



November 20, 2022

California Privacy Protection Agency
2101 Arena Blvd., Sacramento, CA 95834
Attn: Brian Soublet

VIA Email: regulations@coppa.ca.gov.

Dear Members of the Committee:

On behalf of the California Retailers Association please see our comments related to the California Consumer Privacy Act Regulations and the formal rulemaking process to adopt regulations to implement the Consumer Privacy Rights Act of 2020 (CPRA).

General concerns around the discrepancy between the text of CPRA and the CPPA regs concerning the Opt-out Preference Signal.

CPRA makes the Global Privacy Control / Universal opt-out preference signal optional, while the CPPA is making it mandatory in its regulations. Given the text of CPRA's optional treatment of these signals, it's safe to assume many businesses have not yet stood up initiatives or have made investments to support. Now with Attorney General enforcement in this area brought upon retailers, there is concern about regulatory enforcement risk amidst ambiguity.

At a minimum, if making it mandatory, we ask the agency to provide a post-Jan 1, 2023, timeline for compliance with net-new requirements. Additionally, we ask for the establishment of more prescriptive technical standards for the preference signal. Although there are groups who provide a list of browsers that have this preference signal, there are currently 7 different browsers, uniformity in technical standards would make it easier for business to receive and honor signals.

Below are California Retailers Association comments on specific sections:

§7002(b)(3) Restrictions on the Collection and Use of Personal Information.

Revised Rule Text: *The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer. The consumer's reasonable expectations concerning the purpose for which the personal information will be collected or processed shall be based on the following factors: . . . (3) The source of the personal information and the business's method for collecting or processing it. For example, if the consumer is providing their personal information directly to the business while using the business's product or service, the consumer likely expects that the business will use the personal information to provide that product or service. However, **the consumer may not expect that the business will***

use that same personal information for a different product or service offered by the business or the business's subsidiary.

Action Requested: How a business uses collected data across its products and services should not be unduly limited where the privacy notice expressly discloses those potential uses and that it might occur across products/services. To the extent this factor is retained, it should focus on whether the use of the different product or service is unexpected and unrelated.

Proposed Edit: However, the consumer may not expect that the business will use that same personal information for **an unexpected and unrelated use on a** different product or service offered by the business or the business's subsidiary.

§7002(b)(4) Restrictions on the Collection and Use of Personal Information.

Revised Rule Text: *The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer. The consumer's reasonable expectations concerning the purpose for which the personal information will be collected or processed shall be based on the following factors: . . . (4) **The specificity, explicitness, and prominence of disclosures to the consumer about the purpose for collecting or processing the consumer's personal information, such as in the Notice at Collection and in the marketing materials to the consumer about the business's good or service.** For example, the consumer that receives a pop-up notice that the business wants to collect the consumer's phone number to verify their identity when they log in likely expects that the business will use the personal information for the purpose of verifying the consumer's identity. Similarly, the consumer may expect that a mobile application that markets itself as a service that finds cheap gas close to the consumer will collect and use the consumer's geolocation information for that specific purpose when they are using the service.*

Action Requested: Marketing and other non-privacy disclosures should not be a relevant factor in determining a consumer's reasonable expectation about the disclosures in the privacy notice. The purpose of the privacy notice is to provide a one-stop notice for consumers regarding how their data is used. In contrast, marketing materials highlight the benefits for the product or service and thus are not necessarily relevant to how data is used unless the disclosure makes that connection explicit (as occurs in the first example about the pop-up notice).

Proposed Edit: The specificity, explicitness, and prominence of disclosures to the consumer about the purpose for collecting or processing the consumer's personal information, **such as** in the Notice at Collection **and in the marketing materials to the consumer about the business's good or service.** For example, the consumer that receives a pop-up notice that the business wants to collect the consumer's phone number to verify their identity when they log in likely expects that the business will use the personal information for the purpose of verifying the consumer's identity. **Similarly, the consumer may expect that a mobile application that markets itself as a service that finds cheap gas close to the consumer will collect and use the consumer's geolocation information for that specific purpose when they are using the service.**

§7002(b)(5) Restrictions on the Collection and Use of Personal Information.

