacts with consumers when determining which methods to provide for submitting requests to know and requests to delete. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer, even if it requires a business to offer three methods for submitting requests to know.[15]

The Association appreciates the Attorney General's desire to explore whether some businesses should be required to give some consumers additional ways to exercise their right to opt-out. The Association is concerned, however, that Sections 999.306 and 999.312 could create a compliance obstacle for these offline businesses without a corresponding privacy benefit for California consumers. Consumers already will have the opportunity to exercise their opt-out right through a toll-free number or online, but these sections would require creation and processing of another paper form to be offered to the consumer, completed, processed, and retained as required. The Attorney General should consider the operational reality that paper request forms received in-store likely will need to be transferred to a central, secure location for processing.

The Association requests the Attorney General conform the requirements for offline businesses to the requirements of the law but permit those businesses who substantially interact with consumers offline the ability to use a paper form if they so choose. Routing privacy requests online or through phone is consistent with the underlying goals of the CCPA and promotes a consistent, efficient, and secure environment for the collection and processing of these requests.

IV. The Attorney General Should Recognize the Consumer Transparency, Operational and Practical Challenges Associated with the New Obligations Surrounding the Consumer Right to Opt Out of the Sale of Personal Information.

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

The Regulations provide:

> If a business collects personal information from consumers online, the business shall treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a

[14] 11 CCR §999.306(b)(2). *Reference: CIV CODE 1798.120, 1798.135, and 1798.185.*

[15] 11 CCR §999.312(c).

> valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.[16]

Businesses that sell personal information are already required to include a "Do Not Sell My Personal Information" button on the homepage with direct access to methods to opt-out of the sale of personal information. To treat user-enabled privacy controls as another opt-out method exacerbates the complexity facing consumers and conflates the purpose and intent of this user-enabled privacy choice—to prevent tracking generally. It is problematic to treat tracking and selling as interchangeable terms because it weakens consumer control over personal information. A consumer should be able to control tracking separately from selling but current browser-enabled privacy settings do not provide any distinction to allow businesses to understand what the consumer actually intends the privacy setting to communicate. A consumer might not want their browser provider (i.e., Apple, Microsoft, Google) to track their browsing history, and at the same time still want businesses with which they interact to sell their personal information. To require that user privacy controls be interpreted as Do Not Sell opt out requests takes that choice away from the consumer. Indeed, it becomes an all or nothing approach. If consumers want to choose what businesses can and cannot sell (based on personal preference), they will have to disable their user-enabled privacy settings. This does not provide further transparency and in fact gives consumers less control over their privacy and the sale of personal information.

Under the Regulations as drafted, a business will not know how to reconcile a consumer's use of user-enabled privacy controls with a consumer's action or inaction vis-à-vis a "Do Not Sell" button. Further, a business has no way to contact a consumer in this scenario to confirm that it contacted all third parties to which it sold data in the previous 90 days.[17] And if a consumer uses specific user-enabled controls, rather than a global opt-out, a business has no mechanism for contacting the consumer to provide the option to globally opt-out.[18] Moreover, if a consumer uses specific user-enabled controls, retailers have no mechanism in place to put physical locations on notice of each individual consumer's user-enabled privacy control opt-out so they can refrain from asking those individuals, for the following 12 months, to authorize the sale of their personal information.[19]

The Association recommends that the Attorney General remove the references to user-enabled privacy controls from all sections of the Regulations as they are unnecessary and inhibit consumer control over their privacy and sale of personal information.

Alternatively, if the Attorney General does not remove reference to the user-enabled privacy controls, the Association asks that the Regulations provide one clear mechanism for honoring privacy-enabled settings.

---

[16] 11 CCR §999.315(c).

[17] 11 CCR §999.315(f).

[18] 11 CCR. §999.315(d).

[19] CIV. CODE §1798.135(5). "For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information."

B. Businesses that Provide and Honor a "Do Not Sell My Personal Information Button" Should Not Be Required to Notify Third Parties to Whom They Sold the Data in the Previous 90 Days to Stop Selling that Personal Information.

The Regulations provide:

> A business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the consumer's request that the consumer has exercised their right to opt-out and instruct them not to further sell the information. The business shall notify the consumer when this has been completed.[20]

This newly formed requirement is problematic and would apply retroactively without a clear indication that the Legislature intended it.

