



March 8, 2019

Via Email to PrivacyRegulations@doj.ca.gov

California Department of Justice
Attn: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, California 90013

Re: NRF & CRA Joint Comments on CCPA during the Pre-Rulemaking Process

Dear Attorney General Becerra:

The National Retail Federation and California Retailers Association appreciate the opportunity to jointly submit comments to the California Department of Justice as part of the Attorney General's pre-rulemaking process under the California Consumer Privacy Act (CCPA). The Attorney General's Office has an enormous responsibility regarding the CCPA to fulfill within a very short timeframe. The purpose of these comments is to provide the perspective of the retail industry on several of the areas within the Attorney General's rulemaking authority relating to the new privacy standards established by the CCPA.

The National Retail Federation is the world's largest retail trade association. Based in Washington, D.C., NRF represents discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the nation's largest private-sector employer, supporting one in four U.S. jobs — 42 million working Americans. Contributing \$2.6 trillion to annual GDP, retail is a daily barometer for the nation's economy.

The California Retailers Association is the only statewide trade association representing all segments of the retail industry including general merchandise, department stores, mass merchandisers, restaurants, convenience stores, supermarkets and grocery stores, chain drug, and specialty retail such as auto, vision, jewelry, hardware and home stores. CRA works on behalf of California's retail industry, which currently operates over 418,840 retail establishments with a gross domestic product of \$330 billion annually and employs 3,211,805 people—one fourth of California's total employment.

A. THE ATTORNEY GENERAL'S AUTHORITY UNDER THE RULEMAKING PROCESS

The CCPA designates the Office of the Attorney General as an essential partner in the development and enforcement of the new law. The statute expressly authorizes businesses to request

advisory opinions from the Attorney General.¹ The Attorney General’s office has broad enforcement authority and the ability to recover sizable penalties for violations of the Act.² Consumers must effectively seek Attorney General approval before proceeding with private civil actions under the CCPA.³

The CCPA also requires the Attorney General to “solicit broad public participation and adopt regulations to further the purposes of the [statute].”⁴ The statute provides several examples of areas to be addressed as part of this rulemaking activity. These areas are listed in the Public Forum Materials⁵ published by the Attorney General’s Office for the instant pre-rulemaking process. Our comments cover the following listed areas:

1. Categories of Personal Information (*See* Part B.3(b).)
2. Exceptions to CCPA (*See* Part B.1.)
3. Submitting and Complying with Requests (*See* Parts B.3(b), B.3(d).)
4. Notices and Information to Consumers, including Financial Incentive Offerings (*See* Part B.1.)

The CCPA makes clear that the topics set out in the statute are not an exclusive list. The law states that the Attorney General “shall . . . adopt regulations to further the purposes of this title, **including, but not limited to**, the [listed] areas.”⁶ We accordingly have included additional discrete areas⁷ that we suggest the Attorney General should include in its rulemaking efforts in order to “further the purposes of the [CCPA].”⁸ If, in the Attorney General’s determination, he lacks the authority to address these concerns in the rulemaking, we would appreciate his efforts to work with the legislature to support statutory amendments that would address these additional discrete areas.

B. COMMENTS ON DISCRETE AREAS OF THE CCPA

1. Preserving Consumer Benefits from Customer Loyalty and Discount Programs

Protecting consumer privacy is one of retailers’ highest priorities. Retailers know that establishing long-term relationships with their customers requires more than just providing the merchandise they want at the prices they are willing to pay. Successful retailers win their customers’ trust and provide a satisfying shopping experience so that consumers continue to shop with them time and again. A critical element of establishing that trusted relationship lies in how retailers act as reliable stewards of the information their customers share with them when shopping.

Retailers have a long history of nurturing customer relationships and meeting consumer expectations for high quality service. Whether offering goods online or in store, retailers use customer data to provide personalized experiences that consumers value. Customers, in turn, expect retailers to process their personal data responsibly and seamlessly when they are shopping. To meet

¹ Cal. Civ. Code § 1798.155(a).

² Cal. Civ. Code § 1798.155(b).

³ Cal. Civ. Code § 1798.150(b)(2).

⁴ Cal. Civ. Code § 1798.185(a).

⁵ <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-forum-ppt.pdf>

⁶ Cal. Civ. Code § 1798.185(a) (emphases added).