Revised Rule Text: *The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer. The consumer’s reasonable expectations concerning the purpose for which the personal information will be collected or processed shall be based on the following factors: . . . (5) **The degree to which the involvement of service providers, contractors, third parties, or other entities in the collection or processing of personal information is apparent to the consumer.** For example, the consumer likely expects an online retailer’s disclosure of the consumer’s name and address to a delivery service provider in order for that service provider to deliver a purchased product, because that service provider’s involvement is apparent to the consumer. By contrast, the consumer may not expect the disclosure of personal information to a service provider if the consumer is not directly interacting with the service provider or the service provider’s role in the processing is not apparent to the consumer.*

Action Requested: This added factor, as phrased, should not be relevant in determining a consumer’s reasonable expectation. In general, consumers do not have the business background to understand processor relationships or any reason to reflect on how a business processes their data. To the extent this factor is retained, the rule should be modified to focus on uses that are unexpected and offensive with respect to the disclosed uses.

Proposed Edit: The degree to which the involvement of service providers, contractors, third parties, or other entities in the collection or processing of personal information **would be unexpected [and offensive] is apparent to the consumer.**

§7004(a)(2) Symmetry in choice

Revised Rule Text: *The path for a consumer to exercise a more privacy-protective option shall not be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option because it impairs or interferes with the consumer’s ability to make a choice.*

Action Requested: The revised provision still places an undue burden on design to the extent it requires exact symmetry in length, which might not be appropriate in all instances. The revised suggested edit below makes clear that lack of symmetry is a dark pattern only when it results in impairing or interfering with ability to make a choice.

Proposed Edit: The path for a consumer to exercise a more privacy-protective option shall not be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option **because to the extent** it impairs or interferes with the consumer’s ability to make a choice.

§7015(b) Alternative Opt-Out Link.

Revised Rule Text: *A business that chooses to use an Alternative Opt-out Link shall title the link, “Your Privacy Choices” or “Your California Privacy Choices,” **and shall include the following opt-out icon to the right or left of adjacent to the title.** The link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business’s internet Homepage(s). The icon shall be approximately the same size as **any** other icons used by the business in the header or footer **of** on its webpage.*

Action Requested: The draft CPRA rules would mandate the opt-out icon that was only optional under the 2020 CCPA rules. This icon should not be mandated because it has the potential to confuse consumers since the static image looks like a toggle that a consumer can activate. It also prescribes a graphic feature that may not align with a business' design layout, putting unnecessary burden on a business without countervailing consumer benefit.

Proposed Edit: A business that chooses to use an Alternative Opt-out Link shall title the link, "Your Privacy Choices" or "Your California Privacy Choices," and **shall may** include the following opt-out icon adjacent to the title.

§7025(b) Opt-Out Preference Signals

Revised Rule Text: (1) *The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field **or JavaScript object.***

Action Requested: Requirements to honor UOOMs should not exceed the capabilities of eligible UOOMs that are available in the marketplace (e.g., if only browser extensions can serve as UOOMs, the requirement to honor UOOM signals should only extend to browsers).

The preference signal should also offer a consumer to both turn on and off the opt-out preference. As currently drafted, the regulations deprive the consumer of the ability to fully control opt-out preference.

Proposed Edit: A business shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:

(1) The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field.

(2) The signal shall have the capability to indicate that the consumer has selected to turn off the opt-out preference signal.

~~(2)~~(3) The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information. The configuration or disclosure does not need to be tailored only to California or to refer to California.

(4) The business's obligation to process a preference signal shall not exceed the technical capability of the platform, technology, or mechanism that sends the opt-out preference signal. For instance, where a signal is in an HTTP header field format, the business shall process the signal only where it is received on a browser.

§7025(c)(7)(A) Opt-Out Preference Signal Example

Revised Rule Text: *Caleb visits Business N's website using a browser with an opt-out preference signal enabled, **but he is not otherwise logged into his account and the business cannot otherwise associate Caleb's browser with a consumer profile the business maintains.** Business N collects and shares Caleb's **personal information tied to his browser** identifier for cross-contextual advertising, **but Business N does not know Caleb's real identity because he is not logged into his account.** Upon receiving the opt-out preference signal, Business N*

shall stop selling and sharing Caleb’s **information linked to Caleb’s browser** identifier for cross-contextual advertising, but it would not be able to apply the request to opt-out of the sale/sharing to Caleb’s account information because the connection between Caleb’s browser and Caleb’s account is not known to the business.