"New statutes are presumed to operate only prospectively absent some clear indication that the Legislature intended otherwise." *Elsner v. Uveges*, 34 Cal. 4th 915, 936 (2004). The Attorney General should eliminate this requirement.

C. Requiring Businesses to Treat Unverified Requests to Delete as Valid Opt-Out Requests is Inconsistent with Consumer Rights.

The Regulations provide:

> For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified and shall instead treat the request as a request to opt-out of sale.[21]

This new requirement is not found in the CCPA and further inhibits a consumer's ability to control the use and dissemination of their personal information rather than to accommodate the consumer's original intent—to have the personal information deleted.[22] Moreover, it does not consider situations where a business was not selling data in the first place, meaning there is nothing from which to opt out.

---

[20] 11 CCR §999.313(f).

[21] 11 CCR §999.313(d)(1).

[22] Initial Statement of Reasons (ISOR), *H. 11 CCR § 999.313. Responding to Requests to Know and Requests to Delete. Subdivision (d)(1).* "The subdivision also benefits consumers by requiring the business to view the request in a way that can best accommodate consumer's intent to delete the information."

The Regulations also do not take into account the likelihood that businesses may be subject to automated bot attacks via the "Do Not Sell My Personal Information" button/link on the homepage. Small businesses lacking in resources to monitor for these kinds of attacks would be most significantly impacted. Such automated bot requests will have to be reviewed for verification; if the request cannot be verified, a consumer who never even submitted the request in the first place, will be opted-out of the sale. The Attorney General should remove this requirement to safeguard consumer choice and power over their personal information.

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

The Regulations provide:

> The purpose of the notice of right to opt-out of sale of personal information is to inform consumers of their right to direct a business that sells (*or may in the future sell*) their personal information to stop selling their personal information, and to refrain from doing so in the future.[23]

This subdivision is problematic because the emphasized portion implicates businesses not contemplated by the CCPA. In fact, it is inconsistent with the CCPA, which only requires businesses currently selling (not those that might sell) personal information to provide the notice of the right to opt out of the sale of personal information.[24]

The Association finds that this language is inconsistent with the CCPA, which seeks to promote transparency on the part of businesses to the benefit of consumers. If businesses that might potentially sell personal information in the unknown and distant future are required to also put up the notice of the right to opt-out, it will be unclear to consumers which businesses are actually selling and not selling personal information.

There is also a strong concern that requiring businesses to maintain a "Do Not Sell My Personal Information" button, even when not selling personal information, further convolutes the number of opt-out links and buttons consumers are going to see across the majority of online sites and in brick-and-mortar stores that they visit. The fear is that the true bad actors—entities who only want to collect and sell personal information for their own benefit—will get lost in the mix and consumers will not be able to make informed decisions regarding when they should and should not opt out.

The Association recommends that the Attorney General remove "or may in the future sell" from §999.306(a)(1) of the Regulations.

---

[23] 11 CCR §999.306(a)(1) (*emphasis added*).

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

E. The Attorney General Should Clarify the New Obligation Under the Regulations that Requires Businesses that Do Not Post a Notice of Right to Opt-Out to Treat Information Collected as a Request to Opt-Out.

The Regulations provide:

> A consumer whose personal information is collected while a notice of right to opt-out notice is not posted shall be deemed to have validly submitted a request to opt-out.[25]

This obligation is unnecessary and overreaching because it again makes an assumption that consumer data should be treated as opted-out even though the consumer never actively made such a request. As with the challenges raised by the new requirement that user-enabled privacy setting being treated as opt-out requests, this subdivision is difficult to reconcile with other provisions of the CCPA[26] and Regulations.[27] A business has no way to contact the consumer to confirm that third parties have been instructed not to sell the personal information or to provide the consumer will the ability to globally opt-out of this non-existent sale.

Further, if a retailer makes the decision to start selling personal information and puts up a notice of the right to opt-out, retailers will have no way of knowing who visited the site before the notice was posted and after the notice was posted. As such, the Association strongly recommends the Attorney General remove this subdivision from the Regulations and instead recognize that the CCPA and the Regulations already make it sufficiently clear that personal information collected without a notice of the right to opt-out cannot be sold. Alternatively, if the Attorney General chooses not to remove the subdivision from the Regulations, the Association asks the Attorney General to establish a safe harbor such that businesses that do not sell personal information but fail to post a notice of right to opt out are not in violation of the CCPA or Regulations.