⁷ *See* Parts B.2, B.3(a) and B.3(c) below.

⁸ Cal. Civ. Code §§ 1798.185(a), (b).

these high customer expectations, retailers invest heavily in technology and spend years developing appropriate methods to comply with state, federal and global data protection regulations in ways that further their customer relationships and do not frustrate them.

In short, retailers use consumer data for the principal purpose of serving their customers as they wish to be served. Retailers' use of personal information is not an end in itself but primarily a means to achieving the goal of improved customer service. This differentiates retailers' principal use of customer data from businesses – such as service providers, data brokers and other third parties unknown to the consumer – that primarily collect, process and sell consumer data as a business-to-business service.

An important way that many businesses, including retailers, develop lasting relationships with their customers is by providing tailored service and lower prices than their competitors in the same industry sector. “Club” discount cards, airline travel frequent-flyer rewards, hotel repeat-stay programs, retail discount coupons, advanced product release programs, exclusive V.I.P. customer experiences and other forms of customer loyalty and discount programs are ubiquitous across industry and highly popular among consumers as well. According to a recent study published by Forrester Research, 72% of American adults online belong to at least one loyalty program.⁹ The average number of loyalty program memberships that each adult has is nine.¹⁰

Although the authors of A.B. 375 stated during the bill's consideration that it was not their intent to eliminate consumer loyalty programs, the retail industry is concerned that offers of common loyalty program features and practices could be challenged as alleged violations of the CCPA's restrictions on discrimination.¹¹ The CCPA thus puts extraordinary pressure on these customer-favored programs by creating a significant liability risk for businesses which provide rewards or other benefits, such as preferred service or pricing, to customers who sign up for these programs.

If not addressed in the rulemaking or by statutory amendment, the CCPA's existing express prohibition on “charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties”¹² would create a substantial risk of liability for retailers and other consumer-facing businesses that offer loyalty programs, particularly where some of their customers choose not to participate (*i.e.*, by exercising a right under the CCPA) and a claim may be made that the business then violated the CCPA's nondiscrimination section by offering discount prices or better levels of service to its other customers who choose to participate.

Although the legislature recognized the unintended consequence and potential impact on loyalty programs that Californians wish to preserve, it failed in its attempt to create a savings clause that insulates these favored programs from other acts of prohibited discrimination and retaliation against consumers who may exercise a right under the CCPA. Because the statutory language fails to fully correct and guard against the unintentional impact on programs that benefit consumers, we urge

⁹ Forrester Research, *How Consumers Really Feel about Loyalty Programs*, May 8, 2017.

¹⁰ *Id.*

¹¹ Cal. Civ. Code § 1798.125(a) (“A business shall not discriminate against a consumer because the consumer exercised and of the consumer's rights under this title, including, but not limited to, by . . . charging different prices or rates for goods or services, including through the use of discounts or other benefits . . .”).

¹² Cal. Civ. Code § 1798.125(a)(1)(B).

the Attorney General to address this concern in its interpretation of Section 1798.25 of the CCPA and to support statutory changes necessary to correct this mistake in the law.

One way the CCPA currently fails to protect customer loyalty programs is its creation of a novel and uncertain comparative valuation test for hundreds of thousands of businesses – mostly small and mid-sized businesses serving Californians – that already offer discounted goods or preferred services to customers. This new legal mechanism to justify common commercial behavior regarding discounts and service sets a potential litigation trap to be tested in the courts, requiring legal resources most small and mid-sized businesses do not have simply to preserve what are essentially discounts and preferred service programs for their customers.

Under the CCPA, as currently drafted, any practices or programs through which businesses provide preferred service or pricing to their customers who want them, when other customers exercising rights do not wish to participate, are permitted to keep these programs only so long as they can prove that the “value” of the personal information to the participating consumer used by the business is met by an equivalent value in discounts or benefits received by them.¹³ This is a legal equation fraught with such ambiguity that it invites an infinite array of “economic” opinions for state courts to weigh in potentially protracted class action litigation.

