November 8, 2021

California Privacy Protection Agency
Attn: Debra Castanon
915 Capitol Mall, Suite 350A
Sacramento, CA 95814

Dear Ms. Castanon:

On behalf of the California Retailers Association, I am pleased to submit the following preliminary comments in response to your Agency's questions related to the California Privacy Rights Act of 2020.

Our specific responses to Agency questions are listed below; however, I would like to highlight three key issues for retailers at the outset of this proceeding:

- **Automated Decision-Making**: The right to opt out from profiling and automated decision-making should be limited to processing that results in decisions regarding access to healthcare, education, employment, and other essential services and resources. A right for consumers to opt out from all profiling and automated decision-making will disadvantage small to mid-size retailers that do not possess large databases of first-party data, without any corresponding benefit to consumers, and will be a departure from emerging US norms.

  In addition, many retailers will have substantial problems complying with rules on automated decision-making because as a matter of practice, vendors of AI systems do not provide information to retailer clients regarding their algorithms nor does California law obligate processors to do so. As such, all but the largest California-based retailers have no way to force vendors to provide information necessary to a consumer making the request. While large retailers may be able to require their AI or ADM vendors to provide this information contractually, small to mid-sized retailers signing standard form contracts may not have the counsel or leverage to require vendor transparency regarding algorithms or require the vendor to assist the retailer in responding to consumer inquiries. The responsibility for responding to these requests appropriately should fall to the service provider with the information and expertise respond to respond to the requesting consumer appropriately.

- **Dark Patterns**: Consumer trust is paramount for success in the retail world and "dark pattern" practices undermine trust. CRA is supportive of restrictions on behavior that seeks to defraud customers into purchasing items they did not intend or other similar dark pattern tactics. However, those regulations should be narrowly tailored to address truly fraudulent behavior and avoid unintended consequences that would impact traditional retail practices or services that consumers want and expect, such as the highlighting of promotions and discounts consumers can avail themselves of when shopping. Such practices do not limit consumer "choice".

- **Global Opt-Out**: Though the global opt-out remains optional in nature, retailers wish to highlight concerns with the lack of universal standards for global opt-out mechanisms and the substantial implementation challenges. Global opt-out would override any granular opt-in/opt-out decisions made by the same consumer. Retailers will need to know what capabilities they need to turn on and off after receiving such an identifier.

Please see our responses to specific questions below in **BOLD**. If you have any further questions please feel free to contact Steve McCarthy at steve@calretailers.com or (916) 443-1975.

Sincerely,

Steve McCarthy
Vice President, Public Policy

Responses to Questions

1. *Processing that Presents a Significant Risk to Consumers' Privacy or Security: Cybersecurity Audits and Risk Assessments Performed by Businesses*

The CPRA directs the Agency to issue regulations requiring businesses "whose processing of consumers'personal information presents significant risk to consumers' privacy or security" to 1) perform annual cybersecurity audits; and 2) submit to the Agency regular risk assessments regarding their processing ofpersonal information.

Comments on the following topics will assist the Agency in creating these regulations:

a. When a business's processing of personal information presents a "significant risk to consumers' privacy or security."

For many retailers, a risk to consumer information occurs when large amounts of customer data are processed by third-party vendors whose primary purpose is to act as a data processor for the client, as opposed to storing the data or where data processing activities are ancillary to the greater vendor relationship. These data processors should be required to perform assessments and provide audits.

b. What businesses that perform annual cybersecurity audits should be required to do, including what they should cover in their audits and what processes are needed to ensure that audits are "thorough and independent."

No comment.

c. What businesses that submit risk assessments to the Agency should be required to do, including what they should cover in their risk assessments, how often they should submit risk assessments, and how they should weigh the risks and benefits of processing consumers' personal information and sensitive personal information.

Risk assessments should evaluate whether consumer data is used for the business purpose, retained for a finite period of time, and access is limited to those who require it. Where possible, the agency should eliminate unnecessary duplication of risk assessments and accept those assessments performed pursuant to comparable federal or international privacy requirements, or those that may cover multiple processing

operations.

d. When "the risks to the privacy of the consumer [would] outweigh the benefits" of businesses' processing consumer information, and when processing that presents a significant risk to consumers' privacy or security should be restricted or prohibited.

No comment.

2. Automated Decisionmaking

The CPRA provides for regulations governing consumers' "access and opt-out rights with respect tobusinesses' use of automated decisionmaking technology."