---

[25] 11 CCR §999.306(d)(2).

[26] CIV. CODE §1798.135(a)(1)(B)(5). A business shall, "For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that a consumer authorize the sale of the consumer's personal information."

[27] 11 CCR §999.316(a) and (b). "(a) Requests to opt-in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in. (b) A business may inform a consumer who has opted-out when a transaction requires the sale of their personal information as a condition of completing the transaction, along with instructions on how the consumer can opt-in."

F. Businesses that Inform Service Providers and Third Parties that a Consumer has Opted Out of the Sale of Personal Information Should be Deemed to be Compliant Regardless of What the Service Provider or Third Party Does in Response to the Notice.

The CCPA and Regulations require businesses to inform service providers, and certain third parties, when a consumer has made a request to opt-out of the sale of personal information. Unfortunately, there is not an industry consensus on what exchanges of personal information are, and are not, considered a sale for CCPA purposes. Given this uncertainty, it would be easy for certain venders to continue with the exchange of a consumer's personal information even following a retailer's instruction regarding a consumer opt-out.

The Association recommends that the Attorney General provide a clear understanding in the Regulations that by informing service providers and third parties of the opt-out request, businesses have fulfilled their duties under the Regulations and the CCPA, regardless of whether the third parties and service providers honor such requests as instructed by the retailer.

V. The Regulations Create Several New Obligations and Requirements For Businesses and the Attorney General Should Provide Additional Clarification.

A. Businesses Should Have 90 Days From the Date a Request is Verified to Comply With the Request.

The Regulations provide:

> Businesses shall respond to requests to know and requests to delete within 45 days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request. If necessary, businesses may take up to an additional 45 days to respond to the consumer's request, for a maximum totally of 90 days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.[28]

The proposed Regulations also set forth very extensive verification requirements for requests to know and requests to delete that make it almost impossible to verify without doing a case-by-case analysis.[29] For example, for each request received, retailers will need to consider all the different categories of information collected, the type of request received, the sensitivity and value of the personal information, the degree of certainty needed, how that degree of certainty is established, and the risk of harm by unauthorized access or deletion. Depending on the number of requests a retailer receives, especially small retailers not equipped to handle a high volume of requests, the 45-day window may be difficult for many retailers to manage a substantive response.

---

[28] 11 CCR §999.313(b).

[29] *See generally* 11 CCR §§ 999.323-999.326.

In addition, as the Attorney General points out in the Initial Statement of Reasons,[30] the CCPA contains two contradictory timeframes with respect to responding to consumer requests to know and delete.[31]

The Attorney General's reason for only permitting 45 days and no more than 90 days to respond is based on the average consumer notification time for data breaches.[32] This comparison is logically fallacious. Unlike consumer notifications in data breaches, individual requests for information involve extensive and time consuming verification obligations, and businesses must draft individualized responses. Further, data breach notifications are time sensitive because consumers are most likely unaware that a third party has accessed their personal information and that they need to take immediate action to mitigate the risks associated with this unauthorized access.

The Association recommends the Attorney General revise the Regulations so that the response period will begin at the time a request is verified and businesses will then have 90 days to substantively respond to the request with an additional 90 days when reasonably necessary, provided the business puts forth a good-faith effort to verify the request in a timely fashion.

B. Businesses Should Not be Required to Respond to Requests Submitted Via Non-Designated Methods.

The Regulations provide:

> If a consumer submits a request in a manner that is not one of the designated methods of submission…the business shall…treat the request as if it had been submitted in accordance with the business's designated manner, or provide the consumer with specific directions on how to submit the request…"[33]

---

[30] Initial Statement of Reasons (ISOR), *IV.H. 11 CCR §999.313(b). Responding to Requests to Know and Requests to Delete*.

[31] CIV. CODE 1798.130(a)(2). "Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer…[t]he time period to provide the required information may be extended once by an additional 45 days when reasonably necessary…" *See also*. CIV. CODE 1798.145(j)(1). "A time period for a business to respond to any verified consumer request may be extended by up to 90 additional days where necessary…"

[32] California Department of Justice, Attorney General's Office, *California Data Breach Report* (February 2016), p. 25.

[33] 11 CCR §999.312(f).