The value of personal information that may be “priceless” in one consumer’s eyes would never equate subjectively to a reasonable discount on a product. The potential for litigation over this most basic of retail transactions could lead some stores to shut down loyalty programs altogether – or not make them available to Californians – because the CCPA creates an untenable business litigation risk. These stores reasonably could determine that the potential costs of lawsuits testing the meaning of this part of the statute outweighs the potential benefits to the business from providing better service and discounts to their most loyal customers.

For example, assume a consumer requests a retailer to delete any personal information it collected from her.¹⁴ The retailer must comply subject to certain limited exceptions.¹⁵ But what if this same consumer participates in a loyalty program offered by the retailer which provides rewards based on the quantity or dollar value of prior transactions? The data necessary to measure past purchases will no longer be linkable to the consumer, thus impacting the consumer’s entitlement for discounts or rewards under the program. Does this constitute impermissible discrimination under Cal. Civ. Code § 1798.125(a)?

Private label credit cards tied to discounts or coupons provide another example. Assume our consumer opts out of data sales by the retailer pursuant to Cal. Civ. Code § 1798.120. Assume this same consumer has a private label card from the retailer which awards coupons based on monthly spend. Does the retailer sell personal information to the issuing bank when reporting transaction volumes? Does the bank sell personal information to the retailer by issuing coupons to the consumer that the consumer later uses at the store or online?

The retail industry would of course contend these scenarios do not violate the CCPA, but it is likely these questions, and many other similar scenarios raised by common loyalty

¹³ Cal. Civ. Code § 1798.125(a).

¹⁴ Cal. Civ. Code § 1798.105(a).

¹⁵ Cal. Civ. Code § 1798.105(c).

program features and operations, will be resolved only through litigation due to the lack of clarity in Section 1798.125. This concern is heightened by the recent proposal in S.B. 561¹⁶ to amend the CCPA to establish a private right of action with statutory damages for any violation of the law. Plaintiffs’ attorneys would have a powerful incentive to initiate class action proceedings to test the bounds of the CCPA.

We urge the Attorney General to consider the potential litigation that could arise over any provision that conditions the offering of a loyalty program on the “value” of personal information in light of the infinite number of “economists” who might be certified by courts as experts to opine on ranges in value that could be as different as night and day for the same data set. The intent of this provision was not to threaten these programs that consumers love. We therefore ask the Attorney General to clarify in its regulations that consumer loyalty programs and practices providing better prices or service to customers who desire them are exempt from the nondiscrimination provisions of Cal. Civ. Code 1798.125(a) and are not required to meet the financial incentive program standards of Section 1798.125(b). Such clarification would ensure that the CCPA does not lead to the obsolescence of loyalty programs for Californians.

2. Right-Sizing CCPA Enforcement and Penalties to the Severity of the Violation

(a) Proposed Policy Considerations for Interpreting the Text of the CCPA’s Private Right of Action and Statutory Damages

The CCPA establishes a new private right of action and statutory damages for certain data security incidents that result from the business’s failure to satisfy its statutory duties with respect to information security.¹⁷ Claimants may recover damages of between \$100 and \$750 per consumer per incident or actual damages, if greater.¹⁸ Courts are not authorized to award damages less than \$100 per consumer, per incident. Some quick calculations make clear that this restriction on judicial discretion can result in enormous and financially ruinous damage awards without regard to the size of the business, the circumstances of the breach, or mitigating factors such as the good faith or level of cooperation of the business.

For example, an online business that has one million California customers (a modest number by e-commerce standards) could face a *minimum* of a one billion dollar fine for a violation of the data security provision in light of the \$100 per consumer per incident calculation established by statute. A statutory penalty such as this far exceeds any penalty seen anywhere else in the world for privacy violations. Under the European Union’s General Data Protection Regulation (GDPR), for instance, a company’s annual total global revenue would need to be at least \$25 billion to be at risk of facing a one billion dollar fine.

We respectfully request that the Attorney General consider establishing a rule that creates a per-incident cap on the aggregate statutory damages a business may face under the CCPA. The capped amount could be established by reference to the size of the business – a model that would align with the approach adopted by the GDPR.¹⁹ The GDPR authorizes EU data protection

¹⁶ S.B. 561 (Cal. 2019).

¹⁷ Cal. Civ. Code § 1798.150(a)(1).

¹⁸ Cal. Civ. Code § 1798.150(a)(1)(A).