Comments on the following topics will assist the Agency in creating these regulations:

a. What activities should be deemed to constitute "automated decisionmaking technology" and/or "profiling"?

b. When consumers should be able to access information about businesses' use of automated decisionmaking technology and what processes consumers and businesses should follow to facilitate access.

Please see initial comments on "automated decisionmaking".

c. What information businesses must provide to consumers in response to access requests, including what businesses must do in order to provide "meaningful information about the logic" involved in the automated decisionmaking process.

At most, retailers who use third-party data processors could provide categories of data used with AI algorithms and purpose for use. A retailer cannot provide meaningful information about the logic involved because the retailer does not develop the AI logic.

d. The scope of consumers' opt-out rights with regard to automated decisionmaking, and what processes consumers and businesses should follow to facilitate opt outs.

Some automated decisionmaking is tied directly to business processes and service offerings. In these situations, an opt-out is akin to a refusal to do business. Businesses should not be required to create separate products for those who opt-out. Consumers retain the effective ability to opt-out by deleting their information and declining to do business with the company.

3. Audits Performed by the Agency

The CPRA gives the Agency the authority to audit businesses' compliance with the law.

Comments on the following topics will assist the Agency in creating regulations to define its auditauthority:

a. What the scope of the Agency's audit authority should be.

No comment.

b. The processes the Agency should follow when exercising its audit authority, and the criteria it should use to select businesses to audit.

Agency audits should prioritize those entities that are high-risk processors, such as companies whose core business is to process data on behalf of other companies and companies involved in large-scale processing of sensitive personal information.

c. The safeguards the Agency should adopt to protect consumers' personal information from disclosure to an auditor.

The regulations should include standards for the secure handling of consumer information, including limitations on access within the Agency, use of encryption, and ensuring data is deleted when it is no

longer needed. The Agency should make tools available to companies selected for audit to allow for the anonymization or de-identification of records before they are delivered to the Agency. Where possible, the Agency should allow entities to fulfill audit information requests rather than sifting through company information.

4. *Consumers' Right to Delete, Right to Correct, and Right to Know*
    a. The new rules and procedures, or changes to existing rules and procedures, needed for consumers to make requests to correct inaccurate personal information.

Retailers should be allowed to offer both online and offline customer service options to make corrections. Not all retailers may be able to offer electronic service. In addition, there should be a reasonable amount of time for retailers to make corrections or request extensions as necessary.

Consumer correction requests should be accompanied with evidence that proves the consumer's factual information is false. Businesses should not be required to undertake their own research or reviews, nor should "correction" requests include subjective inferences or conclusions about matters such as customer behavior.

b. How often, and under what circumstances, a consumer may request a correction to their personal information.

Requests should be limited to no more than once per day, to protect against hackers using automated systems to burden businesses with requests.

c. How a business must respond to a request for correction, including the steps a business may take to prevent fraud.

The request should be accompanied by identity verification with at least two data points chosen at the retailer's discretion before the retailer may proceed with changes. The Agency may consider including a list of acceptable data points retailers and other businesses may choose. Requests should be limited to consumers themselves or herself or another party with power of attorney.

d. When a business should be exempted from the obligation to take action on a request because responding to the request would be "impossible, or involve a disproportionate effort" or because the information that is the object of the request is accurate.

Retailers have multiple different places where data are kept or stored, but there are primary data stores that constitute a live "master record" from which consumer information is transmitted. Corrections should be required only to that master record. Data that is difficult to access and rarely used, including archived data stores, previous backups, and disconnected systems should be exempt from correction requirements.

e. A consumer's right to provide a written addendum to their record with the business, if the business rejects a request to correct their personal information.

No Comment.

5. *Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information*

The CCPA gives consumers the right to opt out of the sale of their personal information by covered businesses.[28] In 2020, the Attorney General adopted regulations to implement consumers' right to opt out of the selling of their personal data under the CCPA. The CPRA now provides for additional rulemaking to update the CCPA rules on the right to opt-out of the sale of personal information, and tocreate rules to limit the use of sensitive personal information, and to account for other amendments.

Comments on the following topics will assist the Agency in creating these regulations:

a. What rules and procedures should be established to allow consumers to limit businesses' use of their sensitive personal information.

Retailers should have an exception for the use of precise geolocation that is directly related to the retailer fulfilling its obligations to deliver purchases or information about purchases customers have made (e.g., curbside or store pickup), or for other operational purposes (e.g., resource planning within stores based on in-store traffic patterns).

b. What requirements and technical specifications should define an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer's intent to opt out of the sale or sharing of the consumer's personal information or to limit the use or disclosure of the consumer's sensitive personal information.