Action Requested: The added language may require companies to take extra action to associate an unauthenticated visitor with an account which is less privacy friendly. The focus should be on whether the visitor is logged in to avoid any obligation for a company to process additional personal data.

Proposed Edit: Caleb visits Business N’s website using a browser with an opt-out preference signal enabled, but he is not otherwise logged into his account. **and the business cannot otherwise associate Caleb’s browser with a consumer profile the business maintains.**

§7026(a)(1) Requests to Opt-Out of Sale/Sharing.

Revised Rule Text: ~~If a~~ **A** business that collects personal information from consumers online, ~~the business~~ shall, at a minimum, allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and ~~through at least one of the following methods~~—an interactive form accessible via the “Do Not Sell or Share My Personal Information” link, the Alternative Opt-out Link, or the business’s privacy policy **if the business processes an opt-out preference signal in a frictionless manner.**

Action Requested: The Agency should remove the added limitation for processing in a frictionless manner because the alternatives and the benefits to the consumer are unclear.

Proposed Edit: A business that collects personal information from consumers online shall, at a minimum, allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and at least one of the following methods—an interactive form accessible via the “Do Not Sell or Share My Personal Information” link, the Alternative Opt-out Link, or the business’s privacy policy. **if the business processes an opt-out preference signal in a frictionless manner.**

We seek clarity on the following sections:

§7002(a) Restrictions on the Collection and Use of Personal Information.

This section states the business’s information practice must be reasonably necessary and proportionate to achieve (1) the purposes for which the PI was collected or (2) another disclosed purpose that is compatible with the context in which the PI was collected. For (1), the draft states the purposes for which the PI was collected is within “reasonable expectation” narrowly by stating using PI collected in one transaction for a different product/service is not reasonably expected. See 7002(b)(3). For (2), the section then states whether “another disclosed purpose” is compatible would be based on the factors disclosed in (b) or for business purposes disclosed in 1798.140(e), which specifically excludes targeted advertising.

Reading them together, it is no longer clear whether a business can use the information collected during a transaction for subsequent direct marketing (e.g., a customer bought a washer, and the retailer uses the information to market a matching dryer). In addition, it is even more unclear whether a retailer can use the

information for subsequent targeted advertising due to the exclusion stated in (2), even if it discloses the purposes in the privacy statement.

The regulatory language deviates from the CPRA statutory language in two aspects: (1) The language is unclear as to whether it is essentially converting the CCPA from a notice and consent regime to an opt-in regime for secondary marketing use, and (2) for targeted marketing, the current CCPA is an opt-out regime, but the new language deviates from that approach.

§ 7050. Service Providers and Contractors

Proposed section 7050(b) considers someone who contracts with a business to provide cross-contextual behavioral advertising as a third party and not a service provider or contractor, which is a distinction without much value for California consumers. A company that provides cross-contextual behavioral advertising service should be considered a service provider if the business only uses personal information to provide the advertising services. If the company is not using the personal information for its own purposes and only uses it to provide services as laid out in the agreement, there is no reason why they should not be considered a service provider. As written, this section will only harm advertising businesses without benefiting consumers.

Additionally, the example noted in proposed section 7050(c)(2) of the draft regulations purports to prohibit a form of widely accepted advertising based on email addresses. This example is inconsistent with the text of CPRA, including Section 1798.140(e)(6), (j)(1)(A)(iv), and (ag)(1)(D). The example would have significant implications for businesses, particularly small retailers, that rely on these advertising tools to reach their customers with information that has been provided to them for this purpose. A customer list that a business uploads, provided they have the necessary permission to do so, helps them reach their own customers in a privacy-protective way. Restricting the ability for California businesses to continue to use such tools will make it harder for them to reach their customers on social media platforms, increase the costs these businesses incur for advertising, and disproportionately affect their ability to compete against their competitors outside of the State.

Thank you for the consideration of our concerns and our suggestions on clarification. If you have any questions or would like additional input, please do not hesitate to reach out to me directly.



Rachel Michelin
President & CEO
California Retailers Association