¹⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

authorities to assess administrative fines, but these fines are capped at the greater of €20 million or 4% of global annual revenue.²⁰ Uncapped statutory damages calculated based solely on the number of consumers creates virtually unlimited financial exposure for businesses that are not malicious or reckless bad actors, but rather are the victim of often highly sophisticated financial fraud and computer crimes that lead to data security breaches.

In addition, minimum statutory damages (currently set at \$100 per consumer, per incident) create the potential for ruinous financial impact when a different response may be more appropriate. Consider a recent situation in Germany in which a hacker acquired account passwords that a German social media company, Knuddels, had maintained in clear text.²¹ The hacker used these account credentials to steal the information of approximately 1.91 million users, including 808,000 email addresses. Under the CCPA, Knuddels could face statutory damages totaling between \$191 million and \$1.423 **billion**.

The outcome under the GDPR was different, however. The company in Germany was motivated to exhibit significant cooperation with the regulator and to implement recommendations and guidelines of the data protection authority. The regulator in response ultimately assessed a fine of €20,000. Knuddels remained in business, and customer data protections were enhanced. We think this is a more reasonable and practical approach that encourages companies to cooperate with regulators and allows the regulators to assess fines based on the entirety of the facts related to a statutory infringement. We therefore request the Attorney General through the rulemaking process establish a rule that removes the \$100 per consumer, per incident floor on statutory damages. This would afford the courts the discretion to consider the circumstances surrounding a breach, including any mitigating factors, in assigning a damage award to a business.

We look forward to working with the Attorney General to address these concerns with the CCPA's private right of action and statutory damages, and appreciate his consideration of the alternative solutions offered above. If the Attorney General believes that a cap or removal of the minimum statutory amount is warranted but beyond his rulemaking authority, then we would respectfully request the Attorney General support efforts in the legislature to make such statutory modifications as necessary to address the concerns raised above.

(b) Concerns with Provisions of S.B. 561 that would Amend the CCPA's Enforcement Section

The Attorney General has announced support for S.B. 561, introduced in the State Senate on February 22, 2019. This bill, if enacted into law, would (a) expand the CCPA's private right of action and statutory damages to apply to *any* violation of the Act, however minimal; (b) remove the period of time in which businesses may cure alleged noncompliance before being deemed in violation of the law; and (c) withdraw the right of businesses to seek advisory opinions from the Attorney General. While we believe the CCPA's provision on seeking advisory opinions provides a very useful mechanism for delivering helpful guidance to California consumers and businesses, we are more concerned that the proposed extension of the private right of action and the inability to cure

²⁰ GDPR, Art. 83(5). Less significant infringements are subject to a cap equal to the greater of €10 million or 2% of global annual revenue. GDPR, Art. 83(4).

²¹ <https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/02/LfDI-34.-Datenschutz-Tätigkeitsbericht-Internet.pdf>

alleged noncompliance (i.e., the first two elements of S.B. 561 noted above) would create disproportionate liability risk and financial harm to the retailers and other businesses in California. We therefore respectfully request the Attorney General consider the potential consequences of S.B. 561, in the form as introduced, and the policy concerns it raises.

(i) *Expanding the Private Right of Action and Statutory Damages to the Entire CCPA Would Create Disproportionate and Misplaced Liability Risks for Businesses*

A private right of action applying to the entirety of the CCPA is incapable of addressing the fact that not every violation of the CCPA will be equal, and that the consequences and impact on consumers may vary greatly depending on the nature of the violation, the size and nature of the company, the data that was implicated and other factors. The CCPA already allocates greater liability – in the form of the private right of action that exists today – to data security breaches. Other violations of the Act, though, are subject to enforcement by the Attorney General. We believe the Attorney General’s oversight here can provide for a more even-handed approach to CCPA enforcement, particularly with respect to the untested privacy provisions that businesses will need to address through new compliance programs under the statute.

With respect to data security breaches, where the CCPA already provides a private right of action, it should be noted that businesses have had over 15 years of experience with breach notification law in California and there is greater familiarity with the relevant legal standards. Maintaining the role of the Attorney General to exercise prosecutorial discretion with enforcement of a new comprehensive statute requiring extensive modifications to customer data systems and processes is vital to ensuring that CCPA enforcement and penalties are proportionate to the alleged violations of the Act.