This obligation goes beyond the scope of the Attorney General's regulatory power as such an requirement is not contemplated by the statute.[34] This new obligation would require businesses to timely respond to requests received via methods that were not anticipated by the business. For example, requests received through the mail or a voicemail left on a corporate phone number not actively monitored by an employee trained to handle requests would need to be responded to in a timely fashion. This presents an operational nightmare as businesses will need to conceive of every possible way a request could come to the business that is not designated.

Instead, the Association recommends removal of this obligation from the Regulations since both the CCPA and Regulations require businesses to provide several designated methods and to also provide a designated method that reflects how they substantially interact with consumers.

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

The Regulations provide:

> Where a consumer does not have a password-protected account with a business, a business may respond to a request to delete as it pertains to household personal information by providing aggregate household information, subject to verification requirements set forth in Article 4.[35]

The average household size is 2.6 people.[36] It is unclear how any business could provide household information on an aggregated basis for 2.6 people. It is fundamentally inconsistent with the language and the spirit of the CCPA.

As numerous businesses have pointed out to the legislature and to the Attorney General, allowing one member of a household to obtain information about other individuals in the household – even in "aggregated" form –puts the privacy and safety of those household members at risk. The Attorney General should remove subsection (a) and instead require that all consumers of a household jointly request information (as provided in subsection (b)).

---

[34] CIV. CODE 1798.140(i) (where the Legislature defined "designated methods for submitting requests" and provided the Attorney General with the power to approve "any new consumer-friendly means of contacting a business" rather than the power to require businesses to accept requests made through any and all non-designated means).

[35] 11 CCR §999.318(a).

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

VI. The Attorney General Should Remove the Obligation to Publicly Disclose Certain Business Records.

The Regulations provide explicit metrics reporting requirements for businesses "that alone or in combination, annually buy[], receive[] for the business's commercial purposes, sell[], or share[] for commercial purposes, the personal information of 4,000,000 or more consumers."[37]

The Association appreciates the importance of recordkeeping but has several concerns regarding the obligation to disclose such metrics annually in the privacy policy.[38] These concerns include, much like financial incentives, that disclosing such metrics in the privacy policy forces businesses to publish proprietary information. Competitors will be able to view these metrics and make judgments about, for example, the health of the disclosing business, based on the number of requests to delete and requests to opt-out that were received and processed.

The Association encourages the Attorney General to strike §999.317(g)(2) from the Regulations and permit businesses subject to this subdivision to maintain such records privately and make them available to the Attorney General on request.

VII. The Attorney General Should Remove Internet Service Providers and Social Networks From the Definition of "Categories of Third Parties."

The Regulations provide:

> "Categories of third parties" means types of entities that do not collect personal information directly from consumers, including but not limited to advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers.[39]

The Association submits that the determination of whether an entity is an internet service provider or social network should be based on the facts of each case, and is concerned that the broad regulatory designation of these types of entities as "categories of third parties" is misguided and factually inaccurate. The Association recommends the definition of "categories of third parties" not include any list of entity categories that are, *per se*, deemed to be "categories of third parties."

---

[37] 11 CCR §999.317(g)(1).

[38] 11 CCR §999.317(g)(2). "Disclose the information compiled in subsection (g)(1) within their privacy policy posted on their website and accessible from a link included in their privacy policy."

[39] 11 CCR §999.301(e).

VIII. Businesses Should be Permitted to Use Personal Information Kept for Record-Keeping Purposes for Other Limited Administrative Purposes Permitted Under the CCPA.

The Regulations provide:

> Information maintained for record-keeping purposes shall not be used for any other purpose.[40]

This does not take into account that businesses may need to use the information collected and retained under the above subdivision for other purposes consistent with the objectives of the CCPA such as for conducting analytics, preparing reports for the business pertinent to CCPA administration, risk management, and compliance.

The Association encourages the Attorney General to adopt such a carve-out to allow a business to use information kept for purposes of compliance with §999.317 for other purposes contemplated in the CCPA and Regulations.

IX. Conclusion

The Association thanks the Attorney General's Office for its hard work and dedication to the development of the proposed Regulations, and looks forward to the opportunity to continue working with the Attorney General on privacy issues.

Sincerely,

Rachel Michelin
President & CEO
California Retailers Association

[40] 11 CCR §999.317(e).