Please see comments above regarding "global opt-out".

c. What technical specifications should be established for an opt-out preference signal that allows the consumer, or the consumer's parent or guardian, to specify that the consumer is less than 13 years of age or at least 13 years of age and less than 16 years of age?

Any age signal should be universally accepted, identifiable, and should not indicate precise age but perhaps an age range.

d. How businesses should process consumer rights that are expressed through opt-out preference signals?

No comment.

e. What businesses should do to provide consumers who have previously expressed an opt-out preference via an opt-out preference signal with the opportunity to consent to the sale or sharing of their personal information or the use and disclosure of their sensitive personal information.

The selection of more granular preferences with an entity should override the general signal. Otherwise, retailers and others will face a constant challenge of tracking and responding to general preferences and the consumer's own granular preferences.

6. *Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information*

The CCPA gives businesses certain responsibilities, and consumers certain rights, related to consumers' personal information. The CPRA amends the CCPA to give consumers additional rights over a new category of information: "sensitive personal information," and directs the Agency to amend existing regulations and/or issue new regulations to implement these rights. These rights include the new right to limit the use and disclosure of sensitive personal information discussed above.

Comments on the following topics will assist the Agency in creating regulations on this topic:

a. What constitutes "sensitive personal information" that should be deemed "collected or processed without the purpose of inferring characteristics about a consumer" and therefore not subject to the right to limit use and disclosure.

Data used solely for the purposes of establishing identity, and data that is reasonably necessary to provide the service requested by the consumer.

b. What use or disclosure of a consumer's sensitive personal information by businesses should be permissible notwithstanding the consumer's direction to limit the use or disclosure of the consumer's sensitive personal information.

Retailers should be able to use geolocation for the purpose of providing services, and anything required to provide those services, to a customer pursuant to a contract or other purchasing arrangement.

7. *Information to Be Provided in Response to a Consumer Request to Know (Specific Pieces of Information)*

When businesses are required to disclose specific pieces of information to a consumer, the CPRA generally requires the disclosure to cover the 12 months prior to a consumer's request. However, for all information processed on, or after January 1, 2022, consumers may request, and businesses must disclose, information beyond the 12-month window subject to the exception described in a. below.

Comments on the following topic will assist the Agency in creating regulations on this topic:

What standard should govern a business's determination that providing information beyond the12-month window is "impossible" or "would involve a disproportionate effort."
Retrieval and production of such information may be impossible and would certainly require a disproportionate amount of effort if it is located in a non-active or downstream location. This includes information in Service Provider locations/data stores and information that has been de-identified and commingled with other information for analytics purposes.

Relevance of specific information to the purpose of the request should also be a factor in determining whether it should be produced.

8. *Definitions and Categories*

The CCPA and CPRA provide for various regulations to create or update definitions of important termsand categories of information or activities covered by the statute.

Comment on the following topics will assist the Agency in deciding whether and how to update or createthese definitions and categories:

a. Updates or additions, if any, that should be made to the categories of "personal information" given in the law.

No comment.

b. Updates or additions, if any, that should be made to the categories of "sensitive personal information" given in the law.

No comment.

c. Updates, if any, to the law's definitions of "deidentified" and/or "unique identifier." Changes, if any, that should be made to the definition of "designated methods forsubmitting requests" to obtain information from a business.

Do not require more than two designated methods (one online; one with a customer service rep)

d. Further defining the business purposes for which businesses, service providers, and contractors may combine consumers' personal information that was obtained from different sources.

Retailers and their vendors should be allowed to combine such information where it is necessary to fulfill contractual obligations to a customer (e.g., purchase fulfillment), and for product and service improvement purposes. This will be important to avoid disadvantaging small- to mid-sized retaielrs that lack the large databases of first party data held by large entities.

e. The changes, if any, that should be made to further define when a consumer "intentionally interacts" with a person.

f. The changes, if any, that should be made to further define "precise geolocation."

No comment.

g. What definition of "specific pieces of information obtained from the consumer" the Agency should adopt.

No comment.

h. The regulations, if any, that should be adopted to further define "law enforcement agency-approved investigation."

No comment.

i. The regulations, if any, that should be adopted to further define "dark patterns."

Please see comments at the top on "dark patterns".

9. Additional Comments

Please provide any additional comments you may have in relation to the Agency's initial rulemaking.

No Comment.