This distinction between major and minor violations of a privacy law have precedent and are also consistent with the approach adopted by the GDPR. More significant violations of the GDPR are subject to administrative fines capped at the greater of €20 million or 4% of global annual revenue. Less significant violations, though, are subject to a cap equal to the greater of €10 million or 2% of global annual revenue. In this way, the GDPR attempts to right-size the range of penalties to the severity of the potential violation of the rules.

Expanding the private right of action to the entire law will make it more difficult for well-intentioned businesses to balance CCPA compliance with consumer privacy and data security requirements in the face of potential litigation over how they interpret and implement mechanisms in the face of competing requirements of the law. Here are two examples for your consideration that illustrate this point:

- (A) *Identify verification for data access requests:* As businesses that have tried to do so are keenly aware, it is very challenging to verify the identity of customers in a manner that is not overly burdensome to the consumer and does not require a customer to provide even more sensitive information about themselves (e.g., a copy of their driver license or passport) to authenticate who they are. In efforts to improve identity verification, businesses are trying to find the correct balance between the consumer’s ability to easily access data and their right to privacy. For example, a customer-friendly way to verify identity is to have a customer provide an email address to which the business can then

send a verification message. Since this is not the most secure or reliable way to verify identity, however, the retailer using this process may mask sensitive data fields like credit card numbers. With a private right of action potentially being extended to the verification practices businesses adopt to comply with the CCPA, an enterprising plaintiff's lawyer will allege that the business in the example above failed to provide the actual data to the consumer – the data that was masked – even though there is no harm to the customer from such security measures but rather a benefit in terms of security. This scenario could leave businesses forced either to provide the sensitive data to a person that may not be the actual customer, or to put in place more burdensome identify verification requirements to ensure that it only sends data to verified customers after a more thorough process.

- (B) *Deleting data that is contained in logs and backups*: Retaining security logs is a proven method for putting a business in position to quickly identify potential data breaches and prevent them. Security logs often include personal information, especially given the very broad definition of what constitutes personal information under the CCPA. If businesses were to prematurely begin to delete these security logs for fear of facing frivolous lawsuits, the personal information of these customers will be less secure as a result. The CCPA exempts certain security logs from the data deletion requirement but the language is too narrowly crafted. As it stands, it may be difficult for businesses to demonstrate which security logs are truly needed to detect security incidents and which are kept for other reasons.

In these instances, it is critical that Attorney General oversight – and not private rights of action – are the enforcement mechanism to ensure that well-meaning businesses acting in good faith to comply with the CCPA's competing requirements will not be hamstrung in their implementation. The enforcement mechanism should not leave such businesses feeling forced – for fear of facing unwarranted plaintiffs' actions – to require consumers to engage in more burdensome practices to verify their identity than might otherwise be required. Without a private right of action, businesses could have greater certainty in these situations that the Office of Attorney General understands the technical difficulties in compliance and the reasonable efforts of businesses to get it right. This would permit greater innovation in complying with the CCPA – to the benefit of consumers – by removing the threat of litigation from every aspect of compliance.

The privacy standards established in the CCPA are new, not entirely clear (as evidenced by the legislature granting a right for businesses to request advisory opinions from the Attorney General), and have not been tested in the courts. The retail industry, like other California businesses, is deeply concerned about the prospect for class action litigation exposure arising from good faith business practices in this “grey area” or bankrupting levels of statutory damages that courts have no discretion to lower from simply immaterial, technical violations that do not cause harm to consumers. We submit that enforcement of new, comprehensive data privacy provisions in California is a field much more suited to informed Attorney General oversight and enforcement than to enterprising class action lawyers.

(ii) *Elimination of a 30-Day Right to Cure Alleged Violations Creates Disincentives for Businesses*

The CCPA grants businesses the right to cure alleged statutory violations “[i]n the event a cure is possible.”²² Successfully curing a practice within thirty days after notice of the violation bars an individual action or class action for statutory damages. This approach provides a strong incentive for potential plaintiffs to disclose their complaint clearly to potential business defendants. More importantly, it also provides a strong and effective incentive to businesses to quickly address alleged violations within the thirty-day time frame. Without the right to cure under the CCPA, trial lawyers will continue their practice of sending vague demand letters or filing broad complaints of alleged violations that often rely on “information and belief” claims and do not give well-intentioned businesses enough information to address any alleged violations that may be legitimate compliance issues. Businesses will also be reasonably concerned that remediation measures could be used against them in the resulting lawsuit. This may create a financial disincentive to acknowledge and fix issues that impact the privacy rights of consumers – something that would be more likely if the 30-day right to cure were maintained.

We appreciate the Attorney General’s consideration of the concerns discussed above with these two elements of S.B. 561. We submit that the introduction of a broad private right of action will have a disproportionate impact on businesses without corresponding benefit to consumers. Further, the elimination of the thirty-day cure prior may put consumers in a worse position by chilling businesses’ efforts to innovate and work cooperatively with the Attorney General on compliance.

3. Clarifying the CCPA’s Key Definitions

We respectfully request that the Attorney General, under its authority granted in the CCPA, use the rulemaking process to provide much-needed clarity to consumers and industry alike on certain key definitions in the statute before the law would take effect. We have focused on the following four definitions that our members believe are the most pressing ones to get right so that businesses may comply with the CCPA having much greater certainty as to the scope of the law than they presently have.

(a) The Definition of “Sell,” “Selling,” “Sale” or “Sold”

The CCPA defines a “sale” of personal information in a manner that captures any arrangement in which a business not only sells but “rent[s]” or “mak[es] available” personal information “for monetary or other valuable consideration.”²³ The breadth of this definition captures many types of data-sharing arrangements that are necessary in today’s retail environment, are not viewed by consumers as a “sale” of data, and do not implicate the policy issues underlying the CCPA’s “do not sell” right. For example:

²² Cal. Civ. Code § 1798.150(b)(1).

²³ Cal. Civ. Code § 1798.140(t)(1).

- A small retailer may use a customer list to mail coupons on behalf of different brands stocked in its store. Has the retailer “ma[de] available” to the brands its personal information for “valuable consideration”?
- Retailers continue to invest in digital operations to survive and grow in an increasingly competitive industry. This requires engagement with digital advertising and analytics firms that routinely require the ability to retain data to improve their products and services. Does such retention constitute a “sale” under the CCPA?
- Fraud detection and prevention technologies are also essential in ecommerce operations. The CCPA permits the sharing of personal information to enable a vendor to detect fraudulent or illegal activity.²⁴ But fraud detection providers routinely retain the ecommerce information they process for customers to enhance their own databases for use to deliver services to other businesses. Once again, it’s unclear how this beneficial practice to consumers may be interpreted under the CCPA – if it is a “sale” of data from which consumers may opt out, they would have less anti-fraud protection (*i.e.*, a perverse result.)

We submit that these scenarios do not and should not qualify as sales of personal information. Absent clarification of the definition of “sale” by the Attorney General through its rulemaking authority, these questions can only be answered definitively by the courts. We therefore respectfully request that the Attorney General exercise his authority to establish under the CCPA a narrowly-tailored interpretation of the definition of “sale” that requires monetary consideration.

(b) The Definition of “Consumer”

The traditional definition of a consumer is an individual who is purchasing or interested in the purchase of goods or services for personal, family or household purposes.²⁵ The CCPA, however, defines a consumer as any resident of the State of California.²⁶ This means that the California Consumer Privacy Act applies not only to personal information about consumers in the traditional sense, but also to data about employees, contractors and other individuals.

One consequence of this provision – which could be a mere statutory drafting error – is that businesses will now be required to create and publish employee privacy policies on their Internet home page.²⁷ The extension of the CCPA to employees also creates profound issues relating to the deletion of data. Employees cannot operate in an environment of anonymity, which is anathema to existing law with respect to expectations of privacy in the workplace.

We therefore respectfully request the Attorney General clarify the definition of “consumer” to exclude employees under the authority granted to him in Cal. Civ. Code § 1798.185(b) to promulgate regulations generally “as necessary to further the purposes” of the CCPA.

²⁴ Cal. Civ. Code § 1798.140(d)(2).

²⁵ *See, e.g.*, 15 U.S.C. § 2301(3).

²⁶ Cal. Civ. Code § 1798.140(g).

²⁷ Cal. Civ. Code § 1798.130(a)(5).

(c) The Definition of “Personal Information” and its Inclusion of “Households”

Whether data constitutes “personal information” is the threshold for determining if consumer data is subject to the requirements of the CCPA. Clarity and precision in the definition of personal information is critical for retailers and other businesses to build effective privacy compliance programs under the new law. Any proposal to introduce new categories of personal information or otherwise to interpret the definition pursuant to Cal. Civ. Code 1798.185(a)(1) should therefore be undertaken only with great care.

The GDPR can serve as a helpful reference point in the Attorney General’s consideration of the proper interpretation of this definition. The Regulation defines personal data as information relating to an identified or identifiable natural person.²⁸ The CCPA, however, extends beyond this generally-accepted global definition of personal information to include information that can be linked to a “household” – an undefined term in the CCPA that commonly refers to a dwelling with one or more individuals who may be related or unrelated in a familial sense. This has caused significant confusion and, worse, creates a host of implementation concerns when it comes to determining which data is covered by the CCPA.

It is notable that the statute does not define a household because most businesses do not think of their customers in these terms with respect to protecting and honoring requests regarding consumer information. Many retailers and other businesses are therefore, for the first time, trying to identify information in their control that could be linkable to “households,” a term which presumably includes multiple persons.

Most importantly, a definition of personal information that includes data linkable to a household will create challenges for businesses to honor consumer requests for access, portability and deletion of personal information. Businesses are concerned that producing information linkable to a household may result in data getting into the wrong hands. For example, if a college fraternity or religious order constitutes a household, and any member of the household has the right to request specific pieces of information linked to the household, it may create even greater privacy risks and harms to consumers (i.e., other members of the household). Other scenarios can be envisioned where roommates or families with adult children living at home with their parents create similar risks of harm to *individual* privacy.

Retailers and other businesses are therefore faced with an impossible choice – produce specific pieces of personal information in response to a request that relates to multiple individuals living together in a household, which likely results in a privacy incident, or do not produce the information at the risk of being subjected to an Attorney General enforcement proceeding or a class action lawsuit, should S.B. 561 become law as presently drafted.

For these reasons, we strongly urge the Attorney General to take all steps necessary, pursuant to Cal. Civ. Code 1798.185(a)(1), to resolve the uncertainty of this definition and to address the potential of greater privacy harms that may result by establishing through its rulemaking that the definition of personal information relates to identified persons and excludes “households.”

²⁸ GDPR, Art. 4(1).

(d) The Meaning of “Specific Pieces of Information.”

As noted in the examples above, consumers may request and, upon receipt of a verifiable consumer request, a business must disclose to the consumer “the categories and specific pieces of information the business has collected” about the consumer.²⁹ The statute is not clear whether this means businesses must describe both the “categories” and the “specific pieces” of personal information in their possession, or whether the language requires businesses to describe the categories and provide access to the specific pieces of information.

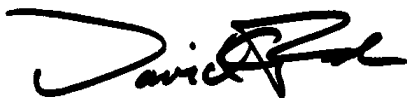
While many interpret the text of the CCPA to provide for the latter, the lack of clarity creates a significant risk of liability for retailers and other businesses, particularly if S.B. 561 is enacted into law. We therefore request the Attorney General, pursuant to his rulemaking authority under Cal Civ. Code §§ 1798.185(a)(7) and 1798.185(b), clarify that the obligation to disclose “specific pieces of information” means businesses must disclose the *categories* of personal information in the business’s control relating to the consumer, subject to applicable conditions and exceptions, rather than to describe each individual piece of information it holds on a consumer.

* * * * *

We appreciate your review of our comments in this letter and look forward to the Attorney General’s continued efforts through the rulemaking process. For any questions or feedback your Office may have concerning our comments, or for more information regarding the concerns of the retail industry more broadly, please contact Paul Martino of the National Retail Federation and Pamela Williams of the California Retailers Association.

Thank you again for the opportunity to provide our views for your consideration at this preliminary stage of the rulemaking process. We look forward to working with you and your staff to address the concerns outlined above.

Sincerely,



David French
Senior Vice President
Government Relations
National Retail Federation



Rachel Michelin
President
California Retailers Association

²⁹ Cal. Civ. Code §§ 1798.100(a), 1798.100(d), 1798